П.А.Крылов
А.А. Туганбаев
А. Р. Чехлов

ЗАДАЧИ И УПРАЖНЕНИЯ ПО ОСНОВАМ ОБЩЕЙ АЛГЕБРЫ

учебное пособие

ФЛИНТА

П.А. Крылов
А.А. Туганбаев
А.Р. Чехлов

ЗАДАЧИ И УПРАЖНЕНИЯ ПО ОСНОВАМ ОБЩЕЙ АЛГЕБРЫ

Учебное пособие

Рекомендовано НМС по математике и механике УМО по классическому университетскому образованию РФ в качестве учебного пособия для студентов высших учебных заведений, обучающихся по группе математических и механических специальностей

Москва
Издательство «ФЛИНТА»
2012

УДК 512.5
ББК 22.144
К85

Крылов П.А.
К85 Задачи и упражнения по основам общей алгебры [Электронный ресурс] : учеб. пособие / П.А. Крылов, А.А. Туганбаев, А.Р. Чехлов. — М.: ФЛИНТА, 2012. —208 с.

ISBN 978-5-9765-1507-9

В форме задач книга содержит основы таких важнейших разделов современной алгебры как группы, кольца и модули, решетки, полугруппы, поля.

Книга будет полезна на занятиях со студентами физико-математических факультетов университетов, в том числе при чтении спецкурсов, и в процессе руководства магистрантами и аспирантами. Ее можно также использовать в качестве справочника.

Для студентов, аспирантов, преподавателей и научных сотрудников, интересующихся алгеброй.

УДК 512.5
ББК 22.144

ISBN978-5-9765-1507-9

Оглавление

Предисловие

Данная книга является сборником задач по различным разделам общей алгебры. Предназначена для самой широкой аудитории: от студентов младших курсов до специалистов. Она рассчитана как учебное пособие для физико-математических факультетов университетов, и одной из ее целей является обеспечение задачами общих и специальных математических курсов. Студентам и аспирантам, специализирующимся по алгебре, она будет полезна при выполнении магистерских и диссертационных работ. Всем категориям читателей она может служить справочником.

Книга содержит как задачи для первоначального ознакомления с некоторыми понятиями и фактами общей алгебры, так и упражнения повышенной трудности для читателя, который обладает достаточной математической культурой и специальной подготовкой. Большинство задач носит теоретический характер. Это поможет в значительной степени удовлетворить запросы сильных студентов и подготовить их к чтению специальной литературы.

Обширный материал делает невозможным охватить все части общей алгебры в одной книге. Преследовалась цель показать читателю богатство содержания и разнообразие методов ряда важнейших разделов этой науки.

При подборе задач использовались сборники [44], [25], [26], [42], [50], [33], [5], [55], а также другие учебники и монографии, приведенные в литературе. Энциклопедическим трудом по алгебре является классическая монография [9]. Признание получили книги [27], [31], [46]. Отличный от традиционного подход к алгебре развивается в [56]. Те или иные направления общей алгебры представлены в книгах [2], [3], [10], [12], [15], [22], [36], [49]. Имеется богатая литература по главным ветвям общей алгебры. Началам теории решеток посвящена книга [45]. Классическая теория решеток отражена в [7] и [14]. Полугруппы рассматриваются в [18], [34] и [57]. Библиография по теории групп довольно обширна. После общепризнанных книг [16], [28], [53] можно перейти к другим указанным источникам: [6], [8], [11], [13], [19], [21], [29], [35], [40], [47], [48], [54], [58], [60], [61]. Книги [4], [17], [30] хороши для первоначального знакомства с теорией колец и модулей. Для пополнения знаний в этой области можно использовать книги [20], [24], [37], [43], [51]. В качестве учебного пособия по теории конечномерных ассоциативных алгебр можно порекомендовать книгу [39]. Весьма полным руководством по теории абелевых групп остается двухтомная монография [52]. Есть также книги [23], [24], [37], [59], [62], [63], [64]. С алгебраической теорией чисел можно ознакомиться по [1]. Знакомство с теорией полей можно начать по книгам [9], [22], [31], [32], [38], [41].

Предполагается, что читатель в целом уже знаком с терминологией и исходными теоремами. Тем не менее, в каждом параграфе приводятся основные понятия и обозначения, встречающиеся далее в упражнениях. Иногда понятия объясняются в текстах задач. Для удобства работы в начале книги имеются список обозначений и терминов и предварительные сведения, а в конце — предметный указатель.

Некоторые задачи снабжены ответами и указаниями, нередко достаточно подробными. Это пригодится читателю в его самостоятельной работе. Часть упражнений имеет форму утверждений. Предполагается, что читатель может попробовать доказать соответствующий факт.

Введение

К общей алгебре обычно относят разделы алгебры, изучающие такие алгебраические системы как группы, кольца, полугруппы, решетки и т.п. Есть разделы алгебры, традиционно не считающиеся принадлежащими общей алгебре. Например, линейная и полилинейная алгебра, алгебраическая теория чисел. Конечно, принцип деления алгебры на общую и «оставшуюся» весьма условен. Неясно, включать ли в общую алгебру теорию полей или категорий.

В любом случае не подлежит сомнению, что теория групп и теория колец остаются фундаментом общей алгебры. И именно упражнения о группах и кольцах составляют главное содержание сборника. С теорией колец неразрывно связана теория модулей — одно из современных направлений в теории колец.

Задачи по абелевым группам составляют самостоятельную главу, что отражает реальную ситуацию с этой ветвью алгебры. Решеткам и полугруппам отведено по одному параграфу, хотя это и не соответствует их значению в математике. Учитывая исключительную важность полей для всей математики, им посвящена отдельная глава.

Некоторые конечные группы и конечномерные алгебры были исследованы в 19 веке. На рубеже 19 и 20 веков было осознано, что алгебраические объекты следует определять аксиоматически. А в 20-е годы прошлого века пришло понимание того, что алгебра должна изучать произвольные множества с заданными на них алгебраическими операциями. Это был период становления современной алгебры, проходивший на фоне проникновения в алгебру теоретико-множественных методов. Алгебра стала аксиоматической наукой. Публикация в 1930 и 1931 годах двухтомной «Современной алгебры» Ван дер Вардена зафиксировала новый статус алгебры.

Последующее развитие общей алгебры характеризуется как исключительно интенсивное. Ее классические объекты, прежде всего группы и кольца, были подвергнуты детальному и систематическому изучению. Появились и оформились в самостоятельные направления новые области исследования, посвященные различным другим алгебраическим образованиям. Открылось большое число связей общей алгебры с сопредельными разделами науки.

Теория групп, несмотря на относительную молодость, имеет интересную и содержательную историю. От Ж.-Л. Лагранжа, стихийно применявшего группы перестановок, до работ Э. Галуа, где уже сознательно используется идея группы (им же впервые введен и сам термин), — вот путь, по которому развивалась эта идея в рамках теории алгебраических уравнений. Независимо идея группы возникла в геометрии, когда в середине 19 столетия на смену единой античной геометрии пришли многочисленные «геометрии» и остро встал вопрос об установлении связей и родства между ними. Выход был указан «Эрлангенской программой» Ф. Клейна, положившей в основу классификации геометрий понятие группы преобразований. Третий источник понятия группы — теория чисел. Здесь можно отметить работы Л. Эйлера и К.Ф. Гаусса.

Осознание в конце 19 века принципиального единства теоретико-групповых идей, существовавших к тому времени независимо в разных областях математики, привело к выработке современного понятия группы (А. Кэли, Г. Фробениус и др.). Итог начального развития теории групп как групп перестановок был подведен в книге К. Жордана «Курс теории перестановок и алгебраических уравнений» (1870). Первой книгой, посвященной абстрактной теории групп и рассматривавшей только конечные группы, является книга У. Бернсайда «Теория групп конечного порядка» (1897). Впервые изложение основ теории групп, без предположения конечности рассматриваемых групп, было предпринято в книге О.Ю. Шмидта «Абстрактная теория групп» (1916).

Подход Клейна к проблеме классификации геометрий оказался полезным в математике и других науках. Это объясняется тем, что свойства группы преобразований, оставляющих инвариантной некоторую структуру, отражают многие свойства самой этой структуры. Например, изучение группы пребразований, относительно которых инвариантны силы, связывающие вместе атомы в молекулах, позволяет многое узнать о поведении спектров молекул.

Теория групп является мощным инструментом познания одной из глубоких закономерностей физического мира — симметрии. Всюду, где идет речь о симметрии, проявляется систематизирующая роль теории групп. В этом одна из причин востребованности данной теории.

Изучая группы преобразований или симметрии, по существу имеют дело с автоморфизмами различных объектов. В математике, как и вообще в естествознании, группы нередко возникают в виде групп автоморфизмов каких-либо математических структур. Такая форма применения теории групп обеспечивает ей уникальное положение в алгебре.

Алгебраическая топология демонстрирует другой распространенный способ изучения неалгебраических объектов с помощью групп. Его суть — в сопоставлении с такими объектами определенных групп и в последующем их исследовании.

В настоящее время теория групп является одной из самых развитых областей алгебры, а понятие группы — одним из наиболее важных, плодотворных и всеобъемлющих математических понятий. Квантовая механика, физика твердого тела, химия и экономика — вот далеко не полный перечень областей, где полезность и необходимость применения теории групп общепризнаны. Как и вся математика, теория групп находится сейчас в состоянии динамического развития.

Произвольные ассоциативные кольца и алгебры стали предметом постоянного интереса в 20–30-е годы 20 века. До этого теория колец развивалась как теория конечномерных алгебр. Теория конечномерных алгебр — один из самых старых разделов современной алгебры. Его появление связано с работами У. Гамильтона, открывшего знаменитое тело кватернионов (1843), А. Кэли, разработавшего теорию матриц, и Г. Грассмана. В это время постепенно начинает формироваться понятие гиперкомплексной системы. Гиперкомлексная система, говоря сегодняшним языком, — это конечномерная ассоциативная алгебра над полем вещественных чисел $\mathbb{R}$ или полем комплексных чисел $\mathbb{C}$. Гиперкомплексными системами занимались многие замечательные математики (К. Вейерштрасс, Р. Дедекинд, К. Жордан, Б. Пирс, К.С. Пирс, Г. Фробениус и др.). Фробениусу принадлежит исторически первая теорема структурной теории алгебр (1886). Всякая конечномерная алгебра с делением над полем $\mathbb{R}$ изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо телу кватернионов (см. 12.70). Теория гиперкомплексных систем достигла своего апогея в самом конце 19 века. Ф.Э. Молин (1893) и Э. Картан (1898) описали полупростые комплексные и вещественные алгебры.

Новый этап в развитии конечномерных алгебр связан с рассмотрением в начале 20 века алгебр над произвольным полем. Дж. Веддерберн (1908) перенес теоремы Молина и Картана на случай произвольного поля.

В 20–30-е годы 20 столетия алгебраисты немецкой школы, группировавшиеся вокруг Э. Нетер, Э. Артина и Р. Брауэра, распространили теорию Молина-Картана-Веддерберна на ассоциативные кольца с условием минимальности для односторонних идеалов (артиновы кольца), после чего она приобрела знакомую нам форму.

Общая структурная теория колец была основана в 40-х годах прошлого века. Центральной идеей этой теории является концепция радикала. Начало общей теории радикалов колец и алгебр было положено А.Г. Курошем.

С формальной точки зрения понятие модуля над кольцом обобщает понятие векторного пространства над полем, когда роль области скаляров играет некоторое кольцо. Такое алгебраическое образование позволяет единообразно трактовать обычные пространства и абелевы группы и группы с операторами. Рассмотрение модулей над кольцом R в определенном смысле равносильно рассмотрению его представлений (гомоморфизмов) в кольцах эндоморфизмов абелевых групп. Модули естественным образом возникают в различных математических исследованиях. Так, центральная задача теории линейных представлений групп — это изучение модулей над групповыми алгебрами.

Конечные абелевы группы, т.е. модули над кольцом целых чисел $\mathbb{Z}$, появились у Гаусса как группы классов бинарных квадратичных форм. Он, в частности, заметил, что не все эти группы являются циклическими. Первый и замечательный пример разложения бесконечной абелевой группы в прямую сумму циклических был дан П. Дирихле (1846) в работе о единицах (обратимых элементах) поля алгебраических чисел. Фробениус и Штикельбергер (1878) доказали разложимость конечной абелевой группы в прямую сумму циклических. Некоторые фрагменты этой основной теоремы о конечных абелевых группах и ее доказательства отыскиваются у Гаусса. Понятие модуля встречается впервые в 60–80-х годах 19 века в работах Р. Дедекинда и Л. Кронекера, посвященных арифметике полей алгебраических чисел и алгебраических функций (Дедекинд называл его «порядком»). Э. Нетер и В. Крулль выявили ведущую и синтезирующую роль понятия модуля для многих ситуаций.

Вторая половина прошлого века была временем бурного развития теории колец и модулей как единой дисциплины. Теория колец и модулей обогатилась мощными методами и замечательными теоремами, превратившись в богатую и разветвленную часть математики. Она нашла многочисленные применения как в математике, так и в смежных науках. Понятие кольца остается, наряду с понятием группы, одним из основных не только алгебраических, но и общематематических понятий.

Абелевы (т.е. коммутативные) группы так названы в честь Н. Абеля (1802–1829), который изучал алгебраические уравнения с коммутативными группами Галуа. Мы уже писали, что конечные коммутативные группы впервые фактически рассматривал Гаусс.

Своеобразие теории абелевых групп в том, что ее лишь формально можно отнести к общей теории групп. Условие коммутативности оказывается весьма специфическим для групповой структуры. Абелевы группы можно также считать модулями над кольцом целых чисел. Подобная точка зрения достигла полной отчетливости в 50–60-е годы прошлого века. Это время старта современной теории модулей и становления в математике теоретико-категорного мышления перестроило теорию абелевых групп.

Характер основных идей, методов и результатов теории абелевых групп определяет ее как ветвь теории модулей, использующую особенности кольца целых чисел. Необходимо сразу уточнить, что мы имеем дело с настолько особой областью, что она (т.е. теория абелевых групп) образует самостоятельный раздел алгебры. Велико и обратное влияние. Развитие теории модулей тесно связано с абелевыми группами как $\mathbb{Z}$-модулями. Немало примеров обобщений теорем об абелевых группах на модули над различными кольцами.

Изучение абелевых групп принесло много образцов того, что алгебраисты называют структурной теорией. До 50-х годов 20 века история абелевых групп была прерывистой, от одной вершины до другой. В 1933-м и 1934-м годах появились теорема Ульма о счетных p-группах и критерий Л.С. Понтрягина свободы счетной группы. Следующие две вехи — это теория Р. Бэра вполне разложимых групп без кручения (1937) и работы Л.Я. Куликова о p-группах (1941, 1945). В 1954-м году вышла в свет богатая новыми идеями книга И. Капланского [62]. В ней впервые продемонстрирована близость теории абелевых групп и теории модулей, особенно над коммутативными областями главных идеалов.

Систематическая работа над абелевыми группами началась в 50-х годах. Одно из достижений этого нового периода — построение теории смешанных групп Уорфилда, объединившей теории счетных p-групп и вполне разложимых групп без кручения.

Основные примеры полей — это числовые поля: поле рациональных чисел $\mathbb{Q}$, поле вещественных чисел $\mathbb{R}$, поле комплексных чисел $\mathbb{C}$, и такие «нечисловые» поля, как конечные, в частности, поля вычетов $\mathbb{Z}_p$. Конечные поля имеют много важных применений, одно из них к теории кодирования. Еще в конце 19 века к примерам «нечисловых» или «абстрактных» полей, какими можно считать конечные поля, прибавились поля формальных степенных рядов, введенные Веронезе, и p-адические поля К. Гензеля.

Хотя поле и является коммутативной областью, однако это весьма специфическое кольцо. Теория полей, а также тесно связанная с ней теория многочленов составляют отдельное направление в математике со своими проблематикой и методами.

Зарождение в середине 19 столетия теории полей проходило в рамках решения алгебраических уравнений — основного содержания алгебры того периода. Набирающие силу во второй половине 19 века исследования по алгебре и теории чисел привели к необходимости изучения природы различных числовых систем. Объекты, близкие к полям, появились в работах Л. Кронекера и Р. Дедекинда (у Дедекинда — «рациональные области»). Термин «поле» употребил Дирихле в книге «Теория чисел» (1871).

Трудно найти такой раздел математики, где не встречались бы поля. Но это и не удивительно, ведь поля наиболее соответствуют нашему интуитивному представлению о том, какими должны быть «абстрактные» числовые системы.

Истоки теории решеток относятся к 19 веку. Систематическая работа над решетками (раньше говорили также «структура») началась в 30-х годах прошлого века. Публикация книги Г. Биркгофа «Lattice Theory» (1940) объявила о появлении нового самостоятельного направления в алгебре — теории решеток. Дальнейшее развитие этой области было отражено во втором (1948) и третьем (1967, имеется русский перевод [7]) изданиях этой книги. Решетку можно задать как алгебраическую систему (упр. 1.3). Но, что несомненно, имеющееся на решетке упо-

рядочивание оказывает неповторимый эффект на ее свойства. Внутренняя красота и диапазон применения теории решеток в математике и других науках напоминают теорию групп.

Вся современная алгебра насыщена теоретико-решеточными понятиями. Решетки постоянно встречаются и в других разделах математики (логике, геометрии и топологии, анализе, теории вероятностей). Хорошо известен прикладной характер теории булевых алгебр (они являются решетками). Кстати, и своему появлению понятие «решетка» во многом обязано изучению булевых алгебр.

Использование решеточных понятий в математике и ряде других наук иногда помогает лучше понять поведение объектов исследования, позволяет формулировать рассматриваемые теории более просто и единообразно.

Место и роль теории полугрупп в математике определяются тем принципиальным обстоятельством, что композиция преобразований произвольного множества M ассоциативна. Всякая замкнутая относительно композиции совокупность преобразований множества M является полугруппой. И обратно, любая полугруппа изоморфна некоторой полугруппе преобразований. Теория полугрупп — это математическая наука о преобразованиях множеств самого общего вида.

Полугруппы, как и решетки, вездесущи! Они возникают всюду, где есть потребность в рассмотрении тех или иных преобразований множеств. Это, например, полугруппы операторов функциональных пространств, полугруппы эндоморфизмов групп, колец, модулей, графов, решеток. Полугруппы часто встречаются там, где имеет смысл понятие «произведения» или «композиции» каких-либо объектов. Например, полугруппа бинарных отношений на данном множестве. Внутри алгебры полугруппы контактируют прежде всего с теорией групп и теорией колец.

Начальные исследования, посвященные полугруппам, были выполнены в 20-е и 30-е годы прошлого столетия. А к концу 50-х годов теория полугрупп уже предстала достаточно развитой и глубокой теорией с собственной системой понятий, широким кругом проблем и богатым набором методов.

Предварительные сведения

Функцией Эйлера $\varphi(m)$ называется число натуральных чисел, не превосходящих данного натурального числа m и взаимно простых с m. Функция Эйлера *мультипликативна*, т.е. $\varphi(mn) = \varphi(m)\varphi(n)$ для взаимно простых m и n. Если $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение числа m, то

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_k}\right) = m\prod_{p|m}\left(1 - \frac{1}{p}\right).$$

Функция

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1, \\ (-1)^k, \text{ если } n = p_1 \dots p_k,\ p_i - \text{ различные простые}, \\ 0, \text{ если } n \text{ делится на квадрат } > 1, \end{cases}$$

называется *функцией Мебиуса.* Она также мультипликативна. Справедлива формула

$$\sum_{d|n}\mu(d) = \begin{cases} 1, \text{ если } n = 1, \\ 0, \text{ если } n > 1 \end{cases}$$

(суммирование ведется по всем делителям $d \geqslant 1$ числа n). А также ее модификация

$$\sum_{d|(n|m)}\mu\left(\frac{m}{n}\right) = \begin{cases} 1, \text{ если } d = m, \\ 0, \text{ если } d|m,\ d < m \end{cases}$$

(суммирование ведется по n, делящим m и делящимся на d).

Теорема 1. *Пусть f и g — две функции, определенные на $\mathbb{N}$, связанные соотношением $f(n) = \sum\limits_{d|n} g(d)$. Тогда справедлива так называемая формула обращения Мебиуса*

$$g(n) = \sum_{d|n}\mu\left(\frac{n}{d}\right)f(d).$$

Имеется еще мультипликативный аналог формулы обращения Мебиуса: если $f(n) = \prod\limits_{d|n} g(d)$, то

$$g(n) = \prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)}.$$

Теорема 2 (Ферма). *Для любого простого числа p и любого натурального a, не делящегося на p, справедливо сравнение*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Теорема 3 (Эйлер). *Для любого модуля m и любого натурального a, взаимно простого с m, справедливо сравнение*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Комплексное число называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами. В противном случае это число называется *трансцендентным*. Алгебраическое число называется *целым алгебраическим числом*, если оно является корнем унитарного многочлена с целыми коэффициентами. Множество целых алгебраических чисел образует кольцо — *кольцо целых алгебраических чисел* (28.18 3)). Если F — подполе поля комплексных чисел, то подмножество в нем, состоящее из целых алгебраических чисел, образует кольцо, называемое *кольцом целых алгебраических чисел* в F .

Если M — модуль, то под *нетривиальным* (соответственно, под *собственным*) понимается подмодуль, отличный от 0 и M (соответственно, от M). Ненулевой (соответственно, собственный) подмодуль модуля M называется минимальным (соответственно, максимальным), если он является минимальным (соответственно, максимальным) элементом в решетке всех подмодулей модуля M. Соответствующее соглашение действует для идеалов и для подгрупп. В литературе (в отличие от вышеприведенного соглашения) часто под «собственной» подгруппой группы G понимается «нетривиальная» ($\neq e, G$) подгруппа.

В книге используются элементарные свойства перестановок, матриц, определителей. Термины «отображение» и «функция» являются синонимами. Встречающиеся термины «инъективное (сюръективное, биективное) отображение» имеют обычный смысл. Вместо «биективное отображение» говорим также «биекция» или «взаимно однозначное соответствие».

Отображение множества A в себя называется *преобразованием* множества A. Подразумеваются известными основные свойства таких операций над множествами как пересечение, объединение, разность и декартово произведение. А также стандартные факты о счетных и континуальных множествах.

Список обозначений и терминов

Используются следующие общепринятые обозначения:

$\mathbb{N}$ — множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{Z}$ — группа или кольцо целых чисел, $\mathbb{Q}$ — группа или поле рациональных чисел, $\mathbb{R}$ и $\mathbb{C}$ — группы или поля вещественных и комплексных чисел соответственно, $\mathbb{R}_+$ — множество всех положительных вещественных чисел, $\mathbb{R}_+^*$ — мультипликативная группа положительных вещественных чисел. $\mathbb{Z}_n$ — группа или кольцо вычетов по модулю n, так же обозначается любая циклическая группа порядка n; $\mathbb{Z}_p$ (или F_p) — поле из p элементов; $\widehat{\mathbb{Z}}_p$ — группа или кольцо целых p-адических чисел; $\mathbb{Z}_{p^\infty}$ — квазициклическая p-группа; $\mathbb{Z}[i] = \{m+ni \mid m, n \in \mathbb{Z}\}$ — кольцо целых гауссовых чисел; $P(M)$ или 2^M — множество всех подмножеств множества M.

Если π — подмножество множества всех простых натуральных чисел Π, то через $\mathbb{Q}^{(\pi)}$ (соответственно, через $\mathbb{Q}_\pi$) обозначается группа или кольцо всех рациональных чисел, знаменатели которых взаимно просты с каждым $p \in \Pi \backslash \pi$ (соответственно, с каждым из $p \in \pi$). В частности, пишут $\mathbb{Q}^{(p)}$ (соответственно, $\mathbb{Q}_p$), если $\pi = \{p\}$.

$S(\Omega)$ — группа всех биекций множества Ω.

S_n и A_n — симметрическая и знакопеременная группы степени n, соответственно.

V_4 — четверная группа.

Q_8 — группа кватернионов.

D_n — группа диэдра (группа симметрий правильного n-угольника).

$\mathrm{GL}(n, K)$ и $\mathrm{SL}(n, K)$ — соответственно, полная и специальная линейные группы степени n над полем K.

a^g — элемент группы, сопряженный с a при помощи g.

a^G — класс сопряженных элементов группы G, содержащий a.

$o(a)$ — порядок элемента a группы G.

Если порядки элементов группы G ограничены в совокупности, то $\exp(G)$ — наименьшее общее кратное порядков ее элементов.

$A \times B$ — прямое произведение групп A и B.

$A \leftthreetimes B$ — полупрямое произведение групп A и B.

G_{x_0} — стабилизатор в G точки $x_0 \in \Omega$ при действии группы G на множестве Ω.

G' — коммутант группы G.

$Z(G)$ — центр группы G.

$t(G)$ — периодическая часть группы G.

$N_H(M)$, $C_H(M)$ — нормализатор, соответственно, централизатор подмножества M в подгруппе H группы G (если $H = G$, то индекс H обычно опускают).

$\operatorname{Aut} G$, $\operatorname{Inn} G$ — группа автоморфизмов, соответственно, внутренних автоморфизмов группы G.

$\operatorname{Hol} G$ — голоморф группы G.

Единица моноида, а также единичная подгруппа (если специально не оговорено) обозначается через e.

Матрица нильтреугольная — треугольная матрица (верхняя или нижняя) с нулями на главной диагонали.

Матрица унитреугольная — треугольная матрица (верхняя или нижняя) с единицами на главной диагонали.

$\mathbb{H}$ — алгебра вещественных кватернионов.

$\mathcal{C}a$ — алгебра Кэли.

Если R — кольцо, то через $M(n, R)$, $R[x]$, $R[[x]]$, $R\langle x\rangle$ обозначены соответственно, кольцо квадратных матриц порядка n, кольцо многочленов, кольцо формальных степенных рядов и кольцо рядов Лорана над кольцом R.

R^+ — аддитивная группа, $Z(R)$ — центр, а $U(R)$ или R^* — группа обратимых элементов (по-другому, мультипликативная группа) кольца R.

$R_1 \oplus \ldots \oplus R_m$ ($\bigoplus\limits_{i=1}^{m} R_i$) или $R_1 \times \ldots \times R_m$ ($\prod\limits_{i=1}^{m} R_i$) — прямая сумма или произведение колец $R_1, \ldots, R_m$.

$\prod\limits_{i\in I} R_i$ — произведение колец R_i, $i \in I$.

R^m — прямое произведение m изоморфных копий кольца R, где m — некоторое кардинальное число.

$A_1 \oplus \ldots \oplus A_m$ — прямая сумма идеалов $A_1, \ldots, A_m$ некоторого кольца.

$\operatorname{End} R$ — полугруппа эндоморфизмов, $\operatorname{Aut} R$ — группа автоморфизмов кольца R.

RG — групповое кольцо группы G над кольцом R.

(a) — главный идеал, порожденный элементом a коммутативного кольца.

(a, b) и $[a, b]$ — наибольший общий делитель и наименьшее общее кратное элементов a, b коммутативной области.

Если $d \neq 1$ — целое число, свободное от квадратов, то $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,|\, a, b \in \mathbb{Q}\}$ — квадратичное расширение поля $\mathbb{Q}$, $\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} \,|\, m, n \in \mathbb{Z}\}$.

$L(M)$ — решетка подмодулей модуля M.

$J(M)$ — радикал, $\operatorname{Soc} M$ — цоколь, $\operatorname{Ann} M$ — аннулятор модуля M.

$\operatorname{Ker} \varphi$ — ядро группового, кольцевого или модульного гомоморфизма φ.

$A_1 + \ldots + A_n$ ($\sum\limits_{i\in I} A_i$) — сумма подмодулей A_i некоторого модуля.

$A_1 \oplus \ldots \oplus A_n$ — (конечная) прямая сумма модулей $A_1, \ldots, A_n$.

$\bigoplus\limits_{i\in I} A_i$ ($\prod\limits_{i\in I} A_i$) — прямая сумма (прямое произведение) модулей A_i, $i \in I$.

$\bigoplus\limits_{m} A$ ($\prod\limits_{m} A$ или A^m) — прямая сумма (прямое произведение) m изоморфных копий абелевой группы или модуля A, где m — некоторое кардинальное число.

$\operatorname{Hom}(A, B)$ — группа гомоморфизмов группы A в абелеву группу B.

$\operatorname{Hom}_R(M, N)$ — группа гомоморфизмов из R-модуля M в R-модуль N.

$\operatorname{End} A$ — кольцо эндоморфизмов абелевой группы A.

$\operatorname{End}_R M$, $\operatorname{Aut}_R M$ — кольцо эндоморфизмов, соответственно, группа автоморфизмов R-модуля M.

$A \otimes B$, $A \otimes_R B$ — тензорное произведение абелевых групп A и B, соответственно, R-модулей A и B.

$\approx$ — квазиравенство.

$\sim$ — квазиизоморфизм.

$m \,|\, a$ — целое число m делит элемент a абелевой группы.

Если A — абелева группа и $a \in A$, то:

$r(A)$, $r_0(A)$ — ее ранг, соответственно, ранг без кручения;

$h_p^A(a)$ или $h_p(a)$ — p-высота элемента a;

$h_p^*(a)$ — обобщенная p-высота элемента a;

если не оговорено, то A_p — p-компонента;

nA (соответственно, $A[n]$) — подгруппа $\{na \,|\, a \in A\}$ (соответственно, $\{a \in A \,|\, na = 0\}$);

$A^1 = \bigcap_{n=1}^{\infty} nA$ — первая ульмовская подгруппа группы A;

$A^\bullet$ — ее копериодическая оболочка.

$H(a)$ — индикатор элемента a p-группы.

$\mathbb{H}(a)$ — высотная матрица элемента a.

$\chi_A(a)$ или $\chi(a)$ — характеристика элемента a в абелевой группе без кручения A.

$\mathbb{Q}\operatorname{End} A$ — кольцо (или алгебра) квазиэндоморфизмов группы без кручения A.

$\operatorname{Ext}(C, A)$, $\operatorname{Pext}(C, A)$ — группа расширений, соответственно, группа чистых расширений абелевой группы A при помощи абелевой группы C.

$\operatorname{Tor}(A, C)$ — периодическое произведение абелевых групп A и C.

$\operatorname{Mult} A$ — группа кольцевых умножений на абелевой группе A.

Если $f\colon A \to B$ — функция множества A в множество B и $a \in A$, то $f(a)$ или a^f обозначает образ элемента a при действии функции f, скобки иногда опускаются; $\operatorname{Im} f$ — образ функции f; если $C \subseteq A$, то $fC = C^f = \{fc \mid c \in C\}$, $f \mid C$ — ограничение f на C. R^A — кольцо всех функций из множества A в кольцо R. Если $g\colon B \to C$ — еще одна функция, то композиция функций f и g обозначается $g \circ f$, где $(g \circ f)(a) = g(f(a))$.

$A \Delta B = (A \setminus B) \cup (B \setminus A)$ — *симметрическая разность* множеств A и B.

Обозначения и термины, не столь часто используемые, даются по ходу изложения.

ГРЕЧЕСКИЙ АЛФАВИТ

A α	B β	Γ γ	Δ δ	E ε	Z ζ	H η	Θ θ
Альфа	*Бета*	*Гамма*	*Дельта*	*Эпсилон*	*Дзета*	*Эта*	*Тэта*
I ι	K κ	Λ λ	M μ	N ν	Ξ ξ	O o	Π π
Йота	*Каппа*	*Лямбда*	*Мю*	*Ню*	*Кси*	*Омикрон*	*Пи*
P ρ	Σ σ	T τ	Υ υ	Φ φ (или ϕ)	X χ	Ψ ψ	Ω ω
Ро	*Сигма*	*Тау*	*Ипсилон*	*Фи*	*Хи*	*Пси*	*Омега*

Глава I. Решетки и полугруппы

1 Решетки

Любое подмножество $R \subseteq M \times M$ называется *бинарным отношением* на множестве M. Если $a, b \in M$ и $(a, b) \in R$, то говорят, что *элемент a находится в отношении R к элементу b* и пишут aRb (вместо R пишут ρ или другие различные значки). *Правым смежным классом* Ra отношения R, определяемым элементом $a \in M$, называется множество всех таких $x \in M$, что xRa. Аналогично определяются *левые смежные классы* aR. *Дополнением* к бинарному отношению R называется бинарное отношение $-R$, определенное равенством: $-R = (M \times M) \setminus R$. Говорят также о включении, пересечении и объединении бинарных отношений, заданных на множестве M. *Произведением* $R \circ S$ бинарных отношений R и S называется бинарное отношение, определяемое следующим образом: $a(R \circ S)b$ в точности тогда, когда существует такой $c \in M$, что aRc и cSb. Для всякого бинарного отношения R на множестве M существует *обратное отношение* R^{-1}: $aR^{-1}b$ в точности тогда, когда bRa. Единичное отношение E определяется следующим образом: aEb в точности тогда, когда $a = b$.

Отношение R, заданное на множестве M, называется:

а) рефлексивным, если aRa для всех $a \in M$, т.е. $E \subseteq R$;

б) симметричным, если aRb влечет за собой bRa, т.е. $R^{-1} = R$;

в) транзитивным, если aRb и bRc влекут за собой aRc, т.е. $R \circ R \subseteq R$;

г) антисимметричным, если aRb и bRa влекут за собой $a = b$, т.е. $R \cap R^{-1} \subseteq E$.

Обобщением понятия бинарного отношения является n-арное отношение (при $n = 3$ — тернарное отношение), определяемое как подмножество множества $M^n = \underbrace{M \times \ldots \times M}_{n}$. Множества, в которых задано некоторое число таких отношений, называются *моделями* и являются предметом самостоятельной теории.

Бинарное отношение, обладающее свойствами рефлексивности, транзитивности и симметричности, называется *отношением эквивалентности*. Всякое разбиение множества M определяет в M отношение эквивалентности (под *разбиением* понимается такой выбор в M системы непустых подмножеств, классов этого разбиения, что всякий элемент из M принадлежит одному и только одному из этих подмножеств). Обратно, всякое отношение эквивалентности R, заданное на множестве M, определяет разбиение этого множества на совокупность смежных классов aR эквивалентности R (левые и правые смежные классы здесь совпадают), называемых также *классами эквивалентности* множества M по отношению R. Множество всех классов разбиения, соответствующего данному отношению эквивалентности R на множестве M, обозначается через M/R и называется *фактормножеством* множества M по отношению эквивалентности R. Отображение $a \mapsto aR$, $a \in M$, называется *каноническим отображением* множества M на M/R.

Бинарное отношение, обладающее свойствами рефлексивности, транзитивности и антисимметричности, называется *отношением частичного порядка*. Множество M в этом случае называется *частично упорядоченным*. Для записи частичного порядка употребляется символ $\leqslant$. Если $a \leqslant b$ и $a \neq b$, то пишут $a < b$. Если $a \leqslant b$ или $b \leqslant a$, то говорят, что элементы a и b *сравнимы*. Частично упорядоченное множество, в котором любые два элемента сравнимы, называется *линейно упорядоченным* множеством или *цепью*. Всякая частичная упорядоченность данного множества M может быть продолжена до линейной упорядоченности этого множества. Подмножество H частично упорядоченного множества M называется *выпуклым*, если для любых $a,\ b \in H$ из условия $a \leqslant x \leqslant b$, где $x \in M$, следует, что $x \in H$.

Остановимся на явлении двойственности для частично упорядоченных множеств. Пусть $(M, \leqslant)$ — частично упорядоченное множество M с порядком $\leqslant$. Введем еще одно бинарное отношение $\geqslant$ на M, полагая, что $a \geqslant b$ имеет место в точности тогда, когда $b \leqslant a$. Несложно убедиться, что $\geqslant$ — частичный порядок на M. Соответствующее частично упорядоченное множество $(M, \geqslant)$ называется *двойственным* к частично упорядоченному множеству $(M, \leqslant)$, а порядок $\geqslant$ — *обратным* к исходному порядку $\leqslant$. Всякое понятие или утверждение, относящееся к частичной упорядоченности, имеет двойственный аналог. Конкретизируем это высказывание. Пусть мы располагаем некоторым понятием или утверждением Ξ о частично упорядоченных множествах. Заменив в описании этого понятия или формулировке утверждения $\leqslant$ на $\geqslant$, получим новое понятие или утверждение о частично упорядоченных множествах, называемое *двойственным* к Ξ. Справедлив следующий

Принцип двойственности. Если истинно утверждение Ξ во всех частично упорядоченных множествах, то двойственное ему утверждение также истинно во всех частично упорядоченных множествах.

Принцип двойственности, не принося глубоких результатов, сокращает для нас количество работы.

Отображение $f\colon M \to M'$ частично упорядоченных множеств называется *изотонным* (*монотонным*), если для любых $a, b \in M$ из $a \leqslant b$ следует, что $fa \leqslant fb$ (термин «порядковый гомоморфизм» в данной книге используется, в основном, для упорядоченных групп). Биекция $f\colon M \to M'$ частично упорядоченных множеств называется *изоморфизмом*, если f и f^{-1} — изотонные отображения; это эквивалентно тому, что для любых $a, b \in M$ неравенство $a \leqslant b$ имеет место если и только если $fa \leqslant fb$. Всякое частично упорядоченное множество M изоморфно вкладывается в множество 2^N всех подмножеств некоторого множества N, частично упорядоченное относительно теоретико-множественного включения; говорят кратко «порядок по включению». В качестве N можно взять само M. Частично упорядоченные множества M и M' называются *антиизоморфными* (*двойственно изоморфными* или *дуально изоморфными*), если одно из них изоморфно другому, взятому с обратной частичной упорядоченностью, т.е. существует биекция $f\colon M \to M'$ такая, что $a \leqslant b$, где $a, b \in M$, если и только если $fb \leqslant fa$.

Прямым произведением AB двух частично упорядоченных множеств A и B называется множество $A \times B$, частично упорядоченное по правилу: $(a, b) \leqslant (a_1, b_1)$ $(a, a_1 \in A; b, b_1 \in B)$ тогда и только тогда, когда $a \leqslant a_1$ в A и $b \leqslant b_1$ в B.

Элемент a частично упорядоченного множества M называется *минимальным* элементом этого множества, если в M нет элемента x, удовлетворяющего условию $x < a$. Если же $a \leqslant x$ для всех $x \in M$, то a называется *наименьшим* элементом множества M.

Теорема 1.1. *Следующие три условия на частично упорядоченное множество M эквивалентны.*

1) (Условие минимальности). *Всякое непустое подмножество $N \subseteq M$ обладает хотя бы одним минимальным (в N) элементом.*

2) (Условие обрыва убывающих цепей). *Для всякой убывающей цепи элементов $a_1 \geqslant a_2 \geqslant \dots$ существует такой индекс n, на котором эта цепь стабилизируется, т.е. $a_n = a_{n+1} = \dots$.*

3) (Условие индуктивности). *Все элементы частично упорядоченного множества M обладают некоторым свойством $\mathcal{E}$, если этим свойством обладают все минимальные элементы этого множества (в случае, когда они существуют) и если из справедливости свойства $\mathcal{E}$ для всех элементов, строго предшествующих некоторому элементу a, может быть выведена справедливость этого свойства для самого элемента a.*

Линейно упорядоченное множество, удовлетворяющее условию минимальности (значит, и двум другим условиям из теоремы 1.1), называется *вполне упорядоченным*.

Минимальные элементы частично упорядоченного множества M относительно обратной упорядоченности называются *максимальными* элементами множества M в его исходной упорядоченности, а убывающие цепи в обратной упорядоченности называются *возрастающими цепями* множества M. Двойственным понятием к наименьшему элементу является понятие *наибольшего* элемента. Наибольший и наименьший элементы частично упорядоченного множества называются его *единицей* и *нулем* соответственно (если таковые существуют).

Если N — подмножество частично упорядоченного множества M, то всякий элемент $a \in M$ (не обязательно $a \in N$), удовлетворяющий условию $a \geqslant x$ для всех $x \in N$, называется *верхней гранью* подмножества N в множестве M. Двойственным является понятие *нижней грани*. *Точной верхней* (*нижней*) гранью подмножества N в M называется наименьшая верхняя (наибольшая нижняя) грань для N, обозначаемая через $\sup_M N$ ($\inf_M N$), индекс M обычно опускается. *Верхним конусом* $N^{\triangle}$ множества N называется множество всех таких элементов $x \in M$, что $x \geqslant a$ для всех $a \in N$. Двойственным образом определяется *нижний конус* N^{∇}.

Множество всех цепей частично упорядоченного множества M само является частично упорядоченным при помощи теоретико-множественного включения. Максимальные элементы этого последнего множества (если они существуют) называются *максимальными цепями* множества M.

Теорема 1.2. *Следующие утверждения эквивалентны.*

1) (Аксиома выбора). *Для всякого множества M существует такая функция $\varphi\colon 2^M \to M$, что $\varphi(A) \in A$ при любом $\varnothing \neq A \subseteq M$.*

2) (Теорема Цермело). *Всякое множество можно вполне упорядочить.*

3) (Теорема Хаусдорфа). *Всякая цепь частично упорядоченного множества содержится в некоторой максимальной цепи.*

4) (Теорема Куратовского-Цорна). *Если всякая цепь частично упорядоченного множества M обладает верхней гранью, то каждый элемент множества M сравним с некоторым максимальным элементом.*

Утверждение, что всякое множество может быть линейно упорядочено, является более слабым, чем аксиома выбора.

Частично упорядоченное множество M называется *верхней* (соответственно, *нижней*) *полурешеткой*, если в нем любое двухэлементное подмножество $\{a, b\}$ имеет точную верхнюю (соответственно, нижнюю) грань, обозначаемую через $a + b$ (соответственно, ab). Если в M для любых $a, b \in M$ существуют как $a + b$, так и ab, то M называется *решеткой*.

«$+$» и «$\cdot$» являются бинарными операциями на M, называемыми, соответственно, *сложением* или *объединением* и *умножением* или *пересечением*. Вместо «$+$» и «$\cdot$» часто употребляют знаки «$\vee$» и «$\wedge$». Понятие решетки допускает определение без использования частичной упорядоченности, а лишь при помощи свойств решеточных операций $+$

и $\cdot$ (см. 1.2, 1.3). Это позволяет трактовать решетки как алгебраические системы с двумя бинарными операциями.

Если частично упорядоченное множество $(L, \leqslant)$ является решеткой, то двойственное ему частично упорядоченное множество $(L, \geqslant)$ — тоже решетка. К решеткам применим принцип двойственности, для которых он принимает следующую форму.

Пусть Ξ — утверждение о решетках, записанное в терминах операций $+$ и $\cdot$, а также символов $\leqslant$ и, возможно, 0 и 1. Образуем утверждение, двойственное Ξ, заменяя друг на друга $+$ и $\cdot$, 0 и 1 и меняя $\leqslant$ на $\geqslant$. Если Ξ истинно во всех решетках, то двойственное ему утверждение также истинно во всех решетках.

Подмножества любого множества составляют решетку с частичной упорядоченностью по включению. Можно говорить о решетке подгрупп и решетке нормальных подгрупп некоторой группы G. Порядок подразумевается по включению, а произведением (решеточным) подгрупп A и B является их теоретико-множественное пересечение $A \cap B$, а роль суммы (решеточной) играет подгруппа $\langle A, B\rangle$, порожденная этими подгруппами, т.е. наименьшая подгруппа, содержащая как A, так и B. Похожим способом вводится решетка подколец, решетка идеалов, решетка левых (правых) идеалов некоторого кольца R, решетка подмодулей некоторого модуля M.

Решетка M называется *полной*, если всякое ее непустое подмножество N имеет $\sup N$ и $\inf N$.

Решетка M называется *дедекиндовой* (или *модулярной*), если для любых $a, b, c \in M$, где $a \leqslant c$, справедлив *модулярный* закон $(a + b)c = a + bc$. Дедекиндовыми являются решетки нормальных подгрупп произвольной группы, идеалов кольца, подмодулей модуля. Напротив, решетка всех подгрупп не обязана быть дедекиндовой.

Решетка M называется *дистрибутивной*, если для любых $a, b, c \in M$ имеет место $(a + b)c = ac + bc$. Важнейшим примером дистрибутивной решетки является решетка всех подмножеств произвольного множества. Однако дедекиндова решетка всех подпространств векторного пространства уже не является дистрибутивной.

Теорема 1.3. *Всякая дистрибутивная решетка изоморфна решетке подмножеств (не обязательно всех) некоторого множества.*

Непустое подмножество I решетки M называется *идеалом*, если для любых $a, b \in I$ следует, что $a+b \in I$ и $x \in I$ для всех $x \leqslant a$. Если $I \neq M$, то идеал I называется *собственным*. Двойственным образом вводится понятие *коидеала* (также называемого *фильтром*). Для любого $a \in M$ множество $(a]$ всех таких элементов $b \in M$, что $b \leqslant a$ (т.е. $(a] = a^{\nabla}$), будет идеалом; это *главный идеал*, порожденный элементом a.

Собственный идеал P называется *простым*, если $ab \in P$ влечет $a \in P$ или $b \in P$. Собственный коидеал F называется *простым*, если $a + b \in F$ влечет $a \in F$ или $b \in F$. Собственные идеалы решетки образуют упорядоченное множество относительно включения. Максимальные элементы этого упорядоченного множества называются *максимальными* идеалами решетки. Непустое пересечение идеалов снова является идеалом решетки. Поэтому для всякого подмножества H решетки существует наименьший идеал, содержащий H, он называется идеалом, *порожденным* подмножеством H. Идеалы решетки также образуют решетку.

Непустое подмножество P решетки называется *подрешеткой*, если $a+b, ab \in P$ для любых $a, b \in P$. Стоит отметить, что решетка подгрупп группы G не будет подрешеткой в решетке подмножеств множества G, так как сложения в этих двух решетках имеют разный смысл. Так же обстоит дело и с решетками подколец, идеалов, подмодулей.

Отображение φ решетки M в решетку L называется *гомоморфизмом*, если $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для всех $a, b \in M$. Гомоморфизм $\varphi\colon M \to L$ решеток, являющийся биекцией, называется *изоморфизмом* (это эквивалентно тому, что φ — изоморфизм частично упорядоченных множеств M и L).

Решетка называется *самодвойственной*, если она антиизоморфна себе.

Эквивалентность $\equiv$, определенная на решетке, называется *конгруэнцией*, если $a \equiv c$ и $b \equiv d$ влечет $a + b \equiv c + d$ и $ab \equiv cd$.

Теорема 1.4. *Если всякое изотонное отображение φ решетки L в себя имеет неподвижную точку (т.е. $\varphi(a) = a$ для некоторого $a \in L$), то L полна.*

Если a, b — элементы частично упорядоченного множества M, причем $a \leqslant b$, то множество $[a, b] = \{x \in M \mid a \leqslant x \leqslant b\}$ называется *интервалом*. Если $[a, b] = \{a, b\}$, то этот интервал называется *простым*. Элемент a частично упорядоченного множества M с 0 называется *атомом*, если интервал $[0, a]$ прост, т.е. a — минимальный элемент в множестве всех ненулевых элементов множества M.

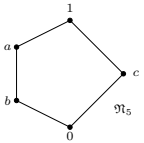
Конечные частично упорядоченные множества удобно иллюстрировать диаграммами, на которых элементы изображаются в виде точек по правилу: если $a < b$, то точка, соответствующая элементу b, расположена выше точки, соответствующей элементу a, причем, если интервал $[a, b]$ прост, то соответствующие точки соединяются отрезком прямой.

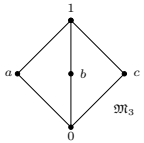
Решетка M называется *решеткой с относительными дополнениями*, если для всякого элемента c из любого интервала $[a, b]$ найдется такой элемент d, что $c + d = b$ и $cd = a$. Этот элемент d называется *дополнением элемента c в интервале* $[a, b]$. Дополнение, в общем случае, определено не однозначно. Решетка с 0 и 1 называется *решеткой с дополнениями*, если каждый ее элемент имеет дополнения в интервале $[0, 1]$, которые в этом случае называются просто *дополнениями*. Любая решетка с относительными дополнениями, имеющая 0 и 1, обладает дополнениями.

Обратное, как показывает, например, решетка $\mathfrak{N}_5$ (см. ниже), вообще говоря, не верно.

Дистрибутивная решетка с дополнениями называется *булевой алгеброй*. В булевой алгебре каждый ее элемент a обладает в точности одним дополнением a' (упр. 1.35). Доказано, что существуют недистрибутивные решетки с единственными дополнениями.

Примерами недистрибутивных решеток являются решетки $\mathfrak{N}_5$ и $\mathfrak{M}_3$.





Решетка называется *пентагоном* или *диамантом*, если она изоморфна $\mathfrak{N}_5$ или $\mathfrak{M}_3$ соответственно.

Теорема 1.5. *Решетка дедекиндова (дистрибутивна) тогда и только тогда, когда она не содержит пентагонов (пентагонов и диамантов).*

Цепь $a_0 < a_1 < \ldots < a_n$, принадлежащая частично упорядоченному множеству с 0 и 1, называется *композиционным рядом*, если $a_0 = 0$, $a_n = 1$ и все интервалы $[a_{i-1}, a_i]$ $(i = 1, \ldots, n)$ простые. Число n называется *длиной* композиционного ряда.

Теорема 1.6. *Все композиционные ряды дедекиндовой решетки имеют одинаковую длину.*

Теорема 1.6 находит применения в теории колец, модулей и групп. Элементы $a_1, \ldots, a_n$ дедекиндовой решетки с нулем 0 называются *независимыми*, если $(a_1 + \ldots + a_{i-1} + a_{i+1} + \ldots + a_n)a_i = 0$ для всех $i = 1, \ldots, n$. Сумму независимых элементов $a_1, \ldots, a_n$ называют *прямой* и обозначают через $a_1 \oplus \ldots \oplus a_n$.

Ненулевой элемент a дедекиндовой решетки с 0 и 1 называется *неразложимым*, если он не может быть представлен в виде $a = b \oplus c$, где $b, c \neq 0$.

Теорема 1.7. *Если дедекиндова решетка обладает композиционным рядом, то всякий ее ненулевой элемент представим в виде конечной прямой суммы неразложимых элементов. Кроме того, если* $1 = a_1 \oplus \ldots \oplus a_m = b_1 \oplus \ldots \oplus b_k$, *где* $a_1, \ldots, a_m, b_1, \ldots, b_k$ *— неразложимые элементы, то* $m = k$ *и для всякого* a_i *найдется такой элемент* b_j, *что* $1 = a_1 \oplus \ldots \oplus a_{i-1} \oplus b_j \oplus a_{i+1} \oplus \ldots \oplus a_m$.

Теорема 1.7 в применении к решетке подпространств конечномерного векторного пространства дает известную *теорему о замене* для двух эквивалентных систем линейно независимых векторов. Из последней вытекает, что все базисы содержат одно и то же число векторов.

Элемент a решетки называется *$\cap$-неразложимым*, если $a = bc$ влечет $a = b$ или $a = c$. Представление элемента a в виде $a = a_1 \ldots a_n$ называется *несократимым $\cap$-представлением*, если элементы $a_1, \ldots, a_n$ $\cap$-неразложимы и $a_1 \ldots a_{i-1} a_{i+1} \ldots a_n \not\leqslant a_i$ для всех $i = 1, \ldots, n$.

Теорема 1.8. *Если* $a = a_1 \ldots a_m = b_1 \ldots b_n$ *— два несократимых $\cap$-представления элемента a дедекиндовой решетки, то* $m = n$ *и для всякого* a_i *найдется такой элемент* b_j, *что* $a = a_1 \ldots a_{i-1} b_j a_{i+1} \ldots a_m$.

Теорема 1.9. *Для дедекиндовой решетки L с композиционным рядом эквивалентны следующие свойства:*

а) *L — решетка с дополнениями;*

б) *каждый элемент из L представим в виде прямой суммы атомов;*

в) *1 представима в виде прямой суммы атомов.*

Задачи

1.1. Решеточные операции обладают следующими свойствами:

а) $a + a = a$, $aa = a$;

б) $a + b = b + a$, $ab = ba$;

в) $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$;

г) $a(a + b) = a$, $a + ab = a$.

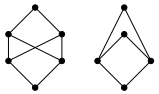
1.2. В решетке L следующие свойства эквивалентны:

а) $a \leqslant b$; б) $a + b = b$; в) $ab = a$.

В частности, для нуля и единицы (если они существуют) справедливы равенства $a \cdot 0 = 0$, $a + 0 = a$, $a \cdot 1 = a$ и $a + 1 = 1$ для всех $a \in L$.

1.3. Пусть L — множество с бинарными операциями $+$ и $\cdot$, обладающими свойствами б) – г) из 1.1. Положим $a \leqslant b$ в точности тогда, когда $a + b = b$. Отношение $\leqslant$ является частичным порядком на L, при этом L — решетка, $a + b = \sup\{a, b\}$ и $ab = \inf\{a, b\}$.

1.4. Почему следующие диаграммы частично упорядоченных множеств не являются решетками?



1.5. Всякий решеточный гомоморфизм является изотонным отображением. Обратное неверно.

1.6. Найдите все изотонные отображения и все решеточные гомоморфизмы из четырехэлементной решетки (рис. 1) в трехэлементную цепь (рис. 2).

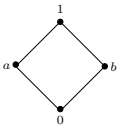


рис. 1

рис. 2

1.7. 1) Существует ровно два неизоморфных двухэлементных частично упорядоченных множества.

2) Существует в точности пять неизоморфных трехэлементных частично упорядоченных множеств, три из которых самодвойственны.

1.8. 1) Имеется только пять неизоморфных решеток, содержащих менее пяти элементов.

2) Имеется в точности пять неизоморфных пятиэлементных решеток и три из них самодвойственны.

1.9. Нарисуйте диаграммы всех решеток из 1.8 1) и 1.8 2).

1.10. В решетке, если $a \leqslant c$ и $b \leqslant d$, то $a + b \leqslant c + d$ и $ab \leqslant cd$.

1.11. Подрешетка I решетки L является идеалом тогда и только тогда, когда если $a \in I$ и $b \in L$, то $ab \in I$.

1.12. Если φ — изоморфизм частично упорядоченного множества L на частично упорядоченное множество M и L — решетка, то M также решетка и φ является изоморфизмом решеток.

1.13. Следующие свойства решетки L эквивалентны:

а) L — цепь;

б) все непустые подмножества множества L являются подрешетками;

в) всякое изотонное отображение частично упорядоченного множества L в решетку M является решеточным гомоморфизмом;

г) $a = bc$ влечет $a = b$ или $a = c$.

1.14. Решетка тогда и только тогда полна, когда в ней есть наибольший элемент и любое ее непустое подмножество имеет точную нижнюю грань.

1.15. 1) Конечное частично упорядоченное множество с 0 и 1 имеет композиционный ряд.

2) Постройте бесконечное частично упорядоченное множество, имеющее композиционный ряд.

3) Прямое произведение двух решеток является решеткой.

1.16. Интервал $[a, b]$ полной решетки L является полной решеткой, причем $\sup_{[a,b]} A = \sup_L A$ и $\inf_{[a,b]} A = \inf_L A$ для всякого непустого подмножества $A \subseteq [a, b]$.

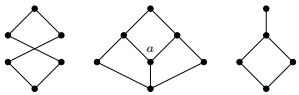
1.17. Если φ — изотонное отображение полной решетки L в себя, то $\varphi a = a$ для некоторого $a \in L$. Кроме того, множество неподвижных точек содержит наименьший элемент.

1.18. Приведите пример частично упорядоченного множества, не являющегося полной решеткой, все изотонные отображения которого в себя имеют неподвижную точку.

1.19. Если решетка удовлетворяет условию максимальности, то все ее идеалы являются главными. Сформулировать двойственное утверждение.

1.20. $\mathfrak{N}_5$ является единственной недедекиндовой пятиэлементной решеткой.

1.21. Какие из элементов следующих решеток имеют дополнения? В каких из этих решетках элементы с дополнениями образуют подрешетку?



1.22. Каждый смежный класс конгруэнции на решетке является выпуклой подрешеткой.

1.23. Пусть $\equiv$ — конгруэнция на решетке L и $\overline{a}$ — смежный класс, определяемый элементом a. Положим $\overline{a} + \overline{b} = \overline{a+b}$ и $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Убедитесь, что операции определены корректно и обладают свойствами б) — г) из 1.1, т.е. факторможество $\overline{L} = L/\equiv$ является решеткой.

Решетка $\overline{L}$ называется *факторрешеткой* решетки L по конгруэнции $\equiv$. Отображение $a \mapsto \overline{a}$ является гомоморфизмом, называемым *каноническим.*

1.24. Пусть $\varphi\colon L \to P$ — решеточный гомоморфизм. Отношение: «aRb тогда и только тогда, когда $\varphi(a) = \varphi(b)$» является конгруэнцией, называемой *ядром гомоморфизма* φ.

1.25 (Теорема о гомоморфизме). Пусть φ — гомоморфизм решетки L на решетку M и R — ядро этого гомоморфизма. Тогда существует такой изоморфизм ψ решетки M на факторрешетку L/R, что $\psi(\varphi(a)) = \overline{a}$ для всех $a \in L$, где $\overline{a}$ — образ элемента a при каноническом гомоморфизме, определяемом конгруэнцией R.

1.26. Если конгруэнция R на решетке L такова, что факторрешетка L/R имеет нуль, то полный прообраз этого нуля является идеалом, называемым *ядерным идеалом* конгруэнции R (*ядерный коидеал* определяется двойственным образом). В отличие от групп, колец и модулей, не всякий идеал решетки является ядерным. Всякий же простой идеал служит ядерным идеалом некоторого решеточного гомоморфизма.

1.27. Подрешетка P решетки L является простым идеалом тогда и только тогда, когда $L \setminus P$ — простой коидеал.

1.28. Следующие свойства решетки L эквивалентны:

а) L дедекиндова;

б) $a(ab + c) = ab + ac$ для любых $a, b, c \in L$;

в) если $a \geqslant b$ и для некоторого $c \in L$ справедливо $a + c = b + c$ и $ac = bc$, то $a = b$.

1.29. Дедекиндовость решетки равносильна каждому из следующих свойств:

а) $a + b(a + c) = (a + b)(a + c)$;

б) $(a + bc)(b + c) = a(b + c) + bc$;

в) если $a \leqslant c$ и $d \leqslant b$, то $a + b(c + d) = (a + b)c + d$;

г) если $a \leqslant c \leqslant a + b$, то $a + bc = c$;

д) если $a \leqslant b \leqslant c + d$, $ac = bc$ и $(a + c)d = (b + c)d$, то $a = b$.

1.30. 1) Если в дедекиндовой решетке $(a + b)c = 0$, то $a(b + c) = ab$.

2) В дедекиндовой решетке справедливо равенство $(ab+ac)(ab+bc) = ab$, а из $(a+b)c = bc$ вытекает, что $a(b+c) = ab$.

3) Дедекиндова решетка с дополнениями является решеткой с относительными дополнениями.

1.31. Если a, b — элементы дедекиндовой решетки, то отображения $\varphi(x) = x + b$ $(ab \leqslant x \leqslant a)$ и $\psi(y) = ay$ $(b \leqslant y \leqslant a + b)$ осуществляют изоморфизм интервалов $[ab, a]$ и $[b, a + b]$.

1.32. Если $a_1, \ldots, a_n, b_1, \ldots, b_n$ — элементы дедекиндовой решетки и $a_i \leqslant b_j$ при $i \neq j$, то $(a_1 + \ldots + a_n)b_1 \cdot \ldots \cdot b_n = a_1b_1 + \ldots + a_nb_n$.

1.33. Дедекиндовость (дистрибутивность) решетки равносильна дедекиндовости (дистрибутивности) решетки ее идеалов.

1.34. Следующие свойства решетки L эквивалентны:

а) L дистрибутивна;

б) $ab + c = (a + c)(b + c)$ для любых $a, b, c \in L$;

в) $ab + bc + ca = (a + b)(b + c)(c + a)$ для любых $a, b, c \in L$;

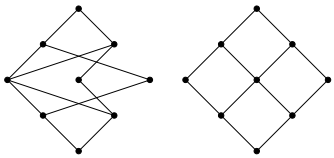
г) если для некоторого $c \in L$ справедливо $a + c = b + c$ и $ac = bc$, то $a = b$.

1.35. В дистрибутивной решетке каждый элемент может иметь не более одного дополнения. В частности, в булевой алгебре каждый элемент обладает единственным дополнением.

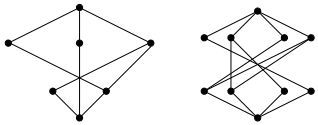
1.36. Дистрибутивная решетка, обладающая композиционным рядом, конечна.

1.37. Решетки $(2^M, \cap, \cup)$, (ℕ, нод, нок) и все цепи дистрибутивны.

1.38. Убедитесь, что следующие две диаграммы изображают одну и ту же решетку.



1.39. Упростите диаграммы на следующих рисунках.



1.40. В дистрибутивной решетке каждый максимальный идеал прост, а произвольный идеал совпадает с пересечением всех содержащих его простых идеалов.

1.41. Нарисуйте диаграмму булевой алгебры всех подмножеств трехэлементного множества $A = \{1, 2, 3\}$.

1.42. В булевой алгебре справедливы соотношения: $(a + b)' = a'b'$, $(ab)' = a' + b'$, $a'' = a$, $0' = 1$, $1' = 0$; если $a \leqslant b$, то $b' \leqslant a'$.

1.43. В булевой алгебре равносильны утверждения: а) $a \leqslant b$; б) $ab' = 0$; в) $a' + b = 1$.

1.44. Если в решетке L с 0 и 1 каждый элемент a обладает единственным дополнением a', причем $(a + b)' = a'b'$ и $(ab)' = a' + b'$, то L — булева алгебра.

1.45. Совокупность элементов дистрибутивной решетки, обладающих дополнениями, образует решетку, являющуюся булевой алгеброй.

1.46. Дедекиндова решетка с единствеными дополнениями является булевой алгеброй.

1.47. Каждая дистрибутивная решетка является подрешеткой некоторой булевой алгебры.

1.48. Если φ — гомоморфизм булевой алгебры B на булеву алгебру, то $\varphi(b') = (\varphi(b))'$ для всех $b \in B$.

1.49. Дистрибутивная решетка является булевой алгеброй тогда и только тогда, когда каждый ее простой идеал максимален.

1.50. Решетка $\mathfrak{M}_3$ изоморфна решетке всех подгрупп четверной группы Клейна V_4, т.е. группы $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

1.51. Постройте диаграммы решеток всех подгрупп следующих групп: $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, симметрической группы S_3, группы диэдра D_4.

1.52. Пусть R — кольцо всех линейных операторов конечномерного векторного пространства V над некоторым полем. Решетка всех подпространств пространства V изоморфна решетке всех правых идеалов кольца R и антиизоморфна решетке всех его левых идеалов.

1.53. Решетка всех правых идеалов кольца матриц порядка n ($n > 1$) над некоторым полем как изоморфна, так и антиизоморфна решетке всех левых идеалов этого кольца. Обе эти решетки и все решетки из предыдущего упражнения самодвойственны.

1.54. Пусть V и W — конечномерные векторные пространства над одним полем. Если решетки всех подпространств этих пространств изоморфны, то пространства V и W имеют одинаковую размерность и, значит, они изоморфны.

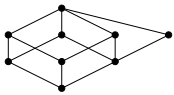
Длина конечной цепи из n элементов по определению полагается равной $n - 1$. *Длиной* частично упорядоченного множества M называется точная верхняя грань длин цепей в M; если она конечна, то говорят, что M имеет *конечную длину*.

1.55. В дедекиндовой решетке:

а) если $a \neq b$ и для некоторого элемента c интервалы $[c, a]$, $[c, b]$ простые, то просты интервалы $[a, a + b]$, $[b, a + b]$;

б) если $a \neq b$ и для некоторого элемента c интервалы $[a, c]$, $[b, c]$ простые, то просты интервалы $[ab, a]$, $[ab, b]$.

Доказано, что в решетке конечной длины условия а) и б) необходимы и достаточны для дедекиндовости. Как показывает следующая диаграмма, решетка с дополнениями и удовлетворяющая свойству а) не обязана обладать относительными дополнениями (ср. с 1.30 3)).



2 Полугруппы

Пусть G — произвольное множество. Всякое отображение $f\colon G \times G \to G$ называется *бинарной алгебраической операцией*, определенной на множестве G. Вместо f часто пишут $\cdot$, $+$, $*$, $\circ$ или другой символ. Множество G с заданной на нем бинарной операцией называется *группоидом*.

Пусть $(G, \cdot)$ — группоид. Операция $\cdot$ называется *коммутативной*, если $a \cdot b = b \cdot a$ для любых $a, b \in G$; *ассоциативной*, если $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых $a, b, c \in G$. Если операция $\cdot$ фиксирована, то элемент $a \cdot b$ часто обозначается через ab.

Говорят, что в группоиде выполняется *левый* (*правый*) *закон сокращения*, если для любых его элементов равенство $ab = ac$ ($ba = ca$) влечет $b = c$. Группоид с левым и правым сокращением называется *группоидом с сокращением*. Непустое подмножество A группоида G называется его *подгруппоидом*, если из $a, b \in A$ следует, что $ab \in A$.

Если в группоиде $(G, \cdot)$ существует такой элемент e, что $ex = xe = x$ для любого $x \in G$, то e называется *нейтральным элементом* или *единицей* группоида. Единицу группоида часто обозначают цифрой 1. Если $e_\ell x = x$ ($xe_r = x$) для любого $x \in G$, то e_ℓ (e_r) называется *левой* (*правой*) *единицей* группоида G.

Группоид с ассоциативной операцией называется *полугруппой*. Полугруппа с нейтральным элементом называется *моноидом*.

Пусть $(G, \cdot)$ — группоид. Элемент $a_r \in G$ ($a_\ell \in G$) называется *правым обратным* (*левым обратным*) для $a \in G$, если $a \cdot a_r = e_r$ ($a_\ell \cdot a = e_\ell$), где e_r — правая (e_ℓ — левая) единица группоида G. Элемент $b \in G$ называется *обратным* (*симметричным, противоположным*) для $a \in G$, если $ab = ba = e$; в этом случае a называется *обратимым* элементом.

Моноид, все элементы которого обратимы, называется *группой*.

Число элементов конечной полугруппы называется ее *порядком*. Число всех попарно неизоморфных полугрупп данного порядка n с увеличением n растет довольно быстро. Представление об этом росте дает следующая таблица

Порядок полугруппы	1	2	3	4	5	6
Число неизоморфных полугрупп данного порядка	1	5	24	188	1915	28634
Из них группы	1	1	1	2	1	2

Элемент z группоида G называется *левым* (*правым*) *нулем*, если $za = z$ ($az = z$) для любого $a \in G$, z называется *нулем*, если z — и левый, и правый нуль.

Элемент a группоида называется *идемпотентом*, если $a^2 = a$.

Элемент a полугруппы S называется *регулярным* (по фон Нейману), если $a = axa$ для некоторого $x \in S$.

Говорят, что полугруппа S *антикоммутативна*, если $ab = ba$ ($a, b \in S$) влечет за собой $a = b$.

Полугруппу G с нулем 0 называют *полугруппой с нулевым умножением*, если $ab = 0$ для всех $a, b \in G$.

Непустое подмножество A группоида G называется его *подгруппоидом*, если $ab \in A$ для любых $a, b \in A$. Если G полугруппа, то любой ее подгруппоид также является полугруппой, которая называется *подполугруппой* полугруппы G.

Подгруппой полугруппы G называют ее подполугруппу, являющуюся группой относительно бинарной операции, определенной в G.

Если A и B — подмножества группоида G, то их *произведением* AB называется следующее множество элементов: $AB = \{\, ab \,|\, a \in A,\ b \in B\}$. Если $A = \{a\}$ ($B = \{b\}$), то иногда пишут aB (Ab) вместо AB.

Если G — группоид, то пересечение любого семейства его подгруппоидов либо пусто, либо является подгруппоидом. Поэтому для каждого непустого подмножества $M \subseteq G$ существует наименьший подгруппоид $\langle M \rangle$, содержащий M. Он называется *подгруппоидом, порожденным подмножеством* M.

Порядком элемента a полугруппы G называется порядок (мощность) подполугруппы $\langle a\rangle$, порожденной элементом a.

Полугруппа называется *моногенной* или *циклической*, если она состоит из положительных степеней одного из своих элементов (такой элемент является ее порождающим).

Левым (*правым*) *идеалом* группоида G называется такое его непустое подмножество A, что $GA \subseteq A$ ($AG \subseteq A$). *Двусторонним идеалом* или просто *идеалом* группоида называется его подмножество, являющееся левым и правым идеалом.

Группоид S называется *простым слева* (*справа*), если S является его единственным левым (правым) идеалом. Группоид S называется *простым,* если S не содержит (двусторонних) идеалов, отличных от S.

Если A — непустое подмножество в группоиде S, то пересечение всех левых идеалов, содержащих A, является наименьшим левым идеалом, содержащим A (он называется *левым идеалом группоида* S, *порожденным подмножеством* A).

Отображение $f\colon (A,\ \cdot) \to (G,\ *)$ группоида A в группоид G называется *гомоморфизмом*, если $f(a \cdot b) = f(a) * f(b)$ для любых $a,\ b \in A$. Биективный гомоморфизм называется *изоморфизмом*. Гомоморфизм (изоморфизм) группоида в себя называется его *эндоморфизмом* (*автоморфизмом*).

Пусть X — непустое множество. Множество $F(X)$ всех отображений $X \to X$ относительно операции композиции образует полугруппу, называемую *симметрической полугруппой* или *полной полугруппой преобразований на* X. Множество $S(X)$ биекций $X \to X$ образует подгруппу в $F(X)$. Группу $S(X)$ называют *симметрической группой* или *группой биекций на* X.

Задачи

2.1. Условия ассоциативности и коммутативности для группоида независимы.

2.2. Если группоид содержит левую единицу и правую единицу, то они совпадают. Аналогичное утверждение справедливо и для нулей. Приведите примеры группоидов с единицей (с нулем), имеющих подгруппоиды, не содержащие единицу (нуля).

2.3. Будет ли $*$ бинарной алгебраической операцией для указанных множеств:

а) $\mathbb{N}$, $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, где $a * b = |a - b|$;

б) $\mathbb{N}$, $\mathbb{Z} \setminus \{0\}$, где $a * b = a^b$;

в) $\mathbb{N}$, где $a * b = [a, b]$; г) $\mathbb{N}$, где $a * b = 25$;

д) $\mathbb{N}$, где $a * b = \{$множество всех общих кратных чисел a и $b\}$;

е) $\mathbb{N}$, $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, где $a * b = \dfrac{a+b}{2}$?

2.4. Являются ли сложение и умножение матриц бинарными алгебраическими операциями на множествах:

а) $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$; б) $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{R} \right\}$;

в) $\left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \,\middle|\, a \in \mathbb{R} \setminus \{0\} \right\}$; г) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$?

В случае положительного ответа найдите левые и правые единицы и элементы, обратимые слева или справа относительно этих единиц (если они существуют).

2.5. Среди приведенных ниже группоидов выделите коммутативные группоиды, группоиды с сокращениями и полугруппы. Укажите нейтральные элементы и взаимно обратные элементы (если они существуют).

а) $(\mathbb{N}, *)$, где $a * b = a^b$;

б) $(\mathbb{N}_0, *)$, $(\mathbb{Z}, *)$, $(2\mathbb{Z}, *)$, $(\mathbb{Q}, *)$, где $a * b = |a - b|$;

в) $(\mathbb{N}, *)$, $(\mathbb{Z}, *)$, $(2\mathbb{Z}, *)$, $(\mathbb{Q}, *)$, где $a * b = (a + b)^2$;

г) $(\mathbb{N}, *)$, где $a * b = a$; д) $(\mathbb{Q}, *)$, где $a * b = a + b - ab$;

е) $(\mathbb{Q}, *)$, где $a * b = \dfrac{a+b}{2}$; ж) $(\mathbb{Z}, *)$, где $a * b = a^2 b$;

з) $(\mathbb{Z}, -)$; и) $(\mathbb{N}, *)$, где $a * b = [a, b]$;

к) $(\mathbb{N}, *)$, где $a * b = (a, b)$; л) $(\mathbb{R}, *)$, где $a * b = a + b + a^2b^2$;

м) $(2^M, \cap)$, $(2^M, \cup)$; н) $(\mathbb{R} \setminus \{-1\}, *)$, где $a * b = a + b + ab$.

2.6. Пусть $(G, \cdot)$ — группоид, c — фиксированный его элемент и ${}_cf(x) = c \cdot x$. В G справедлив левый закон сокращения тогда и только тогда, когда отображение ${}_cf$ инъективно.

2.7. Приведите пример группоида, в котором не выполнен закон сокращения.

2.8. Существуют моноиды, в которых каждый элемент обладает обратным элементом и подгруппоиды которых уже не обладают этим свойством.

2.9. Пусть G — группоид и A, B — его подгруппоиды. Являются ли $A \cap B$ и $A \cup B$ подгруппоидами в G?

2.10. Операция Δ коммутативна, ассоциативна и наделяет множество 2^M групповой структурой для любого множества M, причем операция $\cap$ дистрибутивна относительно Δ.

2.11. Множество матриц $M^0(n, \mathbb{R}) = \left\{ A = (\alpha_{ij}) \,\middle|\, \sum\limits_{j=1}^{n} \alpha_{ij} = 0;\ i = 1, \ldots, n \right\}$ образует полугруппу относительно операции умножения матриц. Является ли $M^0(n, \mathbb{R})$ моноидом?

2.12. Покажите, что $(\mathbb{Z}, \circ)$, где $n \circ m = n + m + nm$, является коммутативным моноидом. Что служит в $(\mathbb{Z}, \circ)$ нейтральным элементом? Найдите в $(\mathbb{Z}, \circ)$ все обратимые элементы.

2.13. На множестве M задана операция по правилу: $a * b = b$. Является ли $(M, *)$ полугруппой, существует ли в $(M, *)$ единичный элемент, существует ли для каждого элемента из $(M, *)$ правый обратный элемент?

Полугруппа из упр. 2.13 называется *полугруппой правых нулей*. Каждый элемент из $(M, *)$ является правым нулем и левой единицей одновременно. *Полугруппа левых нулей* $(M, \circ)$ определяется двойственным образом: $a \circ b = a$ для всех $a, b \in M$. Исследуйте $(M, \circ)$.

2.14. В моноиде $(M, \cdot)$ фиксируется произвольный элемент x и вводится новая операция $*$ по правилу: $a * b = axb$. Покажите, что $(M, *)$ есть полугруппа, являющаяся моноидом тогда и только тогда, когда x — обратимый элемент в $(M, \cdot)$.

2.15. Пусть f — гомоморфизм группоида G. Если группоид G коммутативен (полугруппа), то группоид $f(G)$ также коммутативен (полугруппа). Если e — нейтральный элемент группоида G, то $f(e)$ — нейтральный элемент группоида $f(G)$. Если элемент b — обратный к элементу a, то $f(b)$ — обратный к $f(a)$. Приведите примеры группоидов с сокращениями, гомоморфные образы которых не обладают этими свойствами.

2.16. Изоморфны ли полугруппы:

а) $(\mathbb{Z}_n, +)$ и $(\mathbb{Z}_n, \cdot)$; б) $(\mathbb{R}, \cdot)$ и $(M(2, \mathbb{R}), \cdot)$;

в) $(\mathbb{Z}, +)$ и $(\mathbb{R}, +)$; г) $(\mathbb{N}, +)$ и $(2\mathbb{N}, +)$;

д) $(\mathbb{R}, +)$ и $(\mathbb{R}, \cdot)$; е) $(\mathbb{R} \setminus \{0\}, \cdot)$ и $(\mathbb{R}^*_+, \cdot)$;

ж) $(\mathbb{R}, +)$ и $(\mathbb{R} \setminus \{0\}, \cdot)$; з) $(\mathbb{R}, +)$ и $(\mathbb{R}^*_+, \cdot)$;

и) $(2^M, \cap)$ и $(2^M, \cup)$?

2.17. Полугруппа с сокращениями $(G, \cdot)$ коммутативна тогда и только тогда, когда отображение $\varphi(x) = x^2$ есть ее эндоморфизм. Это утверждение неверно, если полугруппа не обладает свойствами сокращения.

2.18. Если $\mathbb{Q}_{(<1)}$ $(\mathbb{Q}_{(>1)})$ — множество всех положительных рациональных чисел, меньших 1 (больших 1), то $(\mathbb{Q}_{(<1)}, \cdot)$ и $(\mathbb{Q}_{(>1)}, \cdot)$ изоморфны.

2.19. Пусть $\mathbb{R}_+$ и $\mathbb{R}_-$ — соответственно, множества всех положительных и отрицательных вещественных чисел. Полугруппы $(\mathbb{R}_+, +)$ и $(\mathbb{R}_-, +)$ изоморфны.

2.20. Пусть G — полугруппа, A и B — ее подполугруппы и $A \circ B = \langle A, B \rangle$ — подполугруппа, порожденная подмножеством $A \cup B$. Множество подполугрупп из G является полугруппой относительно введенной операции $\circ$, в которой каждый элемент оказывается идемпотентом. Рассмотрите дуальный вариант с операцией $A * B = A \cap B$.

2.21. Подмножество T полугруппы S является подгруппой тогда и только тогда, когда $aT = Ta = T$ для любого $a \in T$.

2.22. Пусть $M = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,\middle|\, x \in \mathbb{R} \right\}$. Относительно матричного умножения M есть группа, изоморфная $\mathbb{R}$.

2.23. Пусть A и B — полугруппы. На $A \times B$ определена операция $(a, b)(a', b') = (aa',\ bb')$. Покажите, что $A \times B$ — полугруппа с единицей тогда и только тогда, когда A и B — полугруппы с единицами. Постройте гомоморфизмы полугруппы $A \times B$ в A и в B. Если полугруппа B содержит единицу, то существует гомоморфное вложение полугруппы A в $A \times B$. Какие свойства A и B наследуются полугруппой $A \times B$?

2.24. Какие из следующих отображений будут гомоморфизмами? В случае положительного ответа найдите их ядра.

а) $\varphi\colon (\mathbb{R}^n, +) \to (\mathbb{R}, +)$, $\varphi(x_1, \dots, x_n) = x_1 + x_n$;

б) $\varphi\colon (\mathbb{R}, +) \to (\mathbb{Z}, +)$, $\varphi(x) = [x]$ — целая часть числа x;

в) $\varphi\colon (\mathbb{R}, \cdot) \to (\mathbb{Z}, \cdot)$, $\varphi(x) = [x]$ — целая часть числа x.

2.25. 1) Если полугруппа имеет левую единицу и каждый элемент в ней обратим слева, то все ее элементы обратимы и справа, причем левый обратный для элемента a является также и правым обратным для этого элемента, т.е. эта полугруппа является группой.

2) В коммутативной полугруппе, обладающей идемпотентами, множество всех идемпотентов является подполугруппой.

3) Во всякой конечной полугруппе найдется идемпотент.

4) Если e — идемпотент полугруппы с левым сокращением, то e является левой единицей.

5) Полугруппа с сокращениями может содержать только один идемпотент, а именно единицу.

2.26. Сколько существует неизоморфных между собой полугрупп порядка 2?

2.27. 1) Моногенная полугруппа конечна тогда и только тогда, когда содержит идемпотент.

2) Конечная моногенная полугруппа либо является группой, либо имеет только один порождающий элемент.

3) Любые две бесконечные моногенные полугруппы изоморфны.

2.28. Приведите пример конечной полугруппы с сокращением слева, не являющейся группой.

Пусть S — произвольная полугруппа без единицы и 1 — символ, не являющийся элементом из S. Распространим бинарную операцию, заданную на S, на множество $S^1 = S \cup \{1\}$, полагая $1 \cdot 1 = 1$ и $1 \cdot a = a$ для любого $a \in S$. Проверьте, что S^1 есть полугруппа с единицей 1. Переход от S к S^1 называется *присоединением единицы к* S. Введем обозначение

$$S^1 = \begin{cases} S, & \text{если } S \text{ имеет единицу,} \\ S \cup \{1\} & \text{в противном случае.} \end{cases}$$

Аналогичным образом можно присоединить нуль 0 к S.

2.29. 1) Если S — полугруппа с сокращениями, то такова и S^1.

2) Если S — полугруппа левых нулей и $|S| > 1$, то S — полугруппа с правым сокращением, но S^1 не обладает этим свойством.

3) S является полугруппой с правым сокращением и не имеет идемпотентов $\neq 1$ тогда и только тогда, когда S^1 — полугруппа с правым сокращением.

2.30. Всякая полугруппа S изоморфна подполугруппе симметрической полугруппы $F(S^1)$ на S^1.

2.31. 1) Любое множество правых нулей группоида S является его левым идеалом.

2) Если S — полугруппа, то ее левый (правый) идеал, порожденный A, равен $A \cup SA = S^1A$ ($A \cup AS = AS^1$), а двусторонний идеал — равен $A \cup SA \cup AS \cup SAS = S^1AS^1$.

3) Полугруппа S проста справа тогда и только тогда, когда $aS = S$ для каждого $a \in S$.

4) Полугруппа является группой тогда и только тогда, когда она проста как слева, так и справа.

2.32. Пусть a — элемент полугруппы S, и пусть $A = \{x \,|\, axa = a,\ x \in S\}$. Если $A \neq \varnothing$, то Aa (aA) есть подполугруппа левых (правых) нулей.

2.33. 1) Полугруппа левых нулей проста слева, и каждый ее элемент образует правый идеал.

2) Каждый идемпотент простой справа полугруппы является ее левой единицей.

2.34. Если S — полугруппа, обладающая правым нулем, то множество K всех правых нулей из S есть подполугруппа, являющаяся полугруппой правых нулей, и, кроме того, двусторонний идеал, содержащийся в каждом двустороннем идеале полугруппы S.

2.35. Элемент $\alpha \in F(X)$ является идемпотентом тогда и только тогда, когда α действует на $\alpha(X)$ как тождественное отображение.

2.36. Если $f\colon A \to B$ — гомоморфизм группоидов и I — левый (правый) идеал в A, то $f(I)$ — левый (правый) идеал в $f(A)$. Если J — левый (правый) идеал в B, то $f^{-1}(J) = \{a \in A \,|\, f(a) \in J\}$ — левый (правый) идеал в A.

2.37. Пусть a — элемент полугруппы S и $\langle a \rangle$ — циклическая подполугруппа в S, порожденная a. Докажите, что $\langle a \rangle$ состоит из всех положительных целых степеней элемента a: $\langle a \rangle = \{\, a, a^2, \dots \}$. Если $\langle a \rangle$ бесконечна, то все степени элемента a различны. Если же $\langle a \rangle$ конечна, то существуют два положительных целых числа, *индекс* r и *период* m

полугруппы $\langle a\rangle$, для которых $a^{m+r} = a^r$ и $\langle a\rangle = \{a, a^2, \dots, a^{m+r-1}\}$. Порядок подполугруппы $\langle a\rangle$ равен $m + r - 1$. Множество $Ka = \{a^r, a^{r+1}, \dots, a^{m+r-1}\}$ является циклической подгруппой порядка m полугруппы S.

2.38. Пусть a — элемент конечного порядка полугруппы S, и пусть r — индекс, а m — период элемента a. Тогда единица подгруппы Ka полугруппы $\langle a\rangle$ равна a^n, где n делится на m и $r \leqslant n < r + m$.

Полугруппа называется *периодической*, если каждый ее элемент имеет конечный порядок.

2.39. 1) Для всякого элемента конечной полугруппы найдется некоторая его степень, являющаяся идемпотентом.

2) Если a — элемент конечного порядка, то полугруппа $\langle a\rangle$ содержит только один идемпотент, а именно единицу группы Ka.

2.40. Если S — полугруппа с правым сокращением, то каждый ее элемент конечного порядка имеет индекс, равный 1.

2.41. Для любых двух заданных чисел r и m можно построить циклическую полугруппу $\langle a\rangle$, индекс которой равен r, а период m. Конечные циклические полугруппы изоморфны тогда и только тогда, когда они имеют одинаковые индекс и период.

2.42. Пусть S — коммутативная периодическая полугруппа и E — множество идемпотентов из S. Для каждого $f \in E$ через S_f обозначим множество всех таких $x \in E$, что $x^n = f$ для некоторого натурального n. Тогда $S_f \cap S_g = \varnothing$ при $f \neq g$, и S есть объединение всех подмножеств S_f. Каждое S_f является подполугруппой полугруппы S, содержащей f и не имеющей других идемпотентов, $S_f S_g \subseteq S_{fg}$ для всех $f, g \in E$.

2.43. 1) Множество P (соответственно, Q) всех обратимых справа (соответственно, слева) элементов полугруппы S с единицей является подполугруппой с правым (соответственно, левым) сокращением.

2) Множество U всех обратимых элементов полугруппы S с единицей есть подгруппа в S и совпадает с пересечением множества P всех обратимых справа элементов с множеством Q всех обратимых слева элементов полугруппы S. В частности, если $S = \langle M\rangle$ и каждый элемент $x \in M$ обратим в S, то S является группой.

2.44. 1) Полугруппа S содержит подгруппу тогда и только тогда, когда она содержит идемпотент.

2) Если e — идемпотент полугруппы S, то eS (Se) состоит из всех элементов $a \in S$, для которых e является левой (правой) единицей, а eSe есть множество всех элементов полугруппы S, для которых e является двусторонней единицей, и $eSe = eS \cap Se$. Кроме того, eS (Se) — главный правый (левый) идеал полугруппы S, порожденный элементом e.

2.45. Пусть e — идемпотент полугруппы S. Тогда eSe является подполугруппой в S. Обозначим через H_e группу обратимых элементов полугруппы eSe. Докажите, что:

а) H_e содержит каждую подгруппу полугруппы S, пересекающуюся с H_e;

б) подгруппы H_e и только они являются максимальными подгруппами полугруппы S, причем $H_e \cap H_f = \varnothing$ при $e \neq f$;

в) максимальная подгруппа H_e полугруппы S, содержащая идемпотент e, может быть охарактеризована как множество всех таких элементов $a \in S$, что $ea = ae = a$ и существуют $x, y \in S$, для которых $xa = ay = e$;

г) Ka (см. 2.37) является единственной максимальной подгруппой в конечной циклической полугруппе.

2.46. Пусть P (Q) — подполугруппа обратимых справа (слева) элементов полугруппы S с единицей 1 и U — группа обратимых элементов полугруппы S.

1) Следующие три условия для полугруппы S эквивалентны: а) $ab = 1$ ($a, b \in S$) влечет за собой $ba = 1$; б) $P = U$; в) $Q = U$.

2) Условия, перечисленные в п. 1), выполняются, если S — периодическая полугруппа или если S — полугруппа с правым сокращением.

3) Условия, перечисленные в п. 1), выполняются для полугрупп P и Q.

Связкой называется полугруппа, каждый элемент которой является идемпотентом.

2.47. Пусть E — множество идемпотентов полугруппы S. Положим $e \leqslant f$ ($e, f \in E$), если $ef = fe = e$. Покажите, что $\leqslant$ есть частичный порядок на E. Он называется *естественным частичным порядком на* E.

Коммутативная связка S является нижней полурешеткой относительно естественного частичного порядка на S. Нижняя грань элементов a, b полугруппы S совпадает с их произведением. Обратно, нижняя полурешетка является коммутативной связкой относительно операции взятия нижней грани.

Ненулевой идемпотент e полугруппы S называется *примитивным*, если каждый идемпотент из S, меньший e, равен e или 0 (если S имеет нуль).

2.48. Полугруппа S антикоммутативна тогда и только тогда, когда она есть связка без нуля, в которой каждый элемент примитивен, или $|S| = 1$.

2.49. Для элементов полугруппы S докажите следующие свойства:

а) если $a = axa$, то $e = ax$ ($f = xa$) является идемпотентом, причем $ea = a$ ($af = a$);

б) если $a = axa$, то главный правый (левый) идеал $aS^1 = \{a\} \cup aS$ ($S^1a = Sa \cup \{a\}$) равен aS (Sa);

в) элемент $a \in S$ регулярен тогда и только тогда, когда главный правый (левый) идеал полугруппы S, порожденный a, порождается некоторым идемпотентом e, т.е. $aS^1 = eS^1$ ($S^1a = S^1e$).

Произведение $\circ$ бинарных отношений (см. начало § 1) обладает свойством ассоциативности, следовательно, множество B_X всех бинарных отношений на X является полугруппой относительно этой операции. Что является единицей и нулем этой полугруппы?

Если ρ — произвольное отношение на X, то отношение

$$\rho^t = \bigcup_{n=1}^{\infty} \rho^n = \rho \cup (\rho \circ \rho) \cup \dots$$

называется *транзитивным замыканием* отношения ρ.

Пересечение произвольного семейства отношений эквивалентности является отношением эквивалентности. Аналогичное утверждение для теоретико-множественного объединения не верно. *Объединением* $\rho \vee \sigma$ двух отношений эквивалентности ρ и σ называется отношение эквивалентности, порожденное теоретико-множественным объединением $\rho \cup \sigma$, т.е. $\rho \vee \sigma$ — транзитивное замыкание отношения $\rho \cup \sigma$.

2.50. Докажите, что $(\rho^{-1})^{-1} = \rho$, $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$, т.е. отображение $\rho \mapsto \rho^{-1}$ является *инволютивным антиизоморфизмом*.

Любое отношение эквивалентности на X является идемпотентом полугруппы B_X. Кроме того:

а) ρ^t транзитивно и содержится в каждом транзитивном отношении на X, содержащим ρ;

б) $\rho_1 = \rho_0 \cup \rho_0^{-1} \cup \iota$, где ι — *отношение равенства* (или «диагональ» множества $X \times X$), есть наименьшее рефлексивное и симметричное отношение на X, содержащее данное отношение ρ_0;

в) транзитивное замыкание $\rho = \rho_1^t$ является отношением эквивалентности на X, которое содержится в каждом отношении эквивалентности на X, содержащим ρ_0, оно называется *отношением эквивалентности на* X, *порожденным* ρ_0.

2.51. Если ρ и σ — отношения эквивалентности на множестве X и $\rho \circ \sigma = \sigma \circ \rho$, то $\rho \circ \sigma$ — также отношение эквивалентности на множестве X и $\rho \circ \sigma = \rho \vee \sigma$.

Говорят, что отношение ρ на группоиде S *стабильно* или *регулярно* справа (слева), если $(a, b) \in \rho$, где $a, b \in S$, влечет за собой $ac\rho bc$ ($ca\rho cb$) для каждого $c \in S$. Стабильное справа (слева) отношение эквивалентности на S называется *правой* (*левой*) *конгруэнцией на* S. Левая и правая конгруэнция называется *конгруэнцией* на группоиде.

2.52. Пусть ρ — конгруэнция на группоиде S и $\overline{a}, \overline{b}$ — элементы множества $\overline{S} = S/\rho$, т.е. классы эквивалентности S по отношению ρ. Определим произведение на $\overline{S}$ по правилу $\overline{a} \cdot \overline{b} = \overline{ab}$. Проверьте, что:

а) $(\overline{S}, \cdot)$ является группоидом, который называется *факторгруппоидом* группоида S по отношению ρ и обозначается S/ρ;

б) отображение $\overline{\rho}$: $a \mapsto \rho a$ есть гомоморфизм группоида S на $\overline{S}$, он называется *каноническим гомоморфизмом* группоида S на $\overline{S}$.

Пусть φ — отображение множества X в множество Y. Тогда φ можно считать отношением на множестве $X \cup Y$. Для каждого $y \in Y$ имеем $\varphi^{-1}y = \{x \in X \mid \varphi x = y\}$. Композиция отношений $\rho = \varphi^{-1} \circ \varphi$ содержится в $X \times X$. Поэтому ее можно считать отношением на X, $a\rho b$ $(a, b \in X)$ если и только если $\varphi a = \varphi b$.

2.53. (Основная теорема о гомоморфизмах). Пусть φ — гомоморфизм группоида S на группоид G, и пусть $\rho = \varphi^{-1} \circ \varphi$. Тогда ρ — конгруэнция на S и существует изоморфизм ψ группоида S/ρ на G, такой, что $\psi\overline{\rho} = \varphi$, где $\overline{\rho}$ — канонический гомоморфизм S на $\overline{S}$.

2.54. Пусть H — подгруппа группы G. Определим отношение ρ на G следующим образом: $a\rho b$ $(a, b \in G)$ в том и только в том случае, когда $ab^{-1} \in H$. Классами отношения ρ являются множества Ha при $a \in G$. Докажите, что:

а) ρ является правой конгруэнцией, и каждая правая конгруэнция получается таким образом;

б) ρ является конгруэнцией тогда и только тогда, когда H — нормальная подгруппа в G.

Два элемента a, b полугруппы S называются *инверсными* (или *регулярно сопряженными*) друг к другу, если $aba = a$ и $bab = b$.

2.55. Если a — регулярный элемент полугруппы S, $axa = a$, то a обладает хотя бы одним инверсным к нему элементом. Таким элементом, в частности, будет xax.

2.56. Два элемента полугруппы S взаимно обратны в некоторой подгруппе полугруппы S тогда и только тогда, когда они инверсны друг к другу и коммутируют.

2.57. Регулярный элемент может иметь несколько инверсных к нему элементов. Приведите пример полугруппы, в которой любые два элемента инверсны друг к другу.

Если e, f, ef и fe — идемпотенты полугруппы S, то ef и fe инверсны друг к другу.

2.58. Следующие три условия для полугруппы S эквивалентны:

а) S регулярна и любые два ее идемпотента коммутируют;

б) каждый главный правый и каждый главный левый идеал полугруппы S имеет единственный порождающий идемпотент;

в) S — *инверсная полугруппа* (т.е. каждый элемент из S обладает единственным инверсным к нему элементом).

Пусть S — инверсная полугруппа. Элемент, инверсный к $a \in S$, обозначается через a^{-1}. Имеем $aa^{-1}a = a$ и $a^{-1}aa^{-1} = a^{-1}$. Идемпотент $e = aa^{-1}$ ($f = a^{-1}a$) называется *левой* (*правой*) *единицей элемента* a; его можно охарактеризовать как единственный идемпотент, порождающий правый (левый) идеал aS (Sa).

2.59. Для любых элементов a, b инверсной полугруппы имеют место соотношения: $(a^{-1})^{-1} = a$ и $(ab)^{-1} = b^{-1}a^{-1}$.

2.60. Полугруппа всех преобразований $F(X)$ множества X регулярна.

2.61. Пусть S — полугруппа левых нулей, причем $|S| > 1$. Тогда каждый главный правый идеал в S имеет единственный порождающий его идемпотент, но S не является инверсной полугруппой.

2.62. В полугруппе S любые два элемента инверсны друг к другу тогда и только тогда, когда S антикоммутативна.

2.63. Если регулярная полугруппа обладает свойством сокращения или содержит точно один идемпотент, то она является группой.

2.64. Пусть a — элемент полугруппы S и $A = \{x \mid axa = a,\ x \in S\}$. Тогда AaA есть множество элементов, инверсных к a.

2.65. Очевидно, что необходимым условием вложения полугруппы в группу является выполнение двустороннего закона сокращения. Докажите, что всякая коммутативная полугруппа с сокращениями вкладывается в группу.

Полугруппа S называется *реверсивной справа*, если $Sa \cap Sb \neq \varnothing$ для всех $a, b \in S$. Говорят также, что полугруппа S удовлетворяет *левому условию Оре*.

2.66. Любая реверсивная справа полугруппа с сокращениями вкладывается в группу.

Говорят, что группа G есть *группа левых частных полугруппы* S, если G — такая группа, содержащая полугруппу S, что каждый элемент из G представим в виде $a^{-1}b$, где $a, b \in S$.

2.67. Полугруппа с сокращениями вкладывается в группу левых частных, если и только если она реверсивна справа.

Пусть S — реверсивная справа полугруппа с сокращениями и G, H — две группы левых частных для S. Тогда существует изоморфизм группы G на H, оставляющий элементы из S неподвижными.

2.68. Пусть S — множество упорядоченных пар (i, j) неотрицательных целых чисел. Определим в S умножение, полагая

$$(i, j)(k, l) = (i + k, 2^k j + l).$$

Покажите, что полугруппа S реверсивна слева, но не справа.

2.69. Пусть S — реверсивная справа полугруппа с сокращениями, и пусть G — группа, содержащая S в качестве подполугруппы и порожденная полугруппой S. Покажите, что G является группой левых частных полугруппы S.

Глава II. Группы

3 Группы. Порождающие множества групп

Напомним (см. § 2), что множество G называется *группой*, если:

1) на множестве G определена бинарная операция: $(x, y) \mapsto xy$;

2) операция ассоциативна: $(xy)z = x(yz)$ для всех $x, y, z \in G$;

3) G обладает нейтральным (единичным) элементом e: $xe = ex = x$ для всех $x \in G$;

4) для каждого элемента $x \in G$ существует обратный x^{-1}: $xx^{-1} = x^{-1}x = e$.

Термин «группа» принадлежит французскому математику Галуа (Э. Галуа, 1811–1832). Подмножество H группы G называется подгруппой в G, если $e \in H$ и $h^{-1} \in H$, $h_1h_2 \in H$ для любых $h, h_1, h_2 \in H$.

Пересечение всех подгрупп группы G, содержащих непустое подмножество $S \subseteq G$, будет минимальной подгруппой в G, содержащей S; ее называют *подгруппой, порожденной множеством* S в группе G и обозначают $\langle S\rangle$, множество S называют *множеством образующих* подгруппы $\langle S\rangle$. Группа, порожденная конечной системой образующих, называется *конечно порожденной*. Если группа порождается одним элементом, то так же, как в случае полугрупп, ее называют *циклической*.

Пусть G — группа, a — ее неединичный элемент конечного порядка (см. § 2); тогда порядок совпадает с наименьшим натуральным числом n со свойством $a^n = e$, и обозначается через $o(a) = n$. Если $x^k \neq e$ для каждого натурального числа k, то элемент x группы G называется *элементом бесконечного порядка*. Если каждый неединичный элемент группы G имеет бесконечный (соответственно, конечный) порядок, то G называется группой *без кручения* (соответственно, *периодической* группой).

Совокупность $t(G)$ всех периодических элементов группы G называется ее *периодической частью*.

Элемент группы порядка два называется *инволюцией*.

Пусть π — некоторое множество простых чисел. Элемент группы называется π*-элементом*, если он имеет конечный порядок, все простые делители которого лежат в π. Группа, состоящая из π-элементов, называется π*-группой*. Группа называется π*-замкнутой*, если множество всех ее π-элементов является в ней подгруппой. При $\pi = \{p\}$ в вышеприведенных терминах пишут просто p.

Коммутативная периодическая группа называется *элементарной*, если всякий ее элемент имеет порядок, не делящийся на квадрат.

Элементы a и b группы G называются *сопряженными* в G, если имеется элемент $g \in G$ такой, что $g^{-1}ag = b$. Элемент $g^{-1}ag$ часто обозначается также через a^g. Множество $a^G = \{a^g \mid g \in G\}$ называется *классом сопряженных элементов* группы G (содержащим элемент a). Если A, B — подмножества группы, то обозначают $A^B = \{a^b \mid a \in A,\, b \in B\}$.

Подгруппой Фраттини $\Phi(G)$ группы G называется пересечение всех ее максимальных подгрупп, если они существуют, и сама группа G — в противном случае.

Еще раз отметим, что по теории групп имеются задачники [5] и [33], их можно использовать для дальнейшего углубления в теорию. Наиболее полно в [5] (наряду с другими разделами) представлена теория конечных групп.

Задачи

3.1. Подмножество H группы G является ее подгруппой тогда и только тогда, когда для любых $a, b \in H$ следует, что $ab^{-1} \in H$ (*критерий подгруппы*).

3.2. Если H — конечное подмножество группы G (или если все элементы из H имеют конечный порядок) и $HH \subseteq H$, то H будет подгруппой в G.

3.3. Пусть H — подмножество группы G. Равносильны следующие условия:

а) H — подгруппа в G; б) $HH \cup H^{-1} \subseteq H$;

в) $HH^{-1} \subseteq H$; г) $H^{-1}H \subseteq H$;

д) $Hx = H$ для каждого $x \in H$; е) $xH = H$ для каждого $x \in H$.

3.4. Пусть M — подмножество группы G. Тогда множество $H = \{g \in G \mid Mg = M\}$ является подгруппой в G, причем $MH = M$ и, если мощность $|M|$ конечна, то $|H|$ делит $|M|$.

3.5. Если A — подгруппа группы G, то $A \subseteq (G \setminus A)(G \setminus A)$ и $G = (G \setminus A)(G \setminus A) \cup (G \setminus A) = \langle G \setminus A \rangle$. А если B — такая подгруппа группы G, что $B \not\subseteq A$, то $B = \langle B \setminus A \rangle$.

3.6. Группа $\mathrm{SL}(2, \mathbb{R})$ содержит элементы $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ порядков 4 и 3 соответственно. Покажите, что $o(ab) = \infty$. В частности, периодическая часть этой группы не является подгруппой.

3.7. Какие из указанных множеств с операциями являются группами:

а) $(A, +)$ (соответственно, $(A \setminus \{0\}, \cdot)$), где A — одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

б) $(n\mathbb{Z}, +)$, где n — натуральное число; в) $(\{-1, 1\}, \cdot)$;

г) множество степеней данного вещественного числа $a \neq 0$ с целыми показателями относительно умножения;

д) множество всех комплексных корней фиксированной степени n (соответственно, всех степеней) из 1 относительно умножения;

е) множество комплексных чисел с фиксированным модулем r относительно умножения;

ж) множество ненулевых комплексных чисел с модулем, не превосходящим фиксированное число r, относительно умножения;

з) множество ненулевых комплексных чисел, расположенных на лучах, выходящих из начала координат и образующих с лучом Ox углы $\varphi_1, \varphi_2, \dots \varphi_n$, относительно умножения;

и) множество всех непрерывных отображений $\varphi\colon [0, 1] \to [0, 1]$, для которых $\varphi(0) = 0$, $\varphi(1) = 1$, и $x < y$ влечет $\varphi(x) < \varphi(y)$, относительно композиции?

3.8. Какие из указанных ниже отображений множества $M = \{1, 2, \dots, n\}$ в себя образуют группу относительно умножения:

а) множество всех (соответственно, инъективных, сюръективных, биективных) отображений;

б) множество всех четных (соответственно, нечетных) перестановок;

в) множество всех транспозиций;

г) множество всех перестановок, оставляющих неподвижными элементы некоторого подмножества $S \subseteq M$;

д) множество всех перестановок, при которых образы всех элементов некоторого подмножества $S \subseteq M$ принадлежат этому подмножеству;

е) множество $V_4 = \{E, (12)(34), (13)(24), (14)(23)\}$;

ж) множество $D_4 = \{E, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$?

Группа V_4 называется *четверной группой* (или *группой Клейна*). Группа D_4 изоморфна группе симметрий квадрата.

3.9. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу (относительно сложения или умножения, если операция не задана):

а) множество симметрических (кососимметрических) матриц;

б) множество матриц с фиксированным определителем d;

в) множество диагональных (соответственно, невырожденных диагональных) матриц;

г) множество верхних треугольных (нильтреугольных) матриц;

д) множество верхних нильтреугольных матриц относительно операции $A \circ B = A + B - AB$;

е) множество верхних унитреугольных матриц;

ж) множество матриц вида $f(A)$, где A — фиксированная нильпотентная матрица (т.е. $A^n = 0$ для некоторого натурального n), $f(t)$ — произвольный многочлен с ненулевым свободным членом;

з) множество ненулевых матриц вида $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}$ $(a, b \in \mathbb{R})$, где λ — фиксированное вещественное число?

3.10. Следующие совокупности функций образуют группы относительно операции композиции:

а) $\{x,\ -x,\ x^{-1},\ -x^{-1} \mid x \in \mathbb{R} \setminus \{0\}\}$;

б) $\{x,\ 1-x,\ x^{-1},\ (x-1)x^{-1},\ x(x-1)^{-1},\ (1-x)^{-1} \mid x \in \mathbb{R} \setminus \{0,1\}\}$;

в) $\left\{x,\ \frac{1}{x},\ -x,\ -\frac{1}{x},\ \frac{x-1}{x+1},\ \frac{1-x}{x+1},\ \frac{x+1}{x-1},\ \frac{x+1}{1-x} \;\middle|\; x \in \mathbb{R} \setminus \{0, \pm 1\}\right\}$;

г) $\{\varepsilon^k x,\ \varepsilon^m x^{-1} \mid \varepsilon$ — первообразный корень n-й степени из единицы, $0 \leqslant k, m < n$, а $x \in \mathbb{R} \setminus \{0\}\}$;

д) $\{kx + m \mid k \neq 0,\ k, m \in \mathbb{Z}_p$, и $x \in \mathbb{Z}_p\}$.

3.11. Пусть $n \geqslant 2$, а $p_1, \ldots, p_n$ — различные простые числа и $\overline{p}_i = p_1 \ldots p_{i-1} p_{i+1} \ldots p_n$. Тогда $\mathbb{Z} = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$, причем ни один из элементов этого порождающего множества нельзя удалить.

3.12. Множество функций вида $f(z) = \frac{az+b}{cz+d}$, где $a, b, c, d \in \mathbb{C}$ и $ad - bc \neq 0$ (соответственно, $ad - bc = 1$ или $ad - bc = \pm 1$), образует группу относительно операции композиции функций.

3.13. Если $G = \mathbb{R} \setminus \{-1\}$, то G — группа относительно операции $x \circ y = x + y + xy$.

3.14. Пусть $S \subseteq G$. Подгруппа $\langle S \rangle$ совпадает с множеством $T \subseteq G$, состоящим из единичного элемента e и всевозможных произведений $t_1 \ldots t_n$, $n = 1, 2, \ldots$, где либо $t_i \in S$, либо $t_i^{-1} \in S$, $i = 1, \ldots, n$.

3.15. 1) Каждая группа имеет порождающее множество, порядки элементов которого либо все конечны, либо все бесконечны.

2) Если группа конечно порожденная, то каждое ее порождающее множество содержит конечное порождающее подмножество.

3.16. Группа $G = \langle a,\ b \rangle$ с условием: $a^3 = e$, $b^7 = e$, $a^{-1}ba = b^3$ является циклической группой третьего порядка.

3.17. Пусть G — группа, в которой среди любых трех элементов (четырех элементов) найдутся два перестановочных между собой (найдутся два подмножества, состоящие из двух перестановочных элементов). Тогда G коммутативна.

3.18. Найдите все образующие группы $\mathbb{Z}$. Приведите примеры образующих группы $\mathbb{Q}$, будет ли она конечно порожденной?

3.19. Если A и B — подгруппы и подгруппа C содержится в $A \cup B$, то $C \subseteq A$ или $C \subseteq B$. В частности, $A \cup B$ — подгруппа тогда и только тогда, когда $A \subseteq B$ или $B \subseteq A$.

3.20. Пусть A, B, C, D — подгруппы группы G такие, что $A \cup B = C \cup D$. Тогда либо $\{A,\ B\} = \{C,\ D\}$, либо левая и правая части равенства — подгруппы в G (и тогда левая часть совпадает с A или B, а правая — с C или D).

3.21. Если a и b — неединичные элементы конечного порядка группы такие, что $a^{-1}ba = b^{-1}$, то хотя бы один из элементов a и b имеет четный порядок.

3.22. Во всякой группе четного порядка имеется элемент порядка 2 (инволюция), причем число инволюций нечетно. В группе нечетного порядка нет инволюций.

3.23. Найдите группу обратимых элементов кольца вычетов $\mathbb{Z}_m$. Будут ли эти группы циклическими при $m =$ 5, 15, 16, 17, 18?

3.24. В группе G нечетного порядка разрешимо уравнение $x^2 = g$ для каждого $g \in G$.

3.25. Если порядки подгрупп A, B группы G взаимно просты, то $A \cap B = e$.

3.26. Если $a^2 = e$ для любого элемента a группы, то эта группа коммутативна.

3.27. Пусть G — группа порядка 8 и $a^2 = e$ для любого ее элемента. Тогда G имеет 16 различных подгрупп.

3.28. Все группы порядка $\leqslant 5$ коммутативны. Напишите таблицы умножения этих групп и представьте эти группы в виде групп подстановок.

3.29. Найдите порядок элемента группы:

$$\text{а) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5, \quad \text{б) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} \in S_6, \quad \text{в) } -\frac{\sqrt{3}}{2} + \frac{1}{2}i \in \mathbb{C}^*;$$

$$\text{г) } \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \in \mathbb{C}^*; \quad \text{д) } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}(4, \mathbb{R});$$

е) $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{C})$; ж) $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{C})$.

3.30. Если группа G обладает конечным или счетным множеством порождающих элементов, то $|G| \leqslant \aleph_0$.

3.31. Пусть n — количество элементов порядка 6 в группе G. Тогда:

а) $n = 2$, если $G = \mathbb{C}^*$;

б) $n = 20$, если $G = S_5$;

в) $n = 0$, если $G = A_5$.

3.32. Пусть x — элемент группы G. Тогда:

а) если $o(x) = \infty$, то $x^n = x^m$ в том и только в том случае, когда $n = m$;

б) если $o(x) = n$, то $x^k = e$ в том и только в том случае, когда k делится на n; $x^m = x^s$ в том и только в том случае, когда $m - s$ делится на n;

в) если группа G конечна, то $G = \langle x \rangle$ в том и только в том случае, когда $o(x) = |G|$.

Найдите порядок элемента x^n. Когда элементы x^n и x^m имеют одинаковые порядки?

3.33. Пусть в группе все неединичные элементы имеют одинаковый порядок p. Тогда p — простое число.

3.34. Существуют ли бесконечные периодические группы?

3.35. Пусть $G = \langle a \rangle$ — циклическая группа порядка n. Тогда:

а) элемент a^k является порождающим для группы G тогда и только тогда, когда $(k, n) = 1$, значит, число таких элементов равно значению $\varphi(n)$, где φ — функция Эйлера;

б) всякая подгруппа группы G порождается элементом вида a^d, где d — некоторый делитель числа n;

в) для всякого делителя d числа n существует единственная подгруппа группы G порядка d;

г) если $(n, k) = 1$, то в G разрешимо уравнение $x^k = a$.

3.36. Группа простого порядка является циклической и любой ее неединичный элемент будет образующим группы.

3.37. Найдите число элементов порядка p^m в циклической группе порядка p^n, где p — простое число, $m = 1, 2, \ldots, n$.

Группа называется *локально циклической,* если каждое ее конечное подмножество порождает циклическую подгруппу. Ясно, что такая группа коммутативна.

Пара (A, B) подгрупп A и B группы G называется *дистрибутивной*, если для всякой подгруппы C группы G выполняется дистрибутивный закон $C \cap \langle A, B\rangle = \langle C \cap A, C \cap B\rangle$.

Порядком элемента c *относительно* подгруппы A называется такое наименьшее $n \in \mathbb{N}$, что $c^n \in A$.

3.38. 1) Подгруппы A и B тогда и только тогда образуют дистрибутивную пару, когда порядки относительно A и B любого элемента $c \in \langle A, B\rangle \setminus (A \cup B)$ конечны и взаимно просты.

2) В группе G решетка ее подгрупп дистрибутивна тогда и только тогда, когда G — локально циклическая группа (решетка подгрупп определяется в начале § 1).

3) Если подгруппы A и B таковы, что $AB = BA$, то выполняется модулярное тождество: $C \cap \langle A, B\rangle = \langle A, C \cap B\rangle$ для всякой подгруппы C со свойством $A \subseteq C$.

3.39. Найдите все подгруппы групп: $\mathbb{Z}_6$, $\mathbb{Z}_{24}$, V_4 и S_3.

3.40. Перестановочные элементы a, b взаимно простых порядков n и m порождают в группе циклическую подгруппу порядка nm.

3.41. Для любых элементов a, b, c группы G:

а) $o(a) = o(a^{-1})$; б) $o(a) = o(bab^{-1})$;

в) $o(ab) = o(ba)$; г) $o(abc) = o(bca) = o(cab)$.

3.42. Пусть G — конечная группа, и m — наименьшее среди натуральных чисел s таких, что $g^s = e$ для всякого элемента $g \in G$. Докажите, что:

а) m делит $|G|$ и равно наименьшему общему кратному порядков элементов группы G, т.е. $m = \exp(G)$;

б) если группа G коммутативна, то существует элемент $g \in G$ порядка $\exp(G)$;

в) конечная коммутативная группа G является циклической тогда и только тогда, когда $\exp(G) = |G|$;

г) конечная p-группа G является циклической тогда и только тогда, когда $\exp(G) = |G|$.

3.43. 1) Решетка подгрупп циклической группы порядка p^n, где p — простое число, образует цепь.

2) Найдите все конечные группы, в которых подгруппы образуют цепь.

3) Представьте группу $\mathbb{Q}$ в виде объединения возрастающей цепочки циклических подгрупп.

Движением евклидовой плоскости называется любое отображение этой плоскости на себя, сохраняющее расстояние между точками. Если F — произвольная фигура на евклидовой плоскости, то множество всех движений плоскости, переводящих F на себя, с операцией композиции (последовательного выполнения) двух движений, является группой; она называется *группой симметрий фигуры* F.

3.44. Опишите группы симметрий:

а) правильного треугольника; б) квадрата;

в) ромба; г) правильного n-угольника.

3.45. Всякая бесконечная группа имеет бесконечное число подгрупп.

3.46. Группа $\mathbb{Q}$ локально циклическая и каждая ее подгруппа является либо бесконечной циклической группой, либо объединением возрастающей последовательности бесконечных циклических групп.

3.47. Группы заданы порождающими множествами элементов и определяющими соотношениями. Выясните, какие из них коммутативны:

а) $G_1 = \langle x_1,\ x_2,\ \dots \rangle$ и $x_n^2 = x_{n-1}$ при $n = 2,\ 3,\ \dots$;

б) $G = \langle x,\ y \rangle$ и $xy^2 = y^2x$;

в) $G_1 = \langle x_1,\ x_2,\ \dots \rangle$ и $x_n^2 = x_1$ при $n = 2,\ 3,\ \dots$.

3.48. Пусть G — коммутативная группа восьмого порядка. Если G — нециклическая группа, то или G обладает порождающим множеством из двух элементов a и b, относительно которых выполняются соотношения $a^4 = b^2 = e$, или G обладает порождающим множеством из трех элементов $a,\ b,\ c$, относительно которых выполняются соотношения $a^2 = b^2 = c^2 = e$.

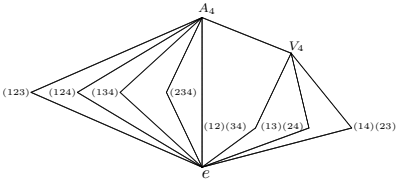
3.49. 1) Множество всех элементов группы $\mathbb{C}^*$, порядки которых есть степени данного простого числа p, является в ней подгруппой (эта подгруппа обозначается через $\mathbb{Z}_{p^\infty}$ и называется *квазициклической* p-группой).

2) $\mathbb{Z}_{p^\infty} = \bigcup\limits_{n=1}^{\infty} \mathbb{Z}_{p^n}$, где через $\mathbb{Z}_{p^n}$ обозначено множество всех комплексных корней степени p^n из единицы.

3) $\mathbb{Z}_{p^\infty}$ есть бесконечная группа, каждая собственная подгруппа которой совпадает с некоторой $\mathbb{Z}_{p^n}$.

4) Группа $\mathbb{Z}_{p^\infty}$ не имеет максимальных подгрупп.

3.50. В нижеприведенной диаграмме изображены все подгруппы знакопеременной группы A_4. Символом V_4 обозначена четверная группа, а возле других вершин диаграммы поставлены образующие циклических подгрупп.



Элемент группы G называется *непорождающим*, если его можно удалить из любого множества порождающих элементов группы G, в которое он входит.

3.51. 1) Множество S всех непорождающих элементов группы G совпадает с подгруппой Фраттини $\Phi(G)$.

2) $\Phi(\mathbb{Z}) = 0$. 3) $\Phi(S_n) = \Phi(A_n) = e$.

4) $\Phi(G) = G$, если $G = \mathbb{Q}$ или $G = \mathbb{Z}_{p^\infty}$.

Говорят, что в группе G выполняется *условие максимальности* (для подгрупп), если всякая возрастающая цепочка ее подгрупп $H_1 \subseteq H_2 \subseteq \dots$ обрывается, т.е. $H_n = H_{n+1} = \dots$ при некотором n.

3.52. В группе G выполняется условие максимальности для подгрупп тогда и только тогда, когда все ее подгруппы конечно порождены.

3.53. Пусть в конечной группе G любые два элемента порождают циклическую подгруппу. Какова G?

3.54. Пусть в функциональном уравнении

$$a_1 f(g_1) + \dots + a_n f(g_n) = b$$

функции $g_1(x) = x$, $g_2(x)$, $\dots$, $g_n(x)$ образуют группу (относительно композиции), где $a_1, \dots, a_n$, b — некоторые функции от x. Замена $x \to g_i$ $(i = 2, \dots, n)$ дает (вместе с исходным уравнением) систему n уравнений, которую используют для нахождения решения.

Решите уравнения:

а) $2f(1-x) + 1 = x\,f(x)$; б) $x\,f(x) + 2f\left(\frac{x-1}{x+1}\right) = 1$;

в) $2x\,f(x) + f\left(\frac{1}{1-x}\right) = 2x$; г) $x\,f(x) + 2f\left(-\frac{1}{x}\right) = 3$;

д) $f\left(\frac{x}{x-1}\right) + x\,f\left(\frac{1}{x}\right) = 2$; е) $f(x) + f\left(\frac{x-1}{x}\right) = 1 - x$.

3.55. Пусть F_q — поле из $q \neq 9$ элементов и a — образующий циклической группы F_q^*. Докажите, что $\mathrm{SL}(2, F_q)$ порождается двумя матрицами $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ a & 1 \end{pmatrix}$.

4 Изоморфизмы групп. Смежные классы

Две группы $(A, \circ)$ и $(B, \times)$ называются *изоморфными*, если они изоморфны как группоиды, т.е. если существует биекция $f\colon A \to B$ со свойством $f(a \circ b) = f(a) \times f(b)$ для всех $a, b \in A$.

Доказано, что всякая счетная группа может быть вложена в группу с двумя образующими, а множество всех неизоморфных групп с двумя образующими имеет мощность континуума. Множество всех неизоморфных групп бесконечной мощности m имеет мощность 2^m. Построены примеры бесконечных p-групп с конечным числом k образующих, здесь p — любое простое число, k — любое натуральное число $\geqslant 2$.

Изоморфизм группы на себя называется ее *автоморфизмом*. Множество автоморфизмов группы G относительно операции композиции образует группу $\mathrm{Aut}\,G$, она является подгруппой группы биекций $S(G)$.

Пусть H — подгруппа группы G. *Левым смежным классом* группы G по подгруппе H называется множество gH элементов вида gh, где g — фиксированный элемент из G, а h пробегает все элементы подгруппы H. Элемент g называется *представителем* смежного класса gH. Аналогично определяется *правый смежный класс* Hg. Между множествами левых смежных классов группы G по подгруппе H и правых смежных классов по той же подгруппе имеется биективное соответствие: $gH \leftrightarrow Hg^{-1}$. Мощность множества левых смежных классов G/H называется *индексом* подгруппы H в G и обозначается символом $(G : H)$.

Задачи

4.1. Пусть на множестве G определены две алгебраические операции $\circ$ и $*$ такие, что $x \circ y = y * x$ для всех $x,\ y \in G$. Тогда если одна из пар $(G, \circ)$ и $(G, *)$ — группа, то группой является и вторая, причем $(G, \circ) \cong (G, *)$.

4.2. Множество G всех пар (a, b) таких, что $a \in \mathbb{R}$ и $b \in \mathbb{R} \setminus \{0\}$, с операцией $(a, b) * (c, d) = (a + bc, bd)$ является группой. Найдите в G два подмножества, каждое из которых относительно ограничения на нем операции $*$ есть группа, причем одна из них изоморфна группе $\mathbb{R}$, другая — $\mathbb{R}^*$. Укажите в G все инволюции. Имеет ли G элементы конечного порядка, большего двух?

4.3. На полуинтервале $[0,\ 1)$ определена операция $*$ следующим образом: $a * b$ есть дробная часть числа $a + b$. Получаемая таким образом группа изоморфна мультипликативной группе U всех комплексных чисел, имеющих единичный модуль.

4.4. Пусть $G = \{x \in \mathbb{R} \,|\, |x| < 1\}$. Определим на G операцию $*$ следующим образом:

$$x * y = \begin{cases} x + y, \text{ если } -1 < x + y < 1, \\ x + y - 1, \text{ если } x + y \geqslant 1, \\ x + y + 1, \text{ если } x + y \leqslant -1. \end{cases}$$

Покажите, что $(G, *)$ — группа и она не изоморфна группе U из 4.3.

4.5. Множество $G = \{e,\ a,\ b,\ c\}$ является группой относительно операции, заданной следующей таблицей умножения:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Эта группа коммутативна, но не циклическая. Каковы порядки ее неединичных элементов? Покажите, что $G \cong V_4$ (см. 3.8 е)), $V_4 \cong \langle a, b \,|\, a^2 = b^2 = e, ab = ba\rangle$ и V_4 изоморфна группе из 3.10 а).

4.6. Если $0 \neq a \in \mathbb{Q}$, то отображение $f\colon x \mapsto ax$ является автоморфизмом группы $\mathbb{Q}$. Найдите все автоморфизмы этой группы.

4.7. Пусть G — ненулевая аддитивная группа, состоящая из вещественных чисел, такая, что в каждом ограниченном промежутке содержится лишь конечное число ее элементов. Тогда $G \cong \mathbb{Z}$.

4.8. Установите изоморфизм между группой комплексных корней степени n из 1 и группой вычетов по модулю n.

4.9. Пусть $G = \{1,\ -1,\ i,\ j,\ k,\ -i,\ -j,\ -k\}$ (здесь знак «$-$» служит лишь для различения некоторых элементов) и $\cdot$ — бинарная операция на G, заданная таблицей:

	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	j	$-i$	-1	$-j$	i	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	$-j$	i	1	j	$-i$	-1

Эта группа часто обозначается через Q_8, а всякая изоморфная ей группа называется *группой кватернионов*.

4.10. Какие из групп $\langle g\rangle$, порожденные элементом $g \in G$, изоморфны:

а) $G = \mathbb{C}^*$, $g = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$;

б) $G = \mathrm{GL}(2, \mathbb{C})$, $g = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$;

в) $G = S_6$, $g = (32651)$; г) $G = \mathbb{C}^*$, $g = 2 - i$;

д) $G = \mathbb{R}^*, g = 10$; е) $G = \mathbb{C}^*$, $g = \cos\frac{6}{5}\pi + i\sin\frac{6}{5}\pi$;

ж) $G = \mathbb{Z}$, $g = 3$?

4.11. Найдите смежные классы:

а) группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$, где n — натуральное число;

б) группы $\mathbb{C}$ по подгруппе $\mathbb{Z}[i]$ целых гауссовых чисел;

в) группы $\mathbb{R}$ по подгруппе $\mathbb{Z}$;

г) группы $\mathbb{C}$ по подгруппе $\mathbb{R}$;

д) группы $\mathbb{C}^*$ по подгруппе чисел с модулем 1;

е) группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^*$;

ж) группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^*_+$;

з) группы подстановок S_n по стационарной подгруппе элемента n;

и) аддитивной группы всех многочленов степени не выше 5 с комплексными коэффициентами по подгруппе многочленов степени не выше 3;

к) циклической группы $\langle a\rangle$ порядка 6 по подгруппе $\langle a^4\rangle$.

4.12. Пусть $g \in \mathrm{GL}(n,\mathbb{C})$ и $H = \mathrm{SL}(n,\mathbb{C})$. Смежный класс gH состоит из всех матриц $a \in \mathrm{GL}(n,\mathbb{C})$, определитель которых равен определителю матрицы g.

4.13. Пусть x, y — элементы группы G и $A,\ B$ — подгруппы в G. Свойства: а) $xA \subseteq yB$ и б) $A \subseteq B$ и $y^{-1}x \in B$ эквивалентны.

4.14. Пусть K — правый смежный класс группы G по подгруппе H. Тогда если $x,\ y,\ z \in K$, то $xy^{-1}z \in K$.

4.15. Пусть K — непустое подмножество в группе G, причем, если $x,\ y,\ z \in K$, то $xy^{-1}z \in K$. Тогда K является правым смежным классом группы G по некоторой подгруппе H.

4.16. Пусть $(G,\cdot)$ — группа. Зафиксируем в G элемент x и зададим в G операцию $a \circ b = a \cdot x \cdot b$. Эта операция задает на G новую группу, изоморфную $(G,\cdot)$ (см. 2.14).

4.17. Пусть x, y — элементы группы G и $A,\ B$ — подгруппы в G. Тогда если $xA \cap yB \neq \varnothing$, то это множество является левым смежным классом группы G по подгруппе $A \cap B$.

4.18. 1) Никакая группа не может быть произведением двух своих собственных сопряженных подгрупп.

2) Если в группе G индексы двух ее подгрупп A и B конечны и взаимно просты, то $G = AB$.

4.19. Пусть A и B — подгруппы группы G. Следующие условия равносильны:

а) $AB \subseteq BA$; б) $AB = BA$;

в) AB — подгруппа в G;

г) $Ab \cap Ba \neq \varnothing$ для любых $a \in A$ и $b \in B$.

4.20. Пусть $A,\ B,\ C$ — подгруппы группы G, причем каждая из них содержится в произведении (в некотором порядке) двух других. Тогда $AB = BC = CA$, кроме того, эти произведения являются подгруппами в G.

4.21. Если A, B, H — подгруппы группы G со свойством $G = AB$ и $A \subseteq H$, то $H = A(B \cap H)$.

4.22. Пусть A и B — подгруппы группы G. Тогда различные двойные смежные классы AgB $(g \in G)$ попарно не пересекаются и G разбивается в объединение двойных смежных классов по A и B.

4.23. Найдите все изоморфизмы между группами $\mathbb{Z}_4$ и $\mathbb{Z}_5^*$.

4.24. 1) Всякая группа порядка 6 либо циклическая, либо изоморфна S_3.

2) $\mathbb{Z}_6 \cong \langle a, b \,|\, a^3 = b^2 = e,\ ab = ba\rangle$, а $S_3 \cong \langle a,\ b \,|\, a^2 = b^3 = (ab)^2 = e\rangle \cong \langle a,\ b \,|\, a^2 = b^2 = (ab)^3 = e\rangle$ и S_3 изоморфна группе из 3.10 б).

3) Группа A_4 не содержит подгрупп порядка 6, хотя число 6 делит ее порядок 12.

4.25. Если A — подгруппа группы G и $g \in G$, то $gAg \subseteq A$ в точности тогда, когда $A \cup gA$ — подгруппа в G.

4.26. Пусть G — множество всех пар элементов (a,b), $a \neq 0$, из поля P. На G задана операция $(a,b) \circ (c,d) = (ac,\ ad{+}b)$. Докажите, что G является группой, изоморфной группе всех линейных функций $x \mapsto ax{+}b$ относительно композиции.

4.27. 1) Группа $\mathbb{R}_+^*$ изоморфна группе $\mathbb{R}$.

2) Группа $\mathbb{Q}_+^*$ не изоморфна группе $\mathbb{Q}$.

4.28. Найдите все (с точностью до изоморфизма) группы, каждая из которых изоморфна любой своей неединичной подгруппе.

4.29. Подгруппа H индекса 2 любой группы G содержит квадраты всех элементов из G.

4.30. Группа $\mathbb{C}^*$ изоморфна группе всех невырожденных матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ с вещественными элементами с операцией умножения матриц.

4.31. Группы $\mathbb{Q}_{\pi_1}$ и $\mathbb{Q}_{\pi_2}$ не изоморфны при $\pi_1 \neq \pi_2$.

4.32. Группа $\mathbb{Q}$ не содержит собственных подгрупп конечного индекса, а также максимальных подгрупп.

4.33. Пусть A, B — подгруппы группы G конечного индекса. Тогда:

а) если $A \subseteq B$ и $(B : A) = n$, а $(G : B) = m$, то $(G : A) = nm$;

б) $(A : A \cap B) \leqslant (G : B)$;

в) $(G : A \cap B) \leqslant (G : A)(G : B)$.

В частности, пересечение конечного числа подгрупп конечного индекса — снова подгруппа конечного индекса. Приведите пример бесконечной группы, в которой пересечение всех подгрупп конечного индекса совпадает с единичной подгруппой.

4.34. С точностью до изоморфизма существует лишь конечное число групп данного порядка n.

4.35. Матрицы:

$$\pm E = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm I = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \pm J = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm K = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

относительно умножения образуют группу, изоморфную Q_8.

4.36. Докажите, что $\operatorname{Aut}\mathbb{Z}_{30} \cong \operatorname{Aut}\mathbb{Z}_{15}$.

4.37. Если $|G| > 2$, то $|\operatorname{Aut} G| > 1$.

4.38. Найдите с точностью до изоморфизма группы, которые: а) не имеют, б) имеют только одну, в) имеют только две, г) имеют только три нетривиальные подгруппы.

4.39. Найдите с точностью до изоморфизма конечные группы, которые имеют только одну максимальную подгруппу (только две максимальные подгруппы).

4.40. 1) Группа $\mathrm{SL}(2, \mathbb{C})$ имеет только одну инволюцию.

2) Найдите все инволюции группы $\mathrm{GL}(2, \mathbb{C})$.

4.41. Пусть группа G порождается любыми двумя своими неединичными элементами. Тогда $G \cong \mathbb{Z}_p$ для некоторого простого числа p, или $|G| = 4$.

4.42. Пусть A — группа. Положим $M = \{(a, \varepsilon) \,|\, a \in A, \varepsilon = \pm 1\}$. Зададим на M операцию $*$ следующим образом:

$$(a_1, \varepsilon_1) * (a_2, \varepsilon_2) = (a_1 a_2^{\varepsilon_1}, \varepsilon_1 \varepsilon_2).$$

Докажите, что:

а) $D(A) = (M, *)$ — группа тогда и только тогда, когда группа A коммутативна;

б) если группа A коммутативна, то $D(A) = A_+ \cup A_-$, где $A_+ = \{(a, 1) \,|\, a \in A\}$, $A_- = \{(a, -1) \,|\, a \in A\}$, причем A_+ относительно ограничения на ней операции $*$ есть группа, изоморфная A, а A_- состоит из инволюций;

в) каждый элемент группы $D(A)$ есть либо инволюция, либо произведение двух инволюций;

г) группа $D(A)$ коммутативна тогда и только тогда, когда каждый неединичный элемент группы A есть инволюция;

д) если A и B — коммутативные группы и $A \cong B$, то $D(A) \cong D(B)$.

4.43. Группа G с конечным числом образующих $a_1, \ldots, a_n$ может иметь лишь конечное число подгрупп данного конечного индекса j.

4.44. 1) $S_n = \langle (12), (12\ldots n) \rangle$.

2) Всякая конечная группа может быть вложена в группу с двумя образующими.

5 Гомоморфизмы. Факторгруппы

Отображение $f\colon A \to B$ группы $(A, \circ)$ в группу $(B, \times)$ называется *гомоморфизмом*, если $f(a \circ b) = f(a) \times f(b)$ для всех $a, b \in A$. *Ядром* гомоморфизма f называется множество $\operatorname{Ker} f = \{a \in A \,|\, f(a) = e\}$, где e — единица группы B. Гомоморфное отображение группы в себя называется ее *эндоморфизмом*.

Подгруппа H группы G называется *нормальной* или *инвариантной* (обозначение $H \trianglelefteq G$), если $H = x^{-1}Hx$ для каждого $x \in G$. Если H — нормальная подгруппа в группе G, то операция $(aH) \cdot (bH) = (ab)H$ определяет на множестве всех левых смежных классов группы G по подгруппе H *факторгруппу* G/H.

Группа G называется *локально нормальной*, если всякое ее конечное подмножество лежит в конечной нормальной подгруппе группы G.

Если M — подмножество, а H — подгруппа группы G, то *нормализатором* M в H называется следующее множество $N_H(M) = \{x \in H \,|\, xM = Mx\}$. Ясно, что подгруппа H нормальна в группе G тогда и только тогда, когда $N_G(H) = G$.

Группа G называется *расширением* группы A при помощи группы B, если в G существует нормальная подгруппа $A' \cong A$ со свойством $G/A' \cong B$.

Теорема 5.1 (основная теорема о гомоморфизмах). *Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Тогда $K = \operatorname{Ker}\varphi$ — нормальная подгруппа в G и $G/K \cong \operatorname{Im}\varphi$. Обратно, если $K \trianglelefteq G$, то существует эпиморфизм $\pi\colon G \to G/K$, ядро которого совпадает с K* (π часто называют *каноническим эпиморфизмом* или *гомоморфизмом*).

Теорема 5.2 (первая теорема об изоморфизме). *Пусть G — группа, H и K — ее подгруппы, причем $K \trianglelefteq G$. Тогда $HK = KH$ — подгруппа в G, содержащая K. Далее, $H \cap K \trianglelefteq H$, а отображение $\varphi\colon hK \mapsto h(H \cap K)$ является изоморфизмом групп: $(HK)/K \cong H/(H \cap K)$.*

Сформулируем лишь облегченный вариант второй теоремы об изоморфизме, носящий специальное название.

Теорема 5.3 (теорема о соответствии). *Пусть G — группа, H и K — ее подгруппы, причем $K \trianglelefteq G$ и $K \subseteq H$. Тогда $\overline{H} = H/K$ — подгруппа в $\overline{G} = G/K$ и $\pi^*\colon H \mapsto \overline{H}$ является биекцией множества $\Omega(G, K)$ подгрупп в G, содержащих K, на множество $\Omega(\overline{G})$ всех подгрупп группы $\overline{G}$. Если $H \in \Omega(G, K)$, то $H \trianglelefteq G$ тогда и только тогда, когда $\overline{H} \trianglelefteq \overline{G}$, причем $G/H \cong \overline{G}/\overline{H} = (G/K)/(H/K)$.*

Доказано, что всякая группа без кручения может быть вложена в группу без кручения с двумя классами сопряженных элементов. Для любого натурального числа $n \geqslant 2$ и любой бесконечной мощности m существует группа мощности m, состоящая ровно из n классов сопряженных элементов.

Неединичная группа называется *простой*, если она не имеет нетривиальных нормальных подгрупп. Все группы A_n при $n \geqslant 5$ являются простыми. Доказано, что всякая простая группа нечетного порядка является циклической из p элементов для некоторого простого числа p. В конце 1980 г. ведущими специалистами было заявлено о завершении классификации конечных простых групп (см. [13]). С помощью этих результатов было доказано, что если в конечной группе сопряжены любые два элемента одного порядка, то порядок группы $\leqslant 6$. Для бесконечных простых групп отметим, что доказано существование таких групп любой бесконечной мощности m, причем множество неизоморфных простых групп мощности m имеет мощность 2^m. Для всякой бесконечной мощности m существует такая простая группа мощности 2^m, в которую изоморфно вкладывается любая группа мощности m. Всякую периодическую группу можно вложить в некоторую простую периодическую группу. Доказано, что существуют простые доупорядочиваемые (см. 9.42) группы.

Задачи

5.1. Подгруппа H группы G нормальна, если:

а) G — коммутативная группа, H — любая ее подгруппа;

б) $G = \mathrm{GL}(n, \mathbb{R})$, $H = \mathrm{SL}(n, \mathbb{R})$;

в) $G = S_n$, $H = A_n$.

5.2. 1) Каждая нормальная подгруппа группы G является объединением некоторого семейства сопряженных классов группы G.

2) Объединение всех конечных классов сопряженных элементов группы является ее нормальной подгруппой.

5.3. Для группы G и ее подгруппы H следующие условия равносильны:

а) H — нормальная подгруппа в G;

б) для любых $a,\ b \in G$ из условия $ab \in H$ следует, что $a^2b^2 \in H$;

в) $H^G \subseteq H$.

5.4. Пусть в группе элемент a сопряжен с b, а элемент c сопряжен с d. Будет ли ac сопряжен с bd?

5.5. В периодической группе никакая подгруппа не может быть сопряжена со своей собственной подгруппой.

5.6. Укажите все пары (m, n) целых чисел, при которых отображение $x \mapsto mx^n$ является эндоморфизмом группы $\mathbb{Q}^*$.

5.7. Пусть G — множество всевозможных троек чисел вида (n, m, ε), где $\varepsilon = \pm 1$. В G определена операция по правилу

$$(n, m, 1)(k, l, \varepsilon) = (n + k, m + l, \varepsilon),$$
$$(n, m, -1)(k, l, \varepsilon) = (n + l, m + k, -\varepsilon).$$

Докажите, что: G является группой; $H_1 = \langle (1, 0, 1),\ (0, 1, 1) \rangle$ — нормальная подгруппа в G, а $H_2 = \langle (1, 0, 1) \rangle$ — нормальная подгруппа в H_1. Будет ли H_2 нормальной подгруппой для G?

5.8. Если произведение двух любых левых смежных классов группы G по подгруппе H снова является левым смежным классом, то H — нормальная подгруппа в G.

5.9. Будет ли нормальной подгруппой в группе $\mathrm{SL}(2, \mathbb{Z})$ подмножество матриц вида $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, где a, d — нечетные, а b, c — четные числа?

5.10. Любая подгруппа индекса 2 нормальна.

5.11. 1) Если K, H — подгруппы группы G, причем $K \trianglelefteq G$ и $K \subseteq H$, то $K \trianglelefteq H$.

2) Покажите, что V_4 является нормальной подгруппой в S_4. Однако нормальная подгруппа $K = \langle (12)(34) \rangle$ группы V_4 не является нормальной в S_4.

5.12. Пусть $A, B \trianglelefteq G$ и $A \cap B = e$. Тогда $ab = ba$ для любых $a \in A$, $b \in B$.

5.13. Приведите примеры:

а) неизоморфных групп с изоморфными нормальными подгруппами и изоморфными факторами по ним;

б) группы с изоморфными нормальными подгруппами, факторгруппы по которым не изоморфны;

в) группы с неизоморфными нормальными подгруппами, факторгруппы по которым изоморфны.

5.14. Отображение $\mathrm{SL}(2,\mathbb{Z}) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f(z) = \frac{az+b}{cz+d}$ является эпиморфизмом на группу унимодулярных дробно-линейных функций. Ядро этого отображения совпадает с центром $\{\pm e\}$ группы $\mathrm{SL}(2,\mathbb{Z})$, где e — единичная матрица. Группа $\mathrm{SL}(2,\mathbb{Z})$ порождается матрицами $u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $v = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ и $-e = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Так как $u^2 = v^3 = -e$, то $\mathrm{SL}(2,\mathbb{Z}) \cong \langle u, v \,|\, u^4 = e,\, u^2 = v^3 \rangle$.

5.15. Ядро любого гомоморфизма группы $\mathbb{C}^*$ в группу $\mathbb{R}$ является бесконечным.

5.16. Если $a \in G$, то отображение $G \ni x \mapsto a^{-1}xa$ является автоморфизмом группы G, он называется *внутренним автоморфизмом* группы G, производимым элементом a. Множество всех внутренних автоморфизмов $\mathrm{Inn}\, G$ является нормальной подгруппой в группе $\mathrm{Aut}\, G$.

5.17. Для каких групп G отображение $f\colon G \to G$, определенное правилом: $f(x) = x^n$, $n \in \mathbb{Z}$, является эндоморфизмом? При каком условии оно будет автоморфизмом?

5.18. Какие из отображений $f\colon \mathbb{C}^* \to \mathbb{R}^*$, $f(z) = |z|^n$, $n \in \mathbb{Z}$, являются гомоморфизмами?

5.19. Если группа G гомоморфно отображается на группу H и $a \mapsto h$, то: $o(a)$ делится на $o(h)$, причем в случае конечности групп порядок группы G делится на порядок группы H.

5.20. Группа H является гомоморфным образом конечной циклической группы G тогда и только тогда, когда H также циклическая, и ее порядок делит порядок группы G. Найдите все гомоморфные отображения:

а) $\mathbb{Z}_6 \to \mathbb{Z}_6$; б) $\mathbb{Z}_6 \to \mathbb{Z}_{18}$; в) $\mathbb{Z}_{18} \to \mathbb{Z}_6$; г) $\mathbb{Z}_{12} \to \mathbb{Z}_{15}$; д) $\mathbb{Z}_6 \to \mathbb{Z}_{25}$.

5.21. 1) Отображение $2^k \cdot \frac{m}{n} \mapsto k$, где $\{k, m, n\} \subseteq \mathbb{Z}$ и m, n нечетные, есть гомоморфизм группы $\mathbb{Q}^*$ на группу $\mathbb{Z}$.

2) Какая из групп $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}^*$ и $\mathbb{Q}^*$ может быть гомоморфно отображена на конечную неединичную группу?

5.22. Группы $\mathbb{R}$ и $\mathbb{Q}$ нельзя гомоморфно отобразить на группу $\mathbb{Z}$.

5.23. Найдите факторгруппы: $\mathbb{Z}/n\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $\mathbb{R}^*/\mathbb{R}^*_+$.

5.24. Докажите,что:

а) $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \cong \mathbb{R}^*$; б) $\mathrm{GL}(n,\mathbb{C})/\mathrm{SL}(n,\mathbb{C}) \cong \mathbb{C}^*$;

в) $\mathrm{GL}(n,\mathbb{R})/H \cong \mathbb{Z}_2$, где $\mathrm{H} = \{A \in \mathrm{GL}(n,\mathbb{R}) \,|\, \det A > 0\}$;

г) $\mathrm{GL}(n,\mathbb{R})/N \cong \mathbb{R}^*_+$, где $N = \{A \in \mathrm{GL}(n,\mathbb{R}) \,|\, \det A = \pm 1\}$.

5.25. Докажите, что:

а) $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ не является нормальной подгруппой в $\mathrm{GL}(2,\mathbb{R})$;

б) $A = \{X \in \mathrm{GL}(2,\mathbb{R}) \,|\, \det X = \pm 1\} \trianglelefteq \mathrm{GL}(2,\mathbb{R})$.

5.26. а) Образует ли $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, 0 \neq a \in \mathbb{R} \right\}$ нормальную подгруппу в $\mathrm{GL}(2,\mathbb{R})$?

б) Является ли подгруппа $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$ нормальной в $\mathrm{GL}(2,\mathbb{R})$?

5.27. Если A и B — конечные группы взаимно простых порядков и $\varphi\colon A \to B$ — гомоморфизм, то $\mathrm{Ker}\, \varphi = A$.

5.28. Эпиморфный образ нормальной подгруппы — нормальная подгруппа.

5.29. Если H – такая подгруппа группы G, что $\varphi(H) \subseteq H$ для каждого $\varphi \in \mathrm{Aut}\, G$, то H — нормальная подгруппа.

5.30. Пересечение любого семейства, произведение конечного числа, а также подгруппа, порожденная любым семейством, нормальных подгрупп является нормальной подгруппой.

5.31. Если $H \trianglelefteq G$ и $(G : H) = n$, то H содержит все элементы из G, порядки которых взаимно просты с n.

5.32. Пусть H — множество всех чисел из $\mathbb{C}^*$, лежащих на вещественных и мнимых осях. Тогда H — подгруппа группы $\mathbb{C}^*$ и $\mathbb{C}^*/H \cong U$, где U — мультипликативная группа всех комплексных чисел с модулем 1.

5.33. Докажите, что $\mathbb{Q}^{(p)}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Q}_p \cong \mathbb{Z}_{p^\infty}$.

5.34. Каковы конечные группы, имеющие только два класса сопряженных элементов?

5.35. Если H — максимальная нормальная подгруппа в конечной группе G, то $(G : H)$ — простое число.

5.36. 1) Четверная группа V_4 служит нормальной подгруппой в A_4. Следовательно, A_4 не является простой группой.

2) $S_4/V_4 \cong S_3$.

3) В группе кватернионов Q_8 (а также в $\mathbb{Z}_2 \times Q_8$) любая подгруппа является нормальной.

5.37. Опишите конечные группы, все собственные подгруппы которых имеют простые порядки.

5.38. Пусть N и K — нормальные подгруппы группы G со свойством $N \cap K = e$. Тогда если:

а) группы G/N и G/K коммутативны, то и G коммутативна;

б) G/N и G/K — π-группы, где π — некоторое множество простых чисел, то и G — π-группа.

5.39. Если $(G : H) = k$, то подгруппа H содержит нормальную в G подгруппу, индекс которой в G делит $k!$.

5.40. Подгруппа, индекс которой является наименьшим простым делителем порядка группы, нормальна.

Подмножество H группы G называется *нормальным*, если $gH = Hg$ для всех $g \in G$.

5.41. Нормальность подмножества H группы G равносильна как равенству $N_G(H) = G$, так и такому условию, что H есть объединение некоторого семейства классов сопряженных элементов группы G.

Если в группе G все классы сопряженных элементов конечны, то говорят, что G — *группа с конечными классами*, такие группы называют еще *FC-группами*.

5.42. 1) Если в группе G дано конечное нормальное подмножество M, состоящее из элементов конечного порядка, то подгруппа, порожденная этим подмножеством, будет конечной.

2) Периодическая группа является FC-группой тогда и только тогда, когда она — локально нормальная.

3) Периодическая часть $t(G)$ FC-группы G является вполне инвариантной подгруппой в G, причем $t(G)$ конечна, если группа G конечно порожденная.

4) Если G — FC-группа, то факторгруппа $G/t(G)$ коммутативна.

5) Группа без кручения является FC-группой тогда и только тогда, когда она коммутативна.

Пусть G — группа с порождающим множеством X. Говорят, что G *порождается множеством X свободно* или что G есть *свободная группа со свободным порождающим множеством X*, если G обладает следующим «свойством универсальности»: каждая функция из X в произвольную группу H единственным образом продолжается до гомоморфизма $G \to H$. Мощность множества X называется *рангом* этой свободной группы G (ранг определяется однозначно), группа G часто обозначается через $F(X)$. Всякая подгруппа свободной группы сама свободна.

5.43. 1) Если $|X| = 1$, то $F(X) \cong \mathbb{Z}$, а если $|X| > 1$, то группа $F(X)$ некоммутативна.

2) В свободной группе ранга $n \geqslant 2$ существуют подгруппы (все они свободные) любого конечного ранга.

3) Любая группа, обладающая порождающим множеством мощности m, является гомоморфным образом свободной группы ранга m.

6 Центр и коммутант. Прямые произведения. Силовские подгруппы

Центром $Z(G)$ группы G называется следующее множество ее элементов $Z(G) = \{z \in G \,|\, zg = gz, g \in G\}$. Любая подгруппа центра является нормальной подгруппой в G. Пусть M — подмножество, H — подгруппа группы G. *Централизатором* M в H называется множество тех элементов из H, которые переставимы с M поэлементно, т.е. $C_H(M) = \{x \in H \,|\, xm = mx,\ m \in M\}$. Ясно, что $C_H(M) \subseteq N_H(M)$, а если M — одноэлементное множество, то его нормализатор и централизатор в H совпадают. Централизатор всей группы совпадает с ее центром.

Коммутатором элементов $a, b \in G$ группы G называют произведение $[a, b] = a^{-1}b^{-1}ab$. Коммутаторы всех элементов группы G порождают подгруппу G' — *коммутант* группы G. Коммутант от коммутанта называют *вторым коммутантом* группы G и обозначают $G^{(2)}$. Ясно, что $G^{(1)} = G'$, $G^{(n)} = (G^{(n-1)})'$.

Доказано, что коммутант свободной группы конечного ранга $n > 1$ является свободной группой счетного ранга.

Если A и B — подмножества группы G, то подгруппа $\langle [a,b] \,|\, a \in A,\, b \in B\rangle$ называется *взаимным коммутантом* A и B и обозначается через $[A,B]$. При $n \geqslant 3$ для подмножеств $A_1, \ldots, A_n \subseteq G$ полагают $[A_1, \ldots, A_n] = [[A_1, \ldots, A_{n-1}], A_n]$.

Если A и B — произвольные группы, то через $G = A \times B$ обозначают множество $\{(a,b) \,|\, a \in A,\, b \in B\}$, с операцией $(a,b)(a_1,b_1) = (aa_1, bb_1)$. Группу G называют (*внешним*) *прямым произведением* групп A и B. Это понятие легко распространяется на произвольное конечное число сомножителей. Подгруппа H из $G = G_1 \times \ldots \times G_n$, проекция которой на любой множитель G_i совпадает с G_i, называется *подпрямым произведением* групп $G_1, \ldots, G_n$.

Если A и B — подгруппы группы G такие, что $G = AB$, $A \cap B = e$ и $A \trianglelefteq G$, $B \trianglelefteq G$, то группу G называют (*внутренним*) *прямым произведением подгрупп* A *и* B. Внешнее прямое произведение $A \times B$ является также внутренним произведением подгрупп $A \times e$ и $e \times B$. Из контекста обычно бывает ясно, какое прямое произведение подразумевается. Поэтому в обоих случаях употребляется обозначение $G = A \times B$. Если $G = \langle G_1, \ldots, G_n\rangle$ и $G_j \cap \langle G_i \,|\, i \neq j\rangle = e$ для всех j, то говорят о внутреннем прямом произведении $G = G_1 \times \ldots \times G_n$ для произвольного числа n нормальных подгрупп G_i группы G. То же самое выражается следующим свойством: G — прямое произведение своих нормальных подгрупп $G_1, \ldots, G_n$, если каждый элемент $g \in G$ допускает единственную запись в виде $g = g_1 \ldots g_n$, где $g_i \in G_i$.

Пусть A — нормальная подгруппа группы G. Если $G = AB$ для некоторой подгруппы $B \subseteq G$ со свойством $A \cap B = e$, то G называется *полупрямым произведением* A и B с нормальным множителем A. В этом случае пишут $G = A \leftthreetimes B$ или $G = B \rightthreetimes A$.

Если $\Phi = \operatorname{Aut} G$, то множество пар φg, $\varphi \in \Phi$, $g \in G$, умножаемых по правилу $\varphi g \cdot \varphi_1 g_1 = \varphi\varphi_1 g^{\varphi_1} g_1$, образует группу $\operatorname{Hol} G$, называемую *голоморфом* группы G. Отображения $\Phi \to \operatorname{Hol} G$, $G \to \operatorname{Hol} G$ по правилам $\varphi \to \varphi e$, $g \to 1g$ вкладывают Φ и G в $\operatorname{Hol} G$. После этого отождествления $\operatorname{Hol} G = \Phi \rightthreetimes G$ и всякий автоморфизм подгруппы G в $\operatorname{Hol} G$ является сужением некоторого внутреннего автоморфизма группы $\operatorname{Hol} G$.

Пусть G — конечная группа порядка $p^n m$, где p — простое число, взаимно простое с m. Подгруппу $P \subset G$ порядка $|P| = p^n$ называют *силовской* p*-подгруппой* группы G. Силовские p-подгруппы всегда существуют. Множество всех p-силовских подгрупп группы G обозначается через $\operatorname{Syl}_p(G)$.

Подгруппа H конечной группы G называется *холловой подгруппой* в G, если $|H|$ и $(G:H)$ взаимно просты.

Группа G называется *группой Фробениуса*, если $G = N \leftthreetimes H$, $N \trianglelefteq G$ и $H \cap H^g = e$ для всех $g \in G \setminus H$; N называется *ядром,* а подгруппа H — *дополнительным множителем* группы G.

Задачи

6.1. Пусть $G = \{2^m \cdot 3^n \,|\, m,\ n \in \mathbb{Z}\}$ и $\cdot$ — обычное умножение. Тогда $(G,\cdot)$ — группа и $(G,\cdot) \cong \mathbb{Z} \times \mathbb{Z}$.

6.2. 1) Пусть G — группа и $a,\ b \in G$. Тогда $a^{-n}b^{-n}(ab)^n \in G'$ для любого натурального n.

2) Конечная коммутативная элементарная p-группа изоморфна $\underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n}$ для некоторого n.

6.3. Пусть $G = \langle a,b\rangle$, причем:

а) $a^2 = b^2 = (ab)^4 = e$, тогда $(ab)^2 \in Z(G)$;

б) $bab = a$, тогда $a^2 \in Z(G)$.

6.4. Пусть H, B — подгруппы группы G. Тогда H^g будет подгруппой группы G для каждого $g \in G$, а $H_G = \bigcap\limits_{g \in G} g^{-1}Hg$ является наибольшей нормальной подгруппой группы G, содержащейся в H. Кроме того, $B_G \cap H_G = (B \cap H)_G$.

6.5. Если H и B — подгруппы группы G и $H \subsetneqq B$, то $N(B \setminus H) = N(H) \cap N(B)$.

6.6. Пусть A, B — подгруппы группы G и $g \in G$. Тогда:

а) $(A \cup B)^g = A^g \cup B^g$; б) $(A \cap B)^g = A^g \cap B^g$;

в) $(A \setminus B)^g = A^g \setminus B^g$; г) $(AB)^g = A^g B^g$;

д) $(A^{-1})^g = (A^g)^{-1}$; е) $\langle A\rangle^g = \langle A^g\rangle$;

ж) $N_B(A)^g = N_{B^g}(A^g)$; з) $C_B(A)^g = C_{B^g}(A^g)$;

и) если $A \subseteq B$, то $(B^g : A^g) = (B : A)$.

6.7. Пусть M — максимальная подгруппа группы G. Тогда для любой подгруппы $A \subseteq G$ либо $Z(A) \subseteq M$, либо $Z(M) \cap A \trianglelefteq G$.

6.8. $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $A_4 = V_4 \leftthreetimes \langle(123)\rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \leftthreetimes \mathbb{Z}_3$, $S_n \cong A_n \leftthreetimes \mathbb{Z}_2$, $S_4 = V_4 \leftthreetimes S_3 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \leftthreetimes (\mathbb{Z}_3 \leftthreetimes \mathbb{Z}_2)$.

6.9. Централизатор нормальной подгруппы сам является нормальной подгруппой.

6.10. Пусть G — конечная группа и $a \in G$. Тогда:

а) нормализатор $N(a)$ является подгруппой в G, причем подгруппа $\langle a\rangle$ нормальна в $N(a)$;

б) число элементов группы G, сопряженных с a, равно $(G : N(a))$;

в) если H — подгруппа в G, то она нормальна в $N(H)$;

г) число подгрупп группы G, сопряженных с H, равно $(G : N(H))$;

д) число элементов (подгрупп) группы G, сопряженных с данным элементом (данной подгруппой), делит порядок группы G.

6.11. Чему равен порядок прямого произведения (элемента прямого произведения) конечных групп?

6.12. Пусть $H \trianglelefteq (A \times B)$, причем $H \cap A = H \cap B = e$. Тогда $H \subseteq Z(A \times B)$.

6.13. Найдите коммутатор невырожденных матриц:

а) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$;

б) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ и $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$;

в) $\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$ и $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

6.14. 1) $[a, G] = [G, a] \trianglelefteq G$ для любого элемента a группы G.

2) $[a, b^{-1}, c]^b [b, c^{-1}, a]^c [c, a^{-1}, b]^a = e$ для любых a, b, $c \in G$.

6.15. Пусть A, B, C — подгруппы группы G.

1) Если $[A, B] \subseteq Z(G)$, то $[A, B'] = [A', B] = e$.

2) Если H — нормальная подгруппа в G, содержащая два из коммутантов $[A, B, C]$, $[B, C, A]$, $[C, A, B]$, то и третий лежит в H (лемма о трех коммутантах).

6.16. Пусть H — подгруппа группы G.

1) $H \subseteq Z(G)$ тогда и только тогда, когда $[H, G] = e$.

2) $H \trianglelefteq G$ тогда и только тогда, когда $[H, G] \subseteq H$.

6.17. Пусть G — конечная группа такая, что $(G : Z(G))^2 < |G'|$. Тогда G' имеет элементы, не являющиеся коммутаторами.

6.18. Пусть $G = \langle X\rangle$ и $N \trianglelefteq G$. Тогда если коммутатор любых двух элементов из X лежит в N, то $G' \subseteq N$.

6.19. Пусть $N \trianglelefteq G$ и $[N, G'] = e$. Тогда $C_N(g) \trianglelefteq G$ для любого $g \in G$.

6.20. Пусть $G = A \leftthreetimes B$ и A_1 — подгруппа в группе A. Тогда если B централизует A_1, то $[A, B] \subseteq C_A(A_1)$.

6.21. Пусть $G = A \leftthreetimes B$. Тогда $G' = (A \cap G') \leftthreetimes (B \cap G')$ и $B \cap G' = B'$.

6.22. Конечная группа, у которой нормализаторы некоторых двух ее силовских подгрупп имеют взаимно простые порядки, совпадает со своим коммутантом.

6.23. 1) Каждый элемент группы A_5 есть коммутатор.

2) Каждый элемент коммутанта группы матриц $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $a \neq 0$, над полем есть коммутатор.

6.24. Любая подгруппа, содержащая коммутант группы, нормальна. Факторгруппа G/G' коммутативна, и G' содержится в каждой нормальной подгруппе K, такой, что G/K коммутативна. В частности, максимальный порядок коммутативной факторгруппы группы G равен индексу $(G : G')$.

6.25. 1) Коммутант группы состоит из всевозможных конечных произведений коммутаторов элементов группы.

2) Если $f\colon A \to B$ — гомоморфизм групп, то $f(A') \subseteq B'$, причем $f(A') = B'$, если f — эпиморфизм.

3) Если $H \trianglelefteq G$, то $H' \trianglelefteq G$.

6.26. Установите биективное соответствие между гомоморфизмами группы в коммутативные группы и гомоморфизмами ее факторгруппы по коммутанту.

6.27. Пусть коммутатор $[a, b]$ перестановочен с элементом a. Тогда:

а) $[a^n,\ b] = [a,\ b]^n$ для любого целого n;

б) если $o(a) < \infty$, то $o([a,\ b]) < \infty$, причем $o([a,\ b])$ делит $o(a)$.

6.28. 1) Если $G = G'$, то $|Z(G/Z(G))| = 1$.

2) Если $a \in G$ и $\langle a\rangle \trianglelefteq G$, то $G' \subseteq C_G(a)$.

3) Если G — конечная группа и $\langle g^G\rangle \neq G$ для всех $g \in G$, то $G' \neq G$.

6.29. Пусть в конечной группе порядок коммутанта равен двум. Тогда:

а) коммутант лежит в центре группы;

б) кроме элементов из коммутанта группа обладает и другими элементами четного порядка;

в) индекс коммутанта — четное число.

6.30. Пусть G — множество всех верхних унитреугольных матриц порядка 3 с элементами из поля F_p. Докажите, что G — группа порядка p^3 относительно умножения, найдите ее центр и $\exp(G)$. Если $p = 2$, то какой группе (см. 6.48 2)) она изоморфна?

6.31. Найдите $Z(\mathrm{GL}(n, \mathbb{R}))$ и $Z(\mathrm{O}(2, \mathbb{R}))$.

6.32. В группе $\mathrm{GL}(2, \mathbb{R})$ найдите централизаторы матриц:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

6.33. Наряду с централизатором в группе G рассматривают еще *косой централизатор* $D(a) = \{x \in G \,|\, xa = a^{-1}x\}$. Докажите, что:

а) $D(a)$ — группа тогда и только тогда, когда $a^2 = e$ и $D(a) = C(a)$;

б) множество $E(a) = C(a) \cup D(a)$ всегда является группой.

6.34. Какие из трех матриц сопряжены между собой в группе $\mathrm{GL}(2, \mathbb{C})$:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix},\ C = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}?$$

6.35. 1) Если H и K — сопряженные подгруппы конечной группы и $K \subseteq H$, то $K = H$.

2) Подгруппы $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$, $K = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$ сопряжены в группе $\mathrm{GL}(2, \mathbb{R})$ и $K \subset H$.

3) Если G — подпрямое произведение конечных групп, то G является локально нормальной группой.

6.36. 1) Силовская p-подгруппа группы G единственна тогда и только тогда, когда она нормальна в G.

2) Эпиморфный образ силовской p-подгруппы конечной группы является силовской p-подгруппой.

3) Силовская p-подгруппа прямого произведения конечных групп A и B изоморфна прямому произведению силовских p-подгрупп сомножителей A и B.

4) $Z(A \times B) \cong Z(A) \times Z(B)$.

5) Если P — силовская p-подгруппа конечной группы G, H — нормальная подгруппа в G, то $P \cap H$ является силовской p-подгруппы группы H.

6) Коммутант прямого произведения изоморфен прямому произведению коммутантов сомножителей.

7) Если K — поле, то коммутант группы $\mathrm{GL}(n, K)$ содержится в $\mathrm{SL}(n, K)$.

8) Конечная группа является p-группой тогда и только тогда, когда ее порядок равен p^n для некоторого натурального числа n.

6.37. 1) Если $|G| = pq$, где p, q — простые числа, причем $p > q$, то силовская p-подгруппы группы G нормальна в G.

2) Все силовские подгруппы группы порядка 100 коммутативны.

3) Любая группа порядка 15, 35, 185, 255 коммутативна.

4) Не существует простых групп порядка 36, 80, 56, 196, 200.

5) Каждая группа порядка pq^2, где p, q — различные простые числа, имеет нормальную силовскую подгруппу.

6) Если p, q — простые числа, $p < q$ и $q - 1$ не делится на p, то любая группа порядка pq коммутативна, если же $q - 1$ делится на p, то имеется некоммутативная группа порядка pq.

6.38. Сколько различных силовских 2-подгрупп и силовских 5-подгрупп в некоммутативной группе порядка 20?

6.39. 1) Группа внутренних автоморфизмов группы G изоморфна факторгруппе группы G по ее центру.

2) Факторгруппа некоммутативной группы по ее центру не может быть циклической.

3) Центр некоммутативной группы не может быть максимальной подгруппой.

4) Центр группы порядка p^n, где p — простое число, содержит более одного элемента.

5) Во всякой неединичной конечной p-группе коммутант отличен от самой группы.

6) Группа порядка p^2, где p — простое число, коммутативна, и есть либо циклическая группа, либо прямое произведение двух циклических групп порядка p.

7) В некоммутативной группе порядка p^3 центр совпадает с коммутантом и имеет порядок p, а все собственные подгруппы коммутативны.

8) При $p \neq 2$ некоммутативная группа порядка p^3 с $\exp(G) = p^2$ представима в виде $G = \langle a\rangle \leftthreetimes \langle b\rangle$, где $o(a) = p^2$, $o(b) = p$ и $a^b = a^{1+p}$ (ср. с 6.66).

6.40. Пусть H — нормальная подгруппа в конечной p-группе G. Тогда $H \cap Z(G) \neq e$. В частности, если порядок H прост, то $H \subseteq Z(G)$.

6.41. Если P — силовская p-подгруппа конечной группы G, и H — подгруппа в G, содержащая нормализатор $N(P)$, то $N(H) = H$.

6.42. Найдите число классов сопряженности и число элементов в каждом классе для некоммутативной группы G порядка p^3, где p — простое число.

6.43. Пересечение любых двух различных максимальных коммутативных подгрупп содержится в центре группы.

6.44. Пусть в конечной группе G для каждого простого числа p, делящего порядок группы, существует лишь единственная силовская p-подгруппа. Тогда элементы из различных силовских p-подгрупп переставимы между собой; кроме того, $Z(G) \neq e$.

6.45. Если группа G имеет только одну инволюцию t, то $t \in Z(G)$.

6.46. 1) Группа D_n симметрий правильного n-угольника (см. 3.44) изоморфна группе $\langle a,\ b \,|\, a^n = b^2 = (ab)^2 = e\rangle$. Группа, изоморфная группе D_n для некоторого n, называется *конечной группой диэдра*.

2) $|D_n| = 2n$. Если $m > 1$, то

при $n = 2m$, $D'_n = \langle a^2\rangle$, $(D_n : D'_n) = 4$, $Z(D_n) = \langle a^m\rangle$, $r = m + 3$,

1	1	2	…	2	m	m
e	a^m	a	…	a^{m-1}	b	ab

;

при $n = 2m + 1$, $D'_n = \langle a\rangle$, $(D_n : D'_n) = 2$, $Z(D_n) = e$, $r = m + 2$,

1	2	…	2	2	n
e	a	…	a^{m-1}	a^m	b

.

Здесь r — число классов сопряженности; в нижних строках таблиц стоят представители сопряженных классов, в верхних строках — мощности этих классов.

Нетривиальные гомоморфные образы группы D_n исчерпываются группами $\mathbb{Z}_2$ и D_k, где $k \,|\, n$ и $k \neq 1, n$.

3) D_n изоморфна мультипликативной группе матриц вида $\left\{ \begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} \,\middle|\, k \in \mathbb{Z}_n \right\}$, которая изоморфна группе $D(\mathbb{Z}_n)$ (определение см. 4.42).

4) Группа $D(\mathbb{Z})$ (и всякая ей изоморфная) называется *бесконечной диэдральной* группой, $D(\mathbb{Z})$ изоморфна мультипликативной группе матриц вида $\left\{ \begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} \,\middle|\, k \in \mathbb{Z} \right\}$ и имеет представление $\langle a,\ b \,|\, b^2 = e,\ ba = a^{-1}b\rangle$; $Z(D(\mathbb{Z})) = e$, $D(\mathbb{Z})' \cong \mathbb{Z}$ и $(D(\mathbb{Z}) : D(\mathbb{Z})') = 4$.

5) Группа G порождается двумя инволюциями (соответственно, двумя сопряженными инволюциями) в точности тогда, когда $G \cong D(\mathbb{Z}_n)$ или $G \cong D(\mathbb{Z})$ (соответственно, $G \cong D(\mathbb{Z}_n)$ для некоторого нечетного n).

6.47. 1) $Q_8 \cong \langle a,\ b \,|\, a^4 = e,\ \ b^2 = a^2,\ \ bab^{-1} = a^{-1}\rangle \cong \langle a,\ b \,|\, ab = b^{-1}a,\ \ ba = a^{-1}b\rangle$.

2) $|Q_8| = 8,\ \ \langle a^2\rangle = Z(Q_8) = Q'_8$.

3) Хотя $|D_4| = 8$, но $D_4 \ncong Q_8$. Сведения о сопряженных классах содержатся в таблице:

1	1	2	2	2
e	a^2	a	b	ab

.

4) Множество

$$P = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \pm \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

матриц над F_3 составляет группу, изоморфную группе Q_8 и являющуюся нормальной силовской 2-подгруппой в $\mathrm{SL}(2, F_3)$.

6.48. 1) Пусть $G = \langle a, b \rangle$, где $a^{-1}ba = b^{-1}$ и $b^{-1}ab = a^{-1}$. Тогда $a^4 = b^4 = e$ и G изоморфна $\mathbb{Z}_2 \times \mathbb{Z}_2$ или Q_8.

2) Опишите с точностью до изоморфизма все группы порядка: а) 4; б) 6; в) 8; г) 9; д) 10.

6.49. 1) Если $N \trianglelefteq G$ и $N \cap G' = e$, то $N \subseteq Z(G)$ и $Z(G/N) = Z(G)/N$.

2) Всякая минимальная нормальная подгруппа группы G содержится либо в G', либо в $Z(G)$.

6.50. Пусть H — холлова подгруппа группы G. Тогда:

1) условие $H \trianglelefteq G$ равносильно тому, что H — единственная подгруппа порядка $|H|$ в G;

2) G p-замкнута в том и только в том случае, когда G имеет нормальную силовскую p-подгруппу;

3) если $H \trianglelefteq K \trianglelefteq G$, то $H \trianglelefteq G$;

4) если $H \trianglelefteq G$ и K — подгруппа в G, то:

   а) $|H|$ делит $|K|$, если и только если H — подгруппа в K,

   б) $|K|$ делит $|H|$, если и только если K — подгруппа в H.

6.51. Пусть H — подгруппа группы G.

1) Из $P \in \mathrm{Syl}_p(G)$ не следует, что $H \cap P \in \mathrm{Syl}_p(H)$.

2) Силовская подгруппа из G не может содержать две силовские подгруппы из H.

6.52. Пусть $P \in \mathrm{Syl}_p(G)$ и $n = (G : P)$. Если ни один отличный от 1 и n делитель числа n не сравним с 1 по модулю p, то либо $P \trianglelefteq G$, либо P максимальна в G.

6.53. Каждая группа порядка $2^2 \cdot 5^2$, $2^3 \cdot 5^2$, $2^3 \cdot 7$, $2^2 \cdot 7^2$, $3^3 \cdot 5$, $5^4 \cdot 7$, $7 \cdot 11 \cdot 13$ или $2^2 \cdot 7 \cdot 23$ имеет нормальную силовскую подгруппу.

6.54. Если в конечной группе G для любого делителя m порядка группы G уравнение $x^m = e$ имеет не больше m решений, то группа G циклическая.

6.55. Число подгрупп порядка p в группе S_p равно $(p-2)!$. В частности, $(p-2)! \equiv 1 \pmod p$.

6.56. Пусть P — подгруппа верхних унитреугольных матриц в $\mathrm{GL}(2, F_p)$.

1) Докажите, что P — силовская p-подгруппа в $\mathrm{SL}(2, F_p)$ и в $\mathrm{GL}(2, F_p)$.

2) Найдите нормализатор подгруппы P в $\mathrm{SL}(2, F_p)$ и в $\mathrm{GL}(2, F_p)$.

3) Найдите число различных силовских p-подгрупп в $\mathrm{SL}(2, F_p)$ и в $\mathrm{GL}(2, F_p)$.

6.57. Пусть q — степень простого числа p, F_q — поле из q элементов. Найдите порядок групп $\mathrm{GL}(n, F_q)$ и $\mathrm{SL}(n, F_q)$. Докажите, что подгруппа верхних унитреугольных матриц является силовской p-подгруппой в $\mathrm{GL}(n, F_q)$ и $\mathrm{SL}(n, F_q)$.

6.58. Пусть $G = AB$, где A и B — подгруппы группы G. Покажите, что:

а) существует силовская p-подгруппа P в A и силовская p-подгруппа Q в B такие, что $PQ \in \mathrm{Syl}_p(G)$;

б) если A_1 — нормальная p-подгруппа из A и B_1 — нормальная p-подгруппа из B, то $\langle A_1, B_1 \rangle$ — p-группа.

6.59. Пусть $G = A \times B$, где A и B — подгруппы группы G. Тогда если $P \in \mathrm{Syl}_p(G)$, то $AP \cap BP = P$.

6.60. Пусть G_1 и G_2 — конечные группы, G_1 имеет n_1 силовских p-подгрупп, G_2 имеет n_2 силовских p-подгрупп (p фиксировано). Сколько силовских p-подгрупп имеет группа $G_1 \times G_2$?

6.61. 1) Если N — пересечение всех максимальных подгрупп группы G, порядки которых делятся на p, то N p-замкнута.

2) Каждая силовская подгруппа из подгруппы Фраттини $\Phi(G)$ нормальна в ней.

6.62. Пусть $n \geqslant 2$ и K — поле. Тогда:

а) $\mathrm{GL}(n, K) = \mathrm{SL}(n, K) \leftthreetimes F$, где $F \cong K^*$;

б) $Z(\mathrm{GL}(n, K)) = \{ke \mid k \in K^*\} \cong K^*$, где e — единичная матрица;

в) $Z(\mathrm{SL}(n,\,K)) = Z(\mathrm{GL}(n,\,K)) \cap \mathrm{SL}(n,\,K)$;

г) $\mathrm{GL}(n,\,K)' = \mathrm{SL}(n,\,K)$, если $|K| > 2$ или $n > 2$;

д) $\mathrm{SL}(n,\,K)' = \mathrm{SL}(n,\,K)$, если $|K| > 3$ или $n > 2$.

6.63. Пусть $G = G_1 \times \ldots \times G_n$ — прямое произведение подгрупп G_i. Тогда если $N \trianglelefteq G$ и $N' = N$, то $N = (N \cap G_1) \times \ldots \times (N \cap G_n)$.

6.64. Пусть $G = N \leftthreetimes H$. Равносильны следующие условия:

а) G — группа Фробениуса с ядром N;

б) ни один неединичный элемент из N не перестановочен ни с одним неединичным элементом из H.

6.65. Опишите все конечные p-группы, имеющие только циклические максимальные подгруппы.

6.66. Следующие условия для конечной p-группы G равносильны:

а) G — некоммутативная группа, все собственные подгруппы которой коммутативны;

б) $|G : Z(G)| = p^2$ и $Z(G) = \Phi(G)$;

в) $G = \langle a,\, b\rangle$ для некоторых $a,\, b \in G$ и $|G'| = p$.

6.67. Пусть q — степень простого числа p, F_q — поле из q элементов. Определите строение централизаторов следующих элементов в группе $G = \mathrm{GL}(2, F_q)$:
$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$, $a \neq 1$; $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \neq 0$.

6.68. Пусть $G = \mathrm{GL}(2,\ F)$, где F — поле. Покажите, что:

а) если $g = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \in G$, то $C_G(g) = \left\{ \begin{pmatrix} x & y \\ ay & x + by \end{pmatrix} \in G \,\middle|\, x, y \in F \right\}$ — коммутативная группа;

б) централизатор в G любого ее нецентрального элемента коммутативен.

6.69. Пусть $G = \mathrm{GL}(2,\ F)$, где F — поле.

1) Определите все инволюции в G (см. 4.40).

2) Подсчитайте число инволюций в G в случае, когда $F = F_q$.

6.70. Покажите, что $\mathrm{Hol}\, G \cong G \times G$, если группа G совершенна.

6.71. Следующие условия для группы G равносильны:

а) G — совершенная группа;

б) всякий раз, когда G — нормальная подгруппа группы A, выполняется $A = G \times C_A(G)$.

6.72. Группа G тогда и только тогда характеристически проста (т.е. G не имеет нетривиальных подгрупп H со свойством $H^f \subseteq H$ для каждого $f \in \mathrm{Aut}\, G$), когда ее группа автоморфизмов является максимальной подгруппой голоморфа группы G.

6.73. Пусть K — любое из колец $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$. Используя, что автоморфизмы аддитивной группы K^+ исчерпываются умножениями из K^*, покажите, что $\mathrm{Hol}\, K^+ \cong \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \,\middle|\, \alpha \in K^*, \beta \in K \right\}$.

6.74. Пусть $G = A \leftthreetimes B$, причем B действует на A точно (т.е. $C_B(A) = e$) и неприводимо (т.е. в A нет собственных B-инвариантных подгрупп). Покажите, что если каждая подгруппа простого порядка из B нормальна в B, то G — группа Фробениуса с ядром A.

6.75. В качестве одного из занимательных приложений кратко остановимся на знаменитой в свое время игре в «15». Эту игру придумал в 70-х годах 19 века американский изобретатель головоломок Сэмюэль Лойд. Успеху головоломки в некоторой степени способствовало напечатанное в газетах объявление о призе в 1000 долларов за решение следующей задачи:

в исходной позиции фишки располагаются по порядку номеров, за исключением двух последних, которые переставлены местами друг с другом (рис. а); передвигая по одной фишке, но, не вынимая их из коробочки, нужно поменять

местами номера 15 и 14 так, чтобы *все* фишки стояли по порядку номеров, а правый нижний угол был свободен (позиция S).

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Рис. а — ловушка Лойда — позиция L

Ажиотаж вокруг игры в «15» начал стихать после того, как головоломкой занялись математики. Элементарная теория групп раскрыла все секреты игры. Действительно, если мысленно заполнить пустое место фишкой 16, то каждое положение игры ассоциируется с перестановкой из S_{16}. Например, рис. б

12	2	1	15
7	9	10	4
11	5	6	8
	14	13	3

Рис. б — магический квадрат

соответствует перестановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 2 & 16 & 8 & 10 & 11 & 5 & 12 & 6 & 7 & 9 & 1 & 15 & 14 & 4 & 13 \end{pmatrix},$$

во второй строке указан номер занимаемого фишкой i-го места.

Несложно доказать, что каким бы способом ни выбрать последовательность взаимных перестановок фишек, превращающих одну заданную расстановку фишек в другую, четность числа перестановок в этой последовательности всегда будет одной и той же. Поэтому правильное расположение достижимо тогда и только тогда, когда соответствующая перестановка четная. В терминах теории групп все позиции в игре «15» разбиваются на две орбиты. Одна орбита содержит правильную расстановку S, другая — ловушку Лойда L. Каждая орбита состоит из $16!/2$ позиций. Определите, какой орбите принадлежит позиция на рис. б.

Практически ровно через сто лет Эрне Рубик предложил новую игру — кубик Рубика. В нашей стране журналы «Квант» и «Наука и жизнь» опубликовали алгоритмы сборки кубика Рубика. В статье В. и С. Залгаллеров «Венгерский шарнирный кубик» в «Кванте» 12 за 1980 год предложен алгоритм сборки кубика, целиком основанный на коммутаторах.

7 Ряды подгрупп. Разрешимые и нильпотентные группы

Цепочка (1): $e = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ вложенных друг в друга подгрупп группы G называется ее *рядом подгрупп*. Число n называется *длиной ряда* (1). Ряд (1) называется:

субнормальным, если $G_i \trianglelefteq G_{i+1}$ для всех $i = 0, \ldots, n-1$;

нормальным, если $G_i \trianglelefteq G$ для всех $i = 0, \ldots, n-1$;

композиционным, если G_i — максимальная нормальная подгруппа в G_{i+1} для всех $i = 0, \ldots, n-1$;

главным, если G_i — максимальная нормальная в G подгруппа из G_{i+1} для всех $i = 0, \ldots, n-1$;

центральным, если $G_i \trianglelefteq G$ и $G_{i+1}/G_i \subseteq Z(G/G_i)$ для всех $i = 0, \ldots, n-1$.

Факторгруппы G_{i+1}/G_i субнормального ряда называются его *факторами*. Подгруппу H группы G, являющуюся членом некоторого ее субнормального ряда, называют *субнормальной подгруппой* группы G и пишут: $H \trianglelefteq\trianglelefteq G$.

Группа G называется:

разрешимой, если она имеет нормальный ряд вида (1) с коммутативными факторами G_{i+1}/G_i $(i = 0, \ldots, n-1)$, наименьшая из длин таких рядов называется ее *ступенью разрешимости*;

сверхразрешимой, если она имеет нормальный ряд с циклическими факторами;

нильпотентной, если она имеет центральный ряд (минимальная из длин таких рядов называется ее *классом* или *ступенью нильпотентности*).

Группа, в которой все конечно порожденные подгруппы нильпотентны, называется *локально нильпотентной*. Известно, что во всякой группе произведение двух нормальных локально нильпотентных подгрупп есть локально нильпотентная подгруппа.

В 1962 году была доказана разрешимость групп нечетного порядка (доказательство заняло 255 с. журнального текста). Кроме того, $p^\alpha q^\beta$-теорема Бернсайда утверждает, что всякая группа порядка $p^\alpha q^\beta$, где p и q — различные простые числа, разрешима.

Пусть G — группа, n — натуральное число. Подгруппы $Z_n(G)$ (n-*й центр* группы G) и $L_n(G)$ (n-*й централ* группы G) определяются индуктивно следующим образом:

$$Z_0(G) = e,\ Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G));$$
$$L_1(G) = G,\ L_{i+1}(G) = [L_i(G), G].$$

Очевидно, $Z_0(G) \subseteq Z_1(G) \subseteq \dots$ и $L_1(G) \supseteq L_2(G) \supseteq \dots$. Первый ряд называется *верхним центральным*, а второй — *нижним центральным*. В нильпотентной группе нижний и верхний ряды обрываются, причем их длины равны ступени нильпотентности группы. Подгруппа $H(G) = \bigcup\limits_{i=1}^{\infty} Z_i(G)$ (другое обозначение $Z_\infty(G)$ или $Z_\omega(G)$) называется *гиперцентром* группы G. Подгруппа $L_\omega = \bigcap\limits_{i=1}^{\infty} L_i(G)$ называется ω-*м централом* группы G.

Важными подгруппами группы G являются:

разрешимый радикал $S(G)$ группы G — подгруппа, порожденная всеми разрешимыми нормальными подгруппами из G;

подгруппа Фиттинга $F(G)$ группы G — подгруппа, порожденная всеми нильпотентными нормальными подгруппами из G;

цоколь $\operatorname{Soc} G$ группы G — подгруппа, порожденная всеми минимальными нормальными подгруппами из G.

Два субнормальных ряда группы называются *изоморфными*, если они имеют равные длины и между их факторами существует взаимно однозначное соответствие, при котором соответственные факторы изоморфны.

Теорема Шрайера утверждает, что любые два субнормальных (нормальных) ряда группы имеют изоморфные субнормальные (нормальные) уплотнения.

Подмножество K группы G называется *скрученным*, если $e \in K$ и $ab^{-1}a \in K$ для любых $a, b \in K$. Группа называется *перекрученной*, если в ней любое скрученное подмножество является подгруппой. Доказано, что конечная группа перекручена тогда и только тогда, когда она представима в виде прямого произведения циклической 2-группы и перекрученной группы нечетного порядка.

Подгруппа H группы G называется *квазинормальной*, если $AH = HA$ для любой подгруппы A группы G.

Через $O_\pi(G)$ обозначается наибольшая нормальная π-подгруппа группы G; а через $O^\pi(G)$ — наибольшая нормальная подгруппа в G, факторгруппа по которой есть π-группа, т.е. подгруппа, порожденная всеми π'-элементами из G, где π' — множество всех простых чисел, не входящих в π.

Задачи

7.1. 1) (Теорема Жордана-Гельдера). Если группа обладает композиционными рядами, то всякие два ее композиционных (соответственно, главных) ряда изоморфны.

2) Если группа обладает композиционными рядами, то всякий ее субнормальный ряд содержится в некотором композиционном ряду и имеет поэтому длину, не превосходящую длины композиционных рядов этой группы.

7.2. Группа разрешима тогда и только тогда, когда она имеет нормальный ряд с коммутативными факторами.

7.3. Пусть G — группа с субнормальным рядом $e = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n \subseteq G$. Тогда:

а) если H — подгруппа в G, то ряд $e = H_0 \subseteq H_1 \subseteq \dots \subseteq H_n \subseteq H$, где $H_i = G_i \cap H$, является субнормальным рядом группы H, причем фактор H_{i+1}/H_i изоморфен подгруппе из G_{i+1}/G_i;

б) если φ — гомоморфизм группы G, то ряд $e = \varphi(G_0) \subseteq \varphi(G_1) \subseteq \dots \subseteq \varphi(G_n) \subseteq \varphi(G)$ есть субнормальный ряд группы $\varphi(G)$, причем $\varphi(G_{i+1})/\varphi(G_i)$ — гомоморфный образ группы G_{i+1}/G_i.

7.4. 1) Коммутант подгруппы содержится в коммутанте группы; выведите отсюда, что всякая подгруппа разрешимой группы разрешима.

2) Если $\varphi\colon A \to B$ — эпиморфизм, то $\varphi(A') = B'$; выведите отсюда, что всякая факторгруппа разрешимой группы разрешима.

3) Если $G/A \cong B$, где A, B — разрешимые группы, то G разрешима.

4) G есть разрешимая группа ступени n, если и только если $G^{(n)} = e$, но $G^{(n-1)} \neq e$ (в этом случае ряд $G \supset G^{(1)} \supset \dots \supset G^{(n)} = e$ называется *рядом коммутантов* группы G).

5) Группы порядка pq, где p, q — различные простые числа, разрешимы.

6) Группы порядков 12, 20, 42, 100 разрешимы.

7) Группы порядка p^n разрешимы.

7.5. Группы порядка p^2q, где p и q — различные простые числа, а также все группы порядка < 60 разрешимы.

7.6. Пусть K — поле, группа верхних унитреугольных матриц, а также группа невырожденных верхних треугольных матриц разрешимы.

7.7. Пусть K — поле, содержащее не менее четырех элементов. Докажите, что группы $\mathrm{SL}(2, K)$ и $\mathrm{GL}(2, K)$ не являются разрешимыми.

7.8. Для группы G равносильны следующие условия:

а) G — нильпотентная группа класса n;

б) $Z_n(G) = G$, но $Z_{n-1}(G) \neq G$;

в) $L_{n+1}(G) = e$, но $L_n(G) \neq e$.

7.9. 1) Всякая нильпотентная группа разрешима.

2) В нильпотентной группе без кручения единица — единственный элемент, сопряженный со своим обратным.

3) Если коммутант некоммутативной группы лежит в ее центре, то группа нильпотентна.

4) Конечная p-группа, где p — простое число, нильпотентна.

5) Существуют пять неизоморфных групп порядка p^3, среди них три — коммутативные.

7.10. 1) Прямое произведение конечного числа разрешимых (нильпотентных) групп разрешимо (нильпотентно).

2) Подгруппа, порожденная квазинормальными подгруппами, квазинормальна. Подгруппа, сопряженная с квазинормальной подгруппой, квазинормальна.

3) Максимальная квазинормальная подгруппа A является нормальной.

4) Если H — квазинормальная подгруппа в конечной группе G, являющаяся p-группой, то $O^p \subseteq N_G(H)$.

7.11. Если G — нильпотентная группа ступени $s \geqslant 2$, то любая ее подгруппа, порожденная коммутантом и одним элементом, имеет ступень нильпотентности меньше s.

7.12. Любая подгруппа нильпотентной группы субнормальна. Более точно, если G — нильпотентная группа ступени s, то для любой ее подгруппы H ряд последовательных нормализаторов достигает G не позже чем через s шагов.

7.13. Пусть G — нильпотентная группа. Тогда:

а) ее подгруппы и факторгруппы нильпотентны;

б) если N — нормальная неединичная подгруппа в G, то $|N \cap Z(G)| > 1$;

в) если факторгруппа G/G' циклическая, то сама группа G циклическая.

7.14. Пусть G — нильпотентная группа. Докажите, что если A — ее подгруппа с условием $AG' = G$, то $A = G$. В частности, $G' \subseteq \Phi(G)$.

7.15. В нильпотентной группе G максимальная коммутативная нормальная подгруппа A совпадает со своим централизатором. В частности, A — максимальная коммутативная подгруппа и G/A изоморфно вкладывается в $\mathrm{Aut}\, A$.

7.16. В нильпотентной группе G ее периодическая часть $t(G)$ является подгруппой.

7.17. В любой нильпотентной группе без кручения G извлечение корней — однозначная операция, т.е. для любых элементов a, b и любого $n \in \mathbb{N}$ из $a^n = b^n$ следует $a = b$.

7.18. В любой нильпотентной группе без кручения условие $x^m y^n = y^n x^m$ $(m, n \in \mathbb{N})$ влечет $xy = yx$.

7.19. Для группы G следующие условия равносильны:

а) G есть нильпотентная группа класса $\leqslant 2$;

б) $G' \subseteq Z(G)$;

в) $[ab, c] = [a, c] \cdot [b, c]$ для любых $a, b, c \in G$;

г) $[a, bc] = [a, b] \cdot [a, c]$ для любых $a, b, c \in G$;

д) $[[a, b], c] = [a, [b, c]]$ для любых $a, b, c \in G$;

е) $[a,b,c]=[a,c,b]$ для любых $a,b,c\in G$.

7.20. Для конечной группы G равносильны условия:

а) G нильпотентна;

б) все подгруппы из G субнормальны в G;

в) все силовские подгруппы из G нормальны в G;

г) $N(H)\supset H$ для любой подгруппы $H\subset G$;

д) каждая максимальная подгруппа из G нормальна в G;

е) $G'\subseteq\Phi(G)$.

7.21. Конечная группа является нильпотентной тогда и только тогда, когда она представима в виде прямого произведения p-групп.

7.22. Пусть G — конечная группа. Тогда:

а) подгруппа Фраттини группы G нильпотентна;

б) если $A\trianglelefteq G$ и $P\in\mathrm{Syl}_p(G)$, то $G=A\cdot N_G(P)$;

в) если A — ее квазинормальная подгруппа, то $A\trianglelefteq\trianglelefteq G$;

г) если A — ее субнормальная π-подгруппа, то $A\subseteq O_\pi(G)$;

д) если A — ее субнормальная разрешимая подгруппа, то A содержится в некоторой разрешимой нормальной в G подгруппе.

7.23. Пусть G — нильпотентная группа класса 2 и $a,\,b\in G$. Тогда:

а) любые два сопряженных элемента группы G перестановочны;

б) $C_G(a)\trianglelefteq G$ и $G/C_G(a)\cong[a,\,G]$;

в) $[a^n,\,b]=[a,\,b^n]=[a,\,b]^n$ для любого $n\in\mathbb{N}$;

г) если экспонента $\exp(G/Z(G))$ конечна, то она делится на $\exp(G')$.

7.24. В нильпотентной группе класса $\leqslant 3$ коммутант коммутативен.

7.25. Подгруппы и факторгруппы сверхразрешимых групп сверхразрешимы.

7.26. Если G — конечная группа, то:

а) разрешимый радикал $S(G)$ есть разрешимая нормальная подгруппа в G;

б) подгруппа Фиттинга $F(G)$ есть нильпотентная нормальная подгруппа в G.

7.27. Если G — разрешимая группа со свойством $Z(G)\subset G$, то $Z(G)\subset F(G)$.

7.28. Если A и B — конечные группы со свойством $(\,|A|,\,|B|\,)=1$, то $H(A\times B)\cong H(A)\times H(B)$.

7.29. Если $G=G'$, то гиперцентр $H(G)$ совпадает с центром $Z(G)$ группы G.

7.30. Если K — нильпотентная подгруппа группы G, то $KH(G)$ нильпотентна.

7.31. Если G — группа с конечным гиперцентром, $N\trianglelefteq G$ и $N\subseteq H(G)$, то $H(G/N)=H(G)/N$.

7.32. Если G — конечная группа, то гиперцентр $H(G)$ есть пересечение:

а) всех ее максимальных нильпотентных подгрупп;

б) нормализаторов всех ее силовских подгрупп.

7.33. Если группа порождается конечным множеством своих минимальных нормальных подгрупп, то она является прямым произведением некоторых из этих подгрупп.

7.34. Если G — конечная группа, то любая нормальная подгруппа группы G, содержащаяся в $\mathrm{Soc}\,G$, является прямым произведением некоторого множества минимальных нормальных подгрупп группы G.

7.35. Следующие условия для конечной группы G равносильны:

а) для любой нормальной подгруппы N группы G найдется такая подгруппа M в G, что $G = N \times M$;

б) $G = \operatorname{Soc} G$;

в) G является прямым произведением нескольких простых нормальных подгрупп.

Каждая подгруппа в нильпотентной группе субнормальна (см. 7.12). Существуют ненильпотентные группы, все подгруппы которых субнормальны. Более слабым условием по сравнению с субнормальностью всех подгрупп является *нормализаторное условие*: каждая собственная подгруппа отлична от своего нормализатора.

7.36. Всякая группа G с нормализаторным условием локально нильпотентна.

Группа G называется *полной*, если для любого ее элемента g и любого натурального m в G существует решение уравнения $x^m = g$.

7.37. Периодическая часть $t(G)$ полной нильпотентной группы G лежит в ее центре $Z(G)$.

7.38. Для группы G равносильны следующие условия:

а) группа G разрешима;

б) группа G обладает субнормальным рядом с коммутативными факторами;

в) группа G удовлетворяет одному из тождеств

$$\delta_n(x_1, \dots, x_{2^n}) = e \ (n = 0, 1, 2, \dots), \text{ где}$$
$$\delta_0(x) = x, \quad \delta_{n+1}(x_1, \dots, x_{2^{n+1}}) = [\delta_n(x_1, \dots, x_{2^n}), \delta_n(x_{2^n+1}, \dots, x_{2^{n+1}})].$$

Группа, обладающая субнормальным рядом с циклическими факторами, называется *полициклической*.

7.39. Подгруппы и факторгруппы полициклической группы — полициклические. Расширение полициклической группы посредством полициклической группы — снова полициклическая группа. Произведение двух полициклических нормальных подгрупп произвольной группы — полициклическая подгруппа.

7.40. 1) Класс групп с условием максимальности (см. 3.52) замкнут относительно взятия подгрупп, гомоморфных образов и расширений.

2) Группа G тогда и только тогда разрешима и удовлетворяет условию максимальности, когда она полициклическая.

7.41. 1) Всякая конечная группа G является расширением разрешимой группы при помощи группы, не имеющей неединичных разрешимых нормальных подгрупп.

2) Если E — множество инволюций группы, то $K = E \cup \{e\}$ является ее скрученным подмножеством.

3) Пусть $G = \langle a \rangle \times \langle b \rangle$, где $a^2 = b^2 = e$. Тогда $K = \{e, a, b\}$ — скрученное подмножество, не являющееся подгруппой.

4) Если K — скрученное подмножество группы G, то $\langle x \rangle \subseteq K$ для любого $x \in K$.

5) Конечная 2-группа G является перекрученной тогда и только тогда, когда G циклична.

6) Все подгруппы и гомоморфные образы перекрученной группы также являются перекрученными группами.

7) Конечная p-группа G, где p — нечетное простое число, перекручена тогда и только тогда, когда решетка подгрупп группы G — дедекиндова.

8) Среди групп порядка p^3 ($p \neq 2$) только группа, имеющая строение: $(\langle a \rangle \times \langle c \rangle) \leftthreetimes \langle b \rangle$, где $o(a) = o(b) = o(c) = p$, $c = [a, b]$, $bc = cb$, не является перекрученной (ср. с 7.9 5)).

8 Автоморфизмы и эндоморфизмы

На множествах эндоморфизмов $\operatorname{End} G$ и автоморфизмов $\operatorname{Aut} G$ группы G определяют умножение, считая произведением двух эндоморфизмов их последовательное выполнение. Тогда $\operatorname{End} G$ становится полугруппой, а $\operatorname{Aut} G$ группой. Все внутренние автоморфизмы группы G образуют нормальную подгруппу $\operatorname{Inn} G$ в группе $\operatorname{Aut} G$ (5.16). Факторгруппа $\operatorname{Aut} G/\operatorname{Inn} G$ называется *группой внешних автоморфизмов* группы G. Группа G называется *совершенной*, если $\operatorname{Aut} G = \operatorname{Inn} G$ и $Z(G) = e$. Теорема Гельдера утверждает, что *при* $n \neq 2, 6$ *группа* S_n *совершенна.*

Автоморфизм группы G называется *регулярным*, если он оставляет на месте лишь один единичный элемент из G. Автоморфизм группы G называется *нормальным*, если он перестановочен с любым внутренним автоморфизмом.

Пусть $\varphi \in \operatorname{End} G$, говорят, что подгруппа H группы G *φ-инвариантна*, или *φ-допустима*, если $H^\varphi \subseteq H$. Если H допустима относительно всех автоморфизмов (эндоморфизмов) группы G, то H называется *характеристической* (*вполне инвариантной*) *подгруппой* в G.

Если A — подгруппа группы $\operatorname{Aut} G$ и $X \subseteq G$, то используются обозначения: $C_A(X) = \{a \in A \,|\, x^a = x$ для всех $x \in X\}$, $C_G(A) = \{g \in G \,|\, g^a = g$ для всех $a \in A\}$, $[X, A] = \langle x^{-1}x^a \,|\, x \in X,\ a \in A\rangle$, $[A, X] = \langle x^{-a}x \,|\, x \in X,\ a \in A\rangle$. Ясно, что $[X, A] = [A, X]$.

Если $A \subseteq \operatorname{Aut} G$, то говорят, что группа A *стабилизирует* или *централизует* цепь $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = e$, если $[A, G_i] \subseteq G_{i+1}$, $i = 0, \ldots, n-1$; A называют *стабилизатором* данной цепи, если A состоит из всех автоморфизмов группы G с указанным выше свойством.

Если π — некоторое множество простых чисел, то через π' обозначаются все простые числа, не входящие в π.

Пусть P — конечная p-группа. Тогда $cl\, P$ обозначает класс нильпотентности P; $\Omega_i(P) = \langle g \in P \,|\, g^{p^i} = e\rangle$, подгруппа $\Omega_1(P)$ называется *нижним слоем* группы P; $\mho_i(P) = \langle g^{p^i} \,|\, g \in P\rangle$. Если a — наибольший из порядков коммутативных подгрупп в P, то $(P) = \{A \,|\, A$ — подгруппа в P, $A' = e$, $|A| = a\}$. $J(P) = \langle A \,|\, A \in (P)\rangle$ — *подгруппа Томпсона* группы P. $SCN\,(P)$ — множество всех максимальных коммутативных нормальных подгрупп из P.

Тождественный автоморфизм группы G обозначается через 1, также обозначается единичная подгруппа в $\operatorname{Aut} G$.

В этом параграфе помещены также некоторые начальные факты о группах автоморфизмов и кольцах эндоморфизмов для абелевых групп, не требующие специальных знаний об этих группах. Группа автоморфизмов абелевой группы коммутативна лишь в исключительных случаях. Напомним, что в абелевых группах принята аддитивная форма записи групповой операции.

Определим *кольцо эндоморфизмов* $\operatorname{End} A$ аддитивной абелевой группы A. Его элементами являются всевозможные эндоморфизмы группы A, т.е. такие отображения $f\colon A \to A$, что $f(a+b) = f(a) + f(b)$ $(a, b \in A)$. *Сумма* $f + g$, *произведение* fg двух эндоморфизмов f и g есть эндоморфизмы, определяемые, соответственно, правилами: $(f+g)(a) = f(a) + g(a)$, $(fg)(a) = f(g(a))$ для $a \in A$ (говорят, что сложение — «поточечное», а в качестве произведения берется композиция).

Задачи

8.1. Покажите, что множество $\operatorname{End} A$ действительно образует ассоциативное кольцо относительно указанных операций сложения и умножения эндоморфизмов. При этом $\operatorname{Aut} A = (\operatorname{End} A)^*$.

8.2. Пусть K — кольцо. Для каждого $x \in K$ можно определить отображение $\alpha_x\colon K \to K$ по правилу $\alpha_x\colon y \mapsto yx$. Покажите, что:

а) $\{\alpha_x \,|\, x \in K\}$ есть подкольцо в $\operatorname{End} K^+$, изоморфное K;

б) если K — кольцо с единицей, то группа $\operatorname{Aut} K^+$ имеет подгруппу, изоморфную K^*.

8.3. 1) $\operatorname{End}\mathbb{Z} \cong \mathbb{Z}$ и $\operatorname{Aut}\mathbb{Z} \cong \mathbb{Z}_2$.

2) $\operatorname{End}\mathbb{Z}_n \cong \mathbb{Z}_n$ и $\operatorname{Aut}\mathbb{Z}_n \cong \mathbb{Z}_n^*$, $|\operatorname{Aut}\mathbb{Z}_n| = \varphi(n)$.

3) $\operatorname{End}\mathbb{Q} \cong \mathbb{Q}$. 4) $\operatorname{Aut} S_3 \cong S_3 \cong \operatorname{Aut} V_4$.

5) $\operatorname{End}\widehat{\mathbb{Z}}_p \cong \widehat{\mathbb{Z}}_p$. 6) $\operatorname{End}\mathbb{Z}_{p^\infty} \cong \widehat{\mathbb{Z}}_p$.

8.4. Опишите группу автоморфизмов: а) группы $\mathbb{Z}_5$ и б) группы $\mathbb{Z}_6$.

8.5. 1) Группа автоморфизмов конечной группы всегда конечна.

2) Группа автоморфизмов бесконечной группы может быть конечной.

3) Группы автоморфизмов неизоморфных групп могут быть изоморфными.

4) Группа автоморфизмов может иметь большую мощность, чем сама группа.

8.6. Пусть $G = \langle x\rangle \times \langle y\rangle$. Покажите, что:

а) для любой пары элементов a, $b \in G$ существует единственный эндоморфизм φ группы G со свойством $\varphi x = a$ и $\varphi y = b$;

б) если $o(x) = o(y)$, то формула $x^m y^n \mapsto y^n x^{m+n}$ $(m, n \in \mathbb{Z})$ задает автоморфизм φ группы G, найдите порядок φ, если $o(x) = o(y) = 4$.

8.7. Если m и n — натуральные числа, то:

а) $\operatorname{End}(\underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}) \cong M(n, \mathbb{Z})$ и $\operatorname{Aut}(\underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}) \cong \operatorname{GL}(n, \mathbb{Z})$;

б) $\operatorname{End}(\underbrace{\mathbb{Z}_m \times \ldots \times \mathbb{Z}_m}_{n}) \cong M(n, \mathbb{Z}_m)$, $\operatorname{Aut}(\underbrace{\mathbb{Z}_m \times \ldots \times \mathbb{Z}_m}_{n}) \cong \operatorname{GL}(n, \mathbb{Z}_m)$.

8.8. Пусть E — элементарная абелева группа порядка p^n. Покажите, что $\operatorname{Aut} E \cong \mathrm{GL}(n, \mathbb{Z}_p)$ и $|\operatorname{Aut} E| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$.

8.9. Если $G = G_1 \times \dots \times G_n$, где G_i — характеристические подгруппы группы G, то $\operatorname{Aut} G \cong \operatorname{Aut} G_1 \times \dots \times \operatorname{Aut} G_n$.

8.10. Если G — группа нечетного порядка, $\alpha \in \operatorname{Aut} G$ и $o(\alpha) = 2$, то $G = G_1 \cdot G_{-1}$, где $G_1 = \{g \in G \mid g^\alpha = g\}$, $G_{-1} = \{g \in G \mid g^\alpha = g^{-1}\}$.

8.11. Пусть A и B — группы, $\alpha\colon A \to B$ и $\beta\colon B \to A$ — гомоморфизмы. Покажите, что если $\beta\alpha \in \operatorname{Aut} A$, то $B = \operatorname{Ker}\beta \leftthreetimes A^\alpha$.

8.12. Пусть G — периодическая группа, n — целое число и α_n — отображение $g \mapsto g^n$ $(g \in G)$. Покажите, что:

а) если группа G коммутативна, то $\alpha_n \in \operatorname{Aut} G$ если и только если $(o(g), n) = 1$ для всех $g \in G$;

б) если $n \in \{-1, 2, 3\}$ и $\alpha_n \in \operatorname{Aut} G$, то группа G коммутативна.

Пусть $n \in Z$. Группа G называется *n-абелевой*, если $x^n y^n = (xy)^n$ для всех x, $y \in G$, т.е. отображение $g \mapsto g^n$ $(g \in G)$ есть эндоморфизм группы G.

8.13. 1) n-абелева группа является n^m-абелевой при любом $m \in \mathbb{N}$.

2) В n-абелевой группе любой $\pi(n)$-элемент перестановочен с любым $\pi(n)'$-элементом ($\pi(n)$ — множество всех простых чисел, делящих n, а $\pi(n)'$ — его дополнение во множестве всех простых чисел).

8.14. Пусть G — конечная группа, $\alpha \in \operatorname{Aut} G$ и $o(\alpha) = p$ — простое число. Если α оставляет на месте каждый класс сопряженных элементов группы G, то p делит порядок группы G.

8.15. Если α — нормальный эндоморфизм группы G, то отображение $-1 + \alpha\colon g \mapsto g^{-1}g^\alpha$ есть эндоморфизм группы G.

8.16. Если группа G совершенна, то $\operatorname{Aut} G \cong G$.

8.17. Если α — нормальный автоморфизм группы G, то α действует тождественно на коммутанте G'.

8.18. Для каждой подгруппы $A \subseteq \operatorname{Aut} G$ подгруппа $[G, A]$ является A-инвариантной нормальной подгруппой в G.

8.19. Пусть G — группа, N — ее нормальная подгруппа, $\alpha \in \operatorname{Aut} G$ и $N \subseteq C_G(\alpha)$. Тогда $N \subseteq C_G([G, \alpha])$.

8.20. Найдите все эндоморфизмы группы S_3. Определите их ядра и образы. Докажите, что группа S_3 совершенна.

8.21. 1) Если $\operatorname{Aut} G$ — циклическая группа, то группа G коммутативна.

2) Группа автоморфизмов конечной абелевой группы порядка > 2 имеет четный порядок.

8.22. Найдите все конечные группы G, для которых $|\operatorname{Aut} G| = 1$.

8.23. Если H — характеристическая подгруппа группы G, то определена факторгруппа $\operatorname{Aut} G / C_{\operatorname{Aut} G}(H)$ и она изоморфна подгруппе группы $\operatorname{Aut} H$.

8.24. Пусть $\varphi \in \operatorname{End} G$ и H — φ-допустимая нормальная подгруппа в G. Тогда:

а) отображение $\overline{\varphi}\colon gH \mapsto g^\varphi H$ есть эндоморфизм группы $\overline{G} = G/H$, причем если $\varphi \in \operatorname{Aut} G$, то $\overline{\varphi} \in \operatorname{Aut} \overline{G}$;

б) если к тому же подгруппа H характеристична в G, то отображение $\varphi \mapsto \overline{\varphi}$ есть гомоморфизм группы $\operatorname{Aut} G$ в $\operatorname{Aut} \overline{G}$ с ядром $C_{\operatorname{Aut} G}\overline{G} = \{\alpha \in \operatorname{Aut} G \mid (gH)^\alpha = gH \text{ для всех } g \in G\}$.

8.25. Конечная абелева группа нечетного порядка > 1 имеет точно один регулярный автоморфизм порядка 2.

8.26. Если G — конечная группа, имеющая регулярный автоморфизм φ порядка 2, то:

а) G — коммутативная группа нечетного порядка;

б) φ отображает каждый элемент группы G в обратный.

8.27. 1) Центр группы, а также подгруппа Фраттини являются характеристическими подгруппами.

2) В конечной простой группе подгруппа Фраттини совпадает с единичной подгруппой.

3) Если H — характеристическая подгруппа группы B, а B — нормальная подгруппа группы G, то H является нормальной подгруппой в G.

8.28. Приведите пример группы, центр которой не является вполне инвариантной подгруппой.

8.29. Если $Z(G) = e$, то $Z(\operatorname{Aut} G) = 1$.

8.30. Все конечные циклические группы нечетных порядков > 1 не могут быть группами автоморфизмов, ни для каких групп.

8.31. 1) $\operatorname{Aut} S_3 \cong S_3$, причем все автоморфизмы — внутренние.

2) $\operatorname{Aut} V_4 \cong S_3$, причем внутренним является лишь тождественный автоморфизм.

8.32. $\operatorname{Aut} A_4 \cong S_4$ и $\operatorname{Aut} Q_8 \cong S_4$.

8.33. Является ли циклической группа автоморфизмов: а) группы $\mathbb{Z}_9$, б) группы $\mathbb{Z}_8$?

8.34. $|\operatorname{Aut}\operatorname{Aut}\operatorname{Aut}\mathbb{Z}_9| = 1$.

8.35. Если G — конечная простая некоммутативная группа, то $\operatorname{Aut} G$ — совершенная группа.

8.36. Пусть $G = A \times B = A \times C$. Каждый элемент $g \in G$ единственным образом представляется в виде $g = ab$, где $a \in A$, $b \in B$. Элемент b имеет единственное представление в виде $b = a_1 c$, где $a_1 \in A$ и $c \in C$. Положим $g^\varphi = a_1$ и $g^\alpha = (g^\varphi)^{-1} g$. Покажите, что $\varphi \in \operatorname{End} G$ и $G^\varphi = B^\varphi \subseteq Z(G)$, $\alpha \in \operatorname{Aut} G$ и $A^\alpha = A$, $B^\alpha = C$.

8.37. Совершенная нормальная подгруппа служит прямым множителем группы.

8.38. Конечная группа не имеет собственных характеристических подгрупп тогда и только тогда, когда она является прямым произведением конечного числа изоморфных простых подгрупп.

8.39. Пусть G — группа и H — некоторое подмножество в группе $G \times G$. Равносильны следующие условия:

а) H — подгруппа в $G \times G$ и $H \cong G$;

б) существуют такие эндоморфизмы α и β группы G, что $\operatorname{Ker}\alpha \cap \operatorname{Ker}\beta = e$ и $\alpha\beta \neq 1$, причем $H = \{(\alpha g,\, \beta g) \,|\, g \in G\}$.

8.40. Стабилизатор цепочки $0 \subseteq B \subseteq A$ абелевой группы A изоморфен группе $\operatorname{Hom}(A/B,\, B)$. Он является нормальной подгруппой группы $\operatorname{Aut} A$, если подгруппа B характеристична в A.

8.41. Пусть $A = B \oplus C$, где B — вполне инвариантная подгруппа абелевой группы A. Покажите, что $\operatorname{Aut} A$ — полупрямое произведение стабилизатора $S \cong \operatorname{Hom}(C,\, B)$ цепочки $0 \subseteq B \subseteq A$ и подгруппы $\operatorname{Aut} B \times \operatorname{Aut} C$.

8.42. Пусть A — абелева группа со свойством $A = 2A$. А ε — такой ее автоморфизм, что $\varepsilon^2 = 1$, т.е. ε — инволюция группы $\operatorname{Aut} A$. Обозначим $A_\varepsilon^+ = \{a \in A \,|\, \varepsilon a = a\}$ и $A_\varepsilon^- = \{a \in A \,|\, \varepsilon a = -a\}$. Покажите, что $A = A_\varepsilon^+ \oplus A_\varepsilon^-$, т.е. такие автоморфизмы $\varepsilon \neq \pm 1$ дают нетривиальные прямые разложения группы A. Найдите ассоциированные с таким разложением проекции группы A.

8.43. Пусть A — абелева группа. Группа $\operatorname{Aut} A$ конечна тогда и только тогда, когда $A = t(A) \oplus B$, где группы $t(A)$, $\operatorname{Aut} B$ и $\operatorname{Hom}(B,\, t(A))$ конечны.

8.44. Пусть A — абелева группа, не являющаяся 2-группой. Покажите, что если группа $\operatorname{Aut} A$ конечна, то порядок ее центра — ненулевое четное число. Выведите отсюда, что конечные простые группы, группы S_n и A_n при $n \geqslant 3$ не могут служить группами автоморфизмов абелевых групп.

8.45. Пусть $A = \bigoplus\limits_{i \in I} A_i$ — абелева группа. Группа $\operatorname{Aut} A$ коммутативна тогда и только тогда, когда каждая $\operatorname{Aut} A_i$ коммутативна и $\operatorname{Hom}(A_i,\, A_j) = 0$ при $i \neq j$.

8.46. Пусть A — абелева группа без кручения. Тогда если $\operatorname{Aut} A$ — периодическая группа, то:

а) кольцо эндоморфизмов $\operatorname{End} A$ группы A не содержит ненулевых нильпотентных элементов;

б) всякая инволюция $\alpha \in \operatorname{Aut} A$ лежит в центре этой группы.

8.47. Для любой абелевой группы A и для произвольного натурального числа n всякий автоморфизм группы nA индуцируется некоторым автоморфизмом группы A.

8.48. Пусть A — абелева группа без кручения и B — квазиравная ей подгруппа, $nA \subseteq B \subseteq A$. Докажите, что автоморфизм (эндоморфизм) φ группы B продолжается до автоморфизма (эндоморфизма) группы A, если и только если для любого элемента $a \in A$ из $na = b \in B$ следует разрешимость в группе A уравнения $nx = \varphi b$.

8.49. 1) Если группа автоморфизмов A некоторой π-группы P стабилизирует цепь $P \supseteq P_1 \supseteq \ldots \supseteq P_n = e$, то A является π-группой.

2) Если A — такая π'-группа автоморфизмов некоторой π-группы P, что $[P,\, A,\, A] = e$, то $[P,\, A] = e$, а потому $A = 1$.

8.50. Любая конечная p-группа P содержит такую характеристическую подгруппу C, что:

а) $cl\, C \leqslant 2$ и $C/Z(C)$ — элементарная группа;

б) $[P,\, C] \subseteq Z(C)$;

в) $C_P(C) = Z(C)$;

г) любой неединичный автоморфизм a взаимно простого с p порядка действует на C нетривиально.

8.51. Пусть P — конечная p-группа, A — p'-подгруппа из $\operatorname{Aut} P$. Тогда:

а) A изоморфна подгруппе группы $\mathrm{Aut}(P/\Phi(P))$;

б) $P = [P,\, A]\, C_P(A)$ и $[P,\, A] = [[P,\, A],\, A]$;

в) если P — коммутативная группа, то $P = [P,\, A] \times C_P(A)$.

8.52. Покажите, что $\mathrm{Hol}\, G \cong G \times G$, если группа G совершенна.

8.53. Следующие условия для группы G равносильны:

а) G — совершенная группа;

б) всякий раз, когда G — нормальная подгруппа группы A, выполняется $A = G \times C_A(G)$.

8.54. Пусть P — конечная p-группа. Тогда если a — ее p'-автоморфизм, централизующий $\Omega_1(P)$, то $a = 1$, за исключением случая, когда P — некоммутативная 2-группа. Если $[a,\, \Omega_2(P)] = e$, то $a = 1$ во всех случаях.

9 Упорядоченные группы

Группа G называется *частично упорядоченной*, если на G задан частичный порядок $\leqslant$ со свойством *монотонности*, т.е. если $a \leqslant b$ ($a,\ b \in G$), то $ac \leqslant bc$ и $ca \leqslant cb$ для каждого $c \in G$. Если частичный порядок $\leqslant$ линеен (является решеткой), то группа называется *линейно упорядоченной* (*решеточно упорядоченной*). Группы частично, решеточно или линейно упорядоченные иногда называют просто *упорядоченными*.

Элемент a упорядоченной группы называется *положительным* (*строго положительным*), если $a \geqslant e$ ($a > e$) и *отрицательным* (*строго отрицательным*), если $a \leqslant e$ ($a < e$). Множество положительных (отрицательных) элементов частично упорядоченной группы G обозначается через $P(G)$ (через $P^{-1}(G)$). Согласно 9.7 $P(G)$ — подмоноид в G (*положительный конус*).

Групповой гомоморфизм f частично упорядоченной группы G в частично упорядоченную группу B называется *порядковым гомоморфизмом* или *у-гомоморфизмом*, если из $a \leqslant b$ в G следует $f(a) \leqslant f(b)$ в B.

Линейно упорядоченная группа называется *архимедовой*, если в ней нет нетривиальных выпуклых подгрупп. Известно, что архимедова линейно упорядоченная группа коммутативна и у-изоморфна подгруппе аддитивной группы вещественных чисел с их естественным порядком (*теорема Гельдера*).

Группа, которую можно сделать линейно упорядоченной, называется *упорядочиваемой*.

Частично упорядоченная группа, не содержащая нетривиальных выпуклых нормальных подгрупп, называется *у-простой*.

Задачи

9.1. Группа $\mathbb{R}$ и группа $\mathbb{R}_+^*$ являются упорядоченными группами с их естественными порядками.

9.2. Если A — подгруппа группы G, то частичная (линейная) упорядоченность группы G индуцирует частичную (линейную) упорядоченность в A.

9.3. Пусть G — упорядоченная группа, $a < b$ и $c \in G$. Тогда:

а) $c^{-1}ac < c^{-1}bc$; б) $b^{-1} < a^{-1}$;

в) если $a' < b'$, то $aa' < bb'$.

9.4. Если G — упорядоченная группа, то:

а) $P(G) \cap P^{-1}(G) = e$;

б) $a \in P^{-1}(G)$, если и только если $a^{-1} \in P(G)$.

9.5. В упорядоченной группе соотношение $a \leqslant b$ имеет место тогда и только тогда, когда $a^{-1}b \in P(G)$ (равносильно $b^{-1}a \in P^{-1}(G)$).

Свойство упр. 9.5 показывает, что задание положительной (отрицательной) части упорядоченной группы вполне определяет упорядоченность.

9.6. Если в упорядоченной группе неединичный элемент имеет конечный порядок, то он не может быть ни положительным, ни отрицательным. Следовательно, периодические группы допускают только тривиальное частичное упорядочение, а линейно упорядоченные группы обязаны быть группами без кручения.

9.7. Пусть G — упорядоченная группа. Тогда:

а) если $x,\ y \in P(G)$, то $xy \in P(G)$;

б) если $x \in P(G)$, $z \in G$, то $z^{-1}xz \in P(G)$.

Свойство а) означает, что $P(G)$ является моноидом.

9.8. Пусть H — подмножество группы G, удовлетворяющее условиям:

а) если $x,\ y \in H$, то $xy \in H$; б) $e \in H$;

в) если $x \in H$, причем $x \neq e$, то $x^{-1} \notin H$;

г) если $x \in H$, $z \in G$, то $z^{-1}xz \in H$.

Тогда в G можно ввести такую упорядоченность, относительно которой H будет положительной частью группы G.

Подполугруппа H группы G тогда и только тогда определяет линейную упорядоченность этой группы, когда она помимо б) — г) также удовлетворяет условию:

д) для любого $a \in G$ или $a \in H$, или $a^{-1} \in H$.

9.9. Всякая частичная упорядоченность группы G продолжается до максимальной (далее не продолжаемой) частичной упорядоченности.

9.10. Групповой гомоморфизм φ частично упорядоченной группы G в частично упорядоченную группу F является порядковым тогда и только тогда, когда $\varphi(P(G)) \subseteq P(F)$. Все у-автоморфизмы частично упорядоченной группы образуют группу.

9.11. Пусть G — упорядоченная группа. Тогда:

а) если $x,\ y \in P^{-1}(G)$, то $xy \in P^{-1}(G)$;

б) если $x \in P^{-1}(G)$, $z \in G$, то $z^{-1}xz \in P^{-1}(G)$.

9.12. Частично упорядоченная группа будет линейно упорядоченной, если и только если $P(G) \cup P^{-1}(G) = G$.

9.13. 1) Если P — подполугруппа группы G, удовлетворяющая свойствам б) — г) из 9.8, то множество P^{-1} также будет подполугруппой с этими свойствами, причем $P \cap P^{-1} = e$.

2) Если P и Q — подполугруппы группы G, удовлетворяющие свойствам б) — г) из 9.8 и $P \cap Q^{-1} = e$, то множество $PQ = \{pq \,|\, p \in P,\ q \in Q\}$ также будет подполугруппой с этими свойствами.

3) Пересечение любой системы подполугрупп группы G, обладающих свойствами б) — г) из 9.8, само будет подполугруппой с этими свойствами.

9.14. Из п. 3) задачи 9.13 следует, что если элемент a группы G содержится в хотя бы одной подполугруппе со свойствами б) — г) из 9.8, то существует наименьшая подполугруппа P_a с этими свойствами, содержащая a. Докажите, что максимальная упорядоченность группы G линейна тогда и только тогда, когда:

а) P_a существует для каждого $a \in G$;

б) если $b, c \in P_a$ и $b, c \neq e$, то $P_b \cap P_c \neq e$.

9.15. Все максимальные упорядоченности абелевой группы без кручения линейны. В частности, всякая абелева группа без кручения линейно упорядочена.

9.16. Если G — произвольная частично упорядоченная группа, у которой $x \leqslant x^2$, то $x^n \leqslant x^m$ имеет место, если и только если $n \leqslant m$.

9.17. 1) Если в упорядоченной группе для любых двух элементов существует верхняя граница, то всякие два элемента обладают и нижней границей.

2) Упорядоченная группа из 1) называется *направленной*. Если G — упорядоченная группа, то она является направленной тогда и только тогда, когда для каждого $x \in G$ найдутся $u,\ v \in P(G)$ со свойством $x = uv^{-1}$.

3) Частично упорядоченная группа G будет направленной тогда и только тогда, когда $G = \langle P(G) \rangle$.

9.18. Если абелева группа обладает двумя различными упорядочениями, то число ее упорядочений бесконечно.

9.19. Пусть $P_1 = \{x + iy \,|\, x > 0 \text{ или } x = 0,\ y \geqslant 0\}$, $P_2 = \{x + iy \,|\, x \geqslant 0, y \geqslant 0\}$. Тогда P_1 определяет линейный, а P_2 — решеточный порядок в $\mathbb{C}$.

9.20. Пусть G — мультипликативная группа положительных рациональных чисел, $P(G)$ — множество натуральных чисел. Тогда G — решеточно упорядоченная группа.

9.21. Пусть $G = \mathbb{R}^*$, $P(G) = \{x \in \mathbb{R} \,|\, x > 1\}$, то G — частично, но не решеточно упорядоченная группа.

9.22. Пусть G — аддитивная группа многочленов над полем вещественных чисел, $P(G)$ состоит из всех таких многочленов $a_0+a_1x+\ldots+a_nx^n$, у которых первый ненулевой коэффициент $a_i>0$. Тогда G — линейно упорядоченная группа.

9.23. Пусть A — подгруппа группы $\mathbb{R}$, B — наибольшая подгруппа группы $\mathbb{R}_+^*$ такая, что из $r\in B$ и $a\in A$ следует $ra\in A$. Рассмотрим множество $T=\{(r,a)\,|\,r\in B,\ a\in A\}$ с операцией умножения: $(r,a)(r',a')=(rr',ra'+a)$. Положим $P(T)=\{(r,a)\,|\,r>1$, либо $r=1$ и $a\geqslant 0\}$. Докажите, что T — линейно упорядоченная группа, множество элементов вида $(1,a)$ образует подгруппу, изоморфную A, и при этом $(r,b)(1,a)(r,b)^{-1}=(1,ra)$, а множество элементов вида $(r,0)$ — подгруппу, изоморфную B.

9.24. Подгруппа A частично упорядоченной группы G выпукла тогда и только тогда, когда в ней вместе со всяким положительным элементом a содержатся все положительные элементы x группы G, удовлетворяющие неравенству $x\leqslant a$.

9.25. Пересечение любого семейства выпуклых подгрупп частично упорядоченной группы — выпуклая подгруппа.

9.26. Ядро всякого гомоморфизма частично упорядоченной группы является выпуклой нормальной подгруппой.

9.27. Выпуклые подгруппы линейно упорядоченной группы составляют цепь по включению.

9.28. Если a — строго положительный элемент линейно упорядоченной группы G, то множество A всех таких элементов $x\in G$, что $e\leqslant x\leqslant a^n$ при некотором натуральном n, и элементов, им обратных, есть минимальная выпуклая подгруппа, содержащая a.

9.29. Наименьшая выпуклая подгруппа H частично упорядоченной группы G, содержащая подгруппу A, равна $AP(G)\cap AP^{-1}(G)$.

9.30. Если A — выпуклая нормальная подгруппа частично упорядоченной группы G, то факторгруппу $\overline{G}=G/A$ можно так частично упорядочить, что групповой канонический эпиморфизм $G\to\overline{G}$ будет порядковым.

Нормальная подгруппа H частично упорядоченной группы G тогда и только тогда является ядром некоторого у-гомоморфизма, когда она выпуклая. Если φ — является у-эпиморфизмом G на $\overline{G}$ с ядром H, то факторгруппа G/H у-изоморфна $\overline{G}$.

9.31. Линейно упорядоченная группа тогда и только тогда будет архимедовой, когда для любой пары a,b ее строго положительных элементов существует $n\in\mathbb{N}$ со свойством $a^n>b$.

9.32. Группа $\mathbb{Q}$ допускает только два линейных порядка, которые взаимно обратные.

9.33. Группа $\mathbb{Q}$ у-проста.

9.34. Пусть G — группа, порожденная символами $g(r)$, заданными для каждого $r\in\mathbb{Q}$, и удовлетворяющая определяющим соотношениям

$g(r_1)g(r_2)=g\left(\frac{r_1+r_2}{2}\right)g(r_1)$ при $r_1>r_2$.

Покажите, что каждый элемент $a\neq e$ из G однозначно записывается в виде $a=g(r_1)^{m_1}\ldots g(r_k)^{m_k}$, $r_1<r_2<\ldots<r_k$, $m_i\neq 0$.

Положим $a>e$, если $m_k>0$. Докажите, что G — некоммутативная линейно упорядоченная группа, имеющая выпуклые подгруппы только следующих видов:

$H_\alpha=\{a\in G\,|\,r_k<\alpha,\ \alpha$ — вещественное число$\}$,

$H^\alpha=\{a\in G\,|\,r_k\leqslant\alpha,\ \alpha$ — рациональное число$\}$.

Группа G является у-простой.

9.35. Если A и A_1 — подгруппы группы $\mathbb{R}$ с ее естественным порядком, а φ есть у-изоморфизм A на A_1, то существует такое вещественное число $r>0$, что $\varphi(a)=ra$ для всех $a\in A$. В частности, группа у-автоморфизмов архимедовой группы изоморфна подгруппе группы $\mathbb{R}_+^*$.

9.36. Пусть $G=\prod\limits_{i\in I}A_i$ — прямое произведение частично упорядоченных групп и $P=\{a=(\ldots,a_i,\ldots)\in G\,|\,a_i\geqslant e$ в A_i для всех $i\}$. Покажите, что G — частично упорядоченная группа.

9.37. Докажите, что прямое произведение упорядочиваемых групп упорядочиваемо. Выведите из этого утверждения упорядочиваемость делимых абелевых групп без кручения, и, значит, всех абелевых групп без кручения.

Система подгрупп, линейно упорядоченных по включению, называется *полной*, если она содержит объединение и пересечение любого множества своих подгрупп. Подмножество H группы G называется *инфраинвариантным*, если $H\subseteq H^g$ или $H^g\subseteq H$ для любого $g\in G$. Система Σ подгрупп группы G называется *инфраинвариантной*, если она полная, $e,G\in\Sigma$ и из $H\in\Sigma$ следует $H^g\in\Sigma$ для любого $g\in G$.

Под *скачком* $A\subset B$ полной системы Σ понимается такая пара подгрупп A и B из Σ, что между A и B нет других подгрупп из Σ.

9.38. 1) Каждый элемент $g\neq e$ группы определяет скачок $A\subset B$ в Σ, если в качестве A взять объединение подгрупп из Σ, не содержащих g, а в качестве B — пересечение подгрупп, содержащих g.

2) Если $A \subset B$ — скачок инфраинвариантной системы, то A инвариантна (нормальна) в B и нормализатор $N(A) = N(B)$.

9.39. Система Σ всех выпуклых подгрупп линейно упорядоченной группы G инфраинвариантна, и если $A \subset B$ — скачок из Σ, то факторгруппа B/A изоморфна подгруппе аддитивной группы вещественных чисел, а группа автоморфизмов группы B/A, порожденная внутренними автоморфизмами группы $N(A)/A$, изоморфна подгруппе мультипликативной группы положительных вещественных чисел.

Модуль $|a|$ элемента a линейно упорядоченной группы определяется равенством $|a| = \max\{a, a^{-1}\}$.

Элемент a называется *бесконечно малым по сравнению с* b, обозначение $a << b$, если $|a|^n < |b|$ справедливо для всех целых n. Если не выполнено ни $a << b$, ни $b << a$, то a и b называются *архимедовски эквивалентными*.

9.40. В линейно упорядоченной группе:

а) архимедовски эквивалентные элементы определяют один и тот же скачок в системах выпуклых подгрупп;

б) $a << b$ тогда и только тогда, когда существует выпуклая подгруппа, содержащая a и не содержащая b;

в) для любых элементов справедливо соотношение

$$|[a, b]| << \max\{|a|, |b|\}.$$

9.41. Коммутант линейно упорядоченной группы с конечным числом образующих содержится в собственной выпуклой подгруппе.

Полугруппа $H \subseteq G$ группы G называется *инвариантной* (нормальной), если $x^{-1}hx \in H$ для любого $x \in G$. Обозначим через $S(a_1, \dots, a_n)$ инвариантную полугруппу, порожденную элементами $a_1, \dots, a_n$. Если частичный порядок $\leqslant'$ с полугруппой положительных элементов P' продолжает частичный порядок $\leqslant$ с полугруппой положительных элементов P, то $P \subseteq P'$.

9.42. Частичный порядок P группы G тогда и только тогда продолжается до линейного, когда

$(*)$ для любого конечного множества элементов $a_1, \dots, a_n \in G$ можно так подобрать значения для $\varepsilon_1, \dots, \varepsilon_n$, равные ± 1, что

$$P \cap S(a_1^{\varepsilon_1}, \dots, a_n^{\varepsilon_n}) = \varnothing.$$

Притом, если P удовлетворяет условию $(*)$ и $a \in G$, то либо $PS(e, a)$, либо $PS(e, a^{-1})$ определяет частичный порядок P' в G, который также удовлетворяет условию $(*)$.

Группы, у которых всякий максимальный порядок является линейным, называются *доупорядочиваемыми*.

9.43. Группа упорядочиваема (доупорядочиваема) тогда и только тогда, когда каждая ее подгруппа с конечным числом образующих упорядочиваема (доупорядочиваема).

Подгруппа $H \subseteq G$ называется *G-упорядочиваемой*, если любой максимальный порядок группы G индуцирует на H линейный порядок.

9.44. Группа G упорядочиваема тогда и только тогда, когда в ней существует инфраинвариантная система Σ подгрупп, удовлетворяющая условию: если $A \subset B$ — скачок из Σ, то факторгруппа B/A является $N(A)/A$-упорядочиваемой (или $N(A)/A$-доупорядочиваемой). Притом в G существует порядок, при котором все подгруппы из Σ выпуклы.

9.45. Если факторгруппа G/H группы G по инвариантной линейно (частично) G-упорядоченной подгруппе H линейно (частично) упорядочена, то в группе G можно ввести такой линейный (частичный) порядок, при котором индуцированные порядки на H и G/H будут совпадать с заданными на них, и подгруппа H будет выпуклой в G.

9.46. Локально нильпотентные группы без кручения упорядочиваемы.

9.47. Свободные группы упорядочиваемы.

9.48. Каждая линейно (частично) упорядоченная группа является у-эпиморфным образом некоторой линейно (частично) упорядоченной свободной группы.

Группа G, одновременно являющаяся топологическим пространством, называется *топологической группой*, если умножение и операция взятия обратного элемента непрерывны в заданной топологии, т.е. для любых $a, b \in G$ и любых окрестностей X и Y элементов ab и c^{-1} найдутся такие окрестности U, V, W элементов a, b, c соответственно, что $UV \subseteq X$ и $W^{-1} \subseteq Y$.

Линейно упорядоченную группу G можно превратить в топологическую группу, взяв в качестве базы окрестностей топологического пространства G множество открытых интервалов $(a, b) = \{x \in G \,|\, a < x < b\}$. Топологию, полученную таким образом, называют *интервальной топологией*, она хаусдорфова.

9.49. Линейно упорядоченная группа с интервальной топологией дискретна тогда и только тогда, когда в ней имеется наименьшая выпуклая подгруппа, являющаяся циклической.

Далее рассматриваются недискретные линейно упорядоченные группы.

9.50. Подгруппа H линейно упорядоченной группы G с интервальной топологией открыта тогда и только тогда, когда H содержит выпуклую подгруппу.

9.51. Линейно упорядоченная группа G с интервальной топологией связна тогда и только тогда, когда G изоморфна группе $\mathbb{R}$ с ее естественным порядком.

9.52. Линейно упорядоченная группа локально компактна тогда и только тогда, когда она имеет наименьшую выпуклую подгруппу, изоморфную группе $\mathbb{R}$.

Линейно упорядоченная группа называется *порядково полной*, если всякое ограниченное сверху множество ее элементов имеет точную верхнюю грань.

9.53. Линейно упорядоченная группа порядково полна тогда и только тогда, когда она изоморфна группе $\mathbb{R}$ с ее естественным порядком.

Пусть G — линейно упорядоченная группа с интервальной топологией. Говорят, что вполне упорядоченная последовательность $\{g_\alpha \,|\, \alpha < \lambda\}$, где λ — порядковый тип последовательности $\{g_\alpha\}$, *сходится* к элементу g, если для любого $a > e$, $a \in G$, найдется номер $\alpha_0(a) < \lambda$ такой, что для всякого $\alpha > \alpha_0(a)$ выполняется соотношение $a^{-1} < g g_\alpha^{-1} < a$.

Вполне упорядоченная последовательность $\{g_\alpha \,|\, \alpha < \lambda\}$, где λ — порядковое число, называется *фундаментальной последовательностью*, если для любого $a > e$, $a \in G$, найдется номер $\alpha_0(a)$, $\alpha_0 < \lambda$ такой, что для всяких α, β, $\alpha_0 < \alpha < \lambda$, $\alpha_0 < \beta < \lambda$, выполняется соотношение $a^{-1} < g_\alpha g_\beta^{-1} < a$.

Линейно упорядоченная группа с интервальной топологией называется *топологически полной*, если для всякой фундаментальной последовательности $\{g_\alpha \,|\, \alpha < \lambda\}$ найдется элемент $g \in G$, к которому сходится эта последовательность.

9.54. Всякая сходящаяся последовательность является фундаментальной.

Всякая линейно упорядоченная группа G вкладывается в топологически полную линейно упорядоченную группу G^*, имеющую ту же систему выпуклых подгрупп, что и G.

10 Действия групп на множествах. Представления групп

Пусть Ω — некоторое множество, G — группа. Под *реализацией* G в $S(\Omega)$ понимают любой гомоморфизм $\Phi\colon G \to S(\Omega)$. Если $\Phi(g) = \Phi_g \in S(\Omega)$, $x \in \Omega$, то образ $\Phi_g(x)$ часто обозначается символом gx, и говорят об отображении $G \times \Omega \to \Omega$. Ясно, что: 1) $ex = x$; 2) $(gh)x = g(hx)$ для любых $g,\ h \in G$ и $x \in \Omega$. В этом случае говорят также, что группа G *действует* на множестве Ω, а Ω является *G-множеством*. Обратно, если имеется G-множество Ω, то формула $\Phi_g(x) = gx$, $x \in \Omega$, определяет гомоморфизм $\Phi\colon g \to \Phi_g$ группы G в $S(\Omega)$. Ядро $\operatorname{Ker}\Phi$ называют *ядром действия* группы G. Если Φ — мономорфизм, то говорят, что G действует *эффективно* на множестве Ω. Перейдя к факторгруппе $\overline{G} = G/\operatorname{Ker}\Phi$, при необходимости всегда можно рассматривать эффективное действие $\overline{G}$ на Ω (см. 10.1 (д)).

Две точки $x,\ y \in \Omega$ называются *эквивалентными* относительно группы G, действующей на Ω, если $y = gx$ для некоторого $g \in G$. Класс эквивалентности, содержащий элемент x_0, обозначают через $G(x_0)$ и называют *орбитой* (содержащей x_0). Множество $\operatorname{St}(x_0) = \{g \in G \,|\, gx_0 = x_0\}$ называют *стационарной подгруппой* (или *стабилизатором*) в G точки $x_0 \in \Omega$ и обозначают символом G_{x_0}. $\operatorname{Fix}(g) = \{x \in \Omega \,|\, gx = x\}$ — *множество неподвижных точек* элемента $g \in G$, $\operatorname{Fix}(H) = \{x \in \Omega \,|\, hx = x \text{ для всех } h \in H\}$ при $H \subseteq G$.

Пусть Ω — G-множество. Подмножество $X \subseteq \Omega$ называется *G-инвариантным*, если $gx \in X$ для всех $g \in G$ и $x \in X$.

Пусть Φ и Ψ — гомоморфизмы группы G в $S(\Omega)$ и $S(\Xi)$ соответственно. Определенные ими действия на Ω и на Ξ называются *эквивалентными*, если существует биективное отображение $\sigma\colon \Omega \to \Xi$, делающее диаграмму

$$\begin{array}{ccc} \Omega & \xrightarrow{\ \sigma\ } & \Xi \\ \downarrow \Phi_g & & \downarrow \Psi_g \\ \Omega & \xrightarrow{\ \sigma\ } & \Xi \end{array}$$

коммутативной при всех $g \in G$. Таким образом, $\Psi_g = \sigma\, \Phi_g \sigma^{-1}$.

Группу перестановок $G \subseteq S(\Omega)$, действующую на множестве Ω, называют *транзитивной*, если орбита некоторой (следовательно, и любой) точки множества Ω совпадает с Ω.

Группа G, действующая на Ω, называется *регулярной* (на Ω), если она транзитивна и $G_x = e$ для любого $x \in \Omega$.

Пусть $\Omega = \bigcup\limits_{i=1}^{m} \Omega_i$ — разбиение Ω на попарно непересекающиеся множества, $S = \{\Omega_i \,|\, i = 1, \ldots, m\}$. Говорят, что S есть *система импримитивности* группы G на Ω, если $g\Omega_i \in S$ для всех $g \in G$ и $i = 1, \ldots, m$. Системы импримитивности $\{\{x\} \,|\, x \in \Omega\}$ и $\{\Omega\}$ называются *тривиальными*. Группа перестановок называется *импримитивной*,

если она транзитивна и обладает нетривиальной системой импримитивности. Транзитивная, но не импримитивная группа называется *примитивной*.

Пусть V — векторное пространство размерности n над полем P, $\mathrm{GL}(V)$ — группа обратимых линейных операторов на V ($\mathrm{GL}(V) = \mathrm{GL}(n, P)$ после выбора базиса в V). Всякий гомоморфизм $\Phi\colon G \to \mathrm{GL}(V)$ называется линейным *представлением* группы G в пространстве V. Представление называется *точным*, если $\operatorname{Ker}\Phi = e$, и *тривиальным*, если $\Phi(g) = I$ — единичный оператор для всех $g \in G$. Если $P = \mathbb{C}$, а $U(n)$ — группа унитарных операторов (через $U(n)$ принято обозначать также и группу унитарных матриц порядка n), то представление $\Phi\colon G \to \mathrm{GL}(n, \mathbb{C})$ со свойством $\operatorname{Im}\Phi \subseteq U(n)$, называется *унитарным*.

Два линейных представления (Φ, V), (Ψ, W) группы G называются *эквивалентными* (*изоморфными* или *подобными*), если существует изоморфизм векторных пространств $\sigma\colon V \to W$, делающий диаграмму

$$\begin{array}{ccc} V & \xrightarrow{\ \sigma\ } & W \\ \downarrow{\scriptstyle \Phi(g)} & & \downarrow{\scriptstyle \Psi(g)} \\ V & \xrightarrow{\ \sigma\ } & W \end{array}$$

коммутативной при всех $g \in G$, или, что равносильно, $\Psi(g) = \sigma\,\Phi(g)\sigma^{-1}$.

Пусть (Φ, V) — линейное представление группы G. Подпространство $U \subset V$ называется *инвариантным относительно* G, если $\Phi(g)\,u \in U$ для всех $u \in U$. Нулевое подпространство и само пространство V относятся к *тривиальным* инвариантным подпространствам. Представление, обладающее лишь тривиальными инвариантными подпространствами, называется *неприводимым*. Если $V = U \oplus W$, где U и W — инвариантные подпространства, то $\Phi = \Phi' \oplus \Phi''$, где $\Phi' = \Phi\,|\,U$ и $\Phi'' = \Phi\,|\,W$. В этом случае говорят о *разложимом* представлении Φ. Линейное представление (Φ, V) группы G, являющееся прямой суммой неприводимых представлений, называется *вполне приводимым*.

Доказано, что:

1) *всякое линейное представление над* $\mathbb{C}$ *конечной группы* G *эквивалентно унитарному представлению*;

2) (теорема Машке) *каждое линейное представление конечной группы* G *над полем* P *характеристики, не делящей* $|G|$, *вполне приводимо*.

С каждым конечномерным линейным представлением (Φ, V) над полем P связывается функция $\chi_\Phi\colon\ G \to P$, определенная соотношением $\chi_\Phi(g) = \operatorname{tr}\Phi(g)$, где $\operatorname{tr}\Phi(g) = \sum\limits_i \varphi_{ii}(g)$ — *след* матрицы $\Phi(g) = [\varphi_{ij}(g)]$. Функция χ_Φ называется *характером представления*, ее часто обозначают χ_V или χ. Функции $f\colon G \to P$, постоянные на каждом классе сопряженных элементов группы G, называют *классовыми*.

Множество $\mathbb{C}^G = \{G \to \mathbb{C}\}$ всех функций из G в $\mathbb{C}$ можно рассматривать как эрмитово пространство со скалярным произведением $(\sigma, \tau)_G = \dfrac{1}{|G|}\sum\limits_{g\in G} \sigma(g)\overline{\tau(g)}$, $\sigma, \tau \in \mathbb{C}^G$. Доказано, что: *если* Φ, Ψ — *неприводимые комплексные представления конечной группы* G, *то*

$$(\chi_\Phi, \chi_\Psi)_G = \begin{cases} 1, & \text{если } \Phi \text{ эквивалентно } \Psi, \\ 0 & \text{в противном случае.} \end{cases}$$

Это так называемое *первое соотношение ортогональности*.

Если $\chi_1, \ldots, \chi_r$ — все различные характеры неприводимых комплексных представлений конечной группы G, то справедливо *второе соотношение ортогональности*:

$$\sum_{i=1}^{r} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} 0, & \text{если } g \text{ и } h \text{ не сопряжены,} \\ |C_G(g)| & \text{в противном случае.} \end{cases}$$

Характером группы G называется характер любого представления G над $\mathbb{C}$. Через $\operatorname{Irr} G$ обозначается множество всех неприводимых характеров группы G.

Для конечной группы число неприводимых попарно неэквивалентных представлений над $\mathbb{C}$ равно числу ее классов сопряженных элементов. Кроме того, характеры всех попарно неэквивалентных неприводимых представлений группы G над $\mathbb{C}$ образуют ортонормированный базис пространства $\chi(G)$ всех классовых функций.

Пусть P — поле нулевой характеристики, $V = \langle e_g \,|\, g \in G\rangle$ — векторное пространство над P. Представление $\rho(a)e_g = e_{ag}$ называется *регулярным*.

Задачи

10.1. Пусть Ω — G-множество. Проверьте, что:

а) отношение $y = gx$ ($x,\ y \in \Omega,\ g \in G$) является отношением эквивалентности;

б) $\mathrm{St}\,(x)$ для каждой точки $x \in \Omega$ является подгруппой в G;

в) левые смежные классы $g\mathrm{St}(x_0)$ группы G по стационарной подгруппе $\mathrm{St}\,(x_0)$ находятся во взаимно однозначном соответствии с точками орбиты $G(x_0)$;

г) $|\,G(x_0)| = (G : \mathrm{St}\,(x_0))$, т.е. длина G-орбиты точки x_0 совпадает с индексом стационарной подгруппы, значит, длина орбиты делит порядок конечной группы;

д) если H — ядро действия G на Ω, то правило $(g + H)x = gx$ задает эффективное действие $\overline{G}$ на Ω.

10.2. 1) Каждое действие группы G на Ω индуцирует действие на:

а) $\Omega^k = \underbrace{\Omega \times \ldots \times \Omega}_{k}$ по правилу $g(x_1,\ \ldots\ ,\ x_k) = (gx_1,\ \ldots\ ,\ gx_k)$;

б) $P(\Omega)$ по правилу: $g\varnothing = \varnothing$, а если H — непустое подмножество в Ω, то $gH = \{gh \,|\, h \in H\}$.

2) Исследуйте орбиты группы $\mathbb{Z}$, действующей на окружности единичного радиуса в пространстве $\mathbb{R}^2$, отождествленном с $\mathbb{C}$, по формуле: $(n, z) \mapsto e^{i\alpha n}z$, в зависимости от свойств вещественного числа α.

10.3. Всякое инвариантное подмножество в Ω является объединением орбит, причем G-орбита любого элемента $x \in \Omega$ есть наименьшее инвариантное подмножество, содержащее x.

10.4. Пусть Ω — G-множество. Тогда:

а) если точки $x_0,\, y_0 \in \Omega$ лежат в одной орбите, то их стационарные подгруппы сопряжены: условие $y_0 = gx_0$ влечет $\mathrm{St}(y_0) = g\mathrm{St}(x_0)g^{-1}$;

б) если G — конечная группа и $\Omega = \Omega_1 \cup \ldots \cup \Omega_r$ — разбиение Ω на конечное число орбит с представителями $x_1,\ \ldots\ , x_r$, то $|\,\Omega| = \sum\limits_{i=1}^{r} (G : \mathrm{St}(x_i))$.

10.5. Найдите все орбиты группы G невырожденных линейных операторов, действующих на n-мерном пространстве V, если G — группа:

а) всех невырожденных линейных операторов;

б) ортогональных операторов;

в) операторов, матрицы которых в базисе $e_1,\ \ldots\ ,\ e_n$ диагональны;

г) операторов, матрицы которых в базисе $e_1,\ \ldots\ ,\ e_n$ верхние треугольные.

10.6. Пусть G — группа всех невырожденных линейных операторов в n-мерном векторном пространстве V и X — множество всех подпространств размерности k в V.

1) Найдите орбиты группы G в X.

2) Пусть $e_1,\ \ldots\ ,\ e_n$ — такой базис в V, что $e_1,\ \ldots\ ,\ e_k$ — базис некоторого подпространства U. Найдите в базисе $e_1,\ \ldots\ ,\ e_n$ матрицы операторов из стационарной подгруппы G_U.

10.7. Пусть на $\Omega = G$ определяется действие любого элемента $g \in G$ посредством сопряжения: $x \to I_g(x) = g^{-1}xg$, $x \in G$. Определите, что является:

а) ядром этого действия;

б) орбитой и стационарной подгруппой элемента $x \in G$.

Рассмотрите также индуцированное действие на множестве всех подгрупп группы G.

10.8. Пусть G — конечная группа и $x_1^G,\ \ldots, x_r^G$ — ее сопряженные классы, причем первые t из них — одноэлементные: $x_i^G = \{x_i\}$, $i = 1,\ \ldots\ , t$ $(x_1 = e)$. Докажите, что

$$Z(G) = \{x_1,\ \ldots\ , x_t\} \text{ и } |\,G| = |Z\,(G)| + \sum_{i=t+1}^{r} (G : C(x_i)),$$

где $C(x_i)$ — централизатор элемента x_i.

Используя последнюю формулу, покажите, что всякая конечная p-группа имеет неединичный центр.

10.9. Пусть H — подгруппа группы G. Тогда $(x,\ gH) \mapsto x(gH) = xgH$ определяет действие L^H группы G на множестве левых смежных классов G/H. Что является ядром этого действия?

10.10. Пусть $G = S_3$. Покажите, что $Z(S_3) = e$ и $S_3 = \{e\} \cup \{(12),\ (13),\ (23)\} \cup \{(123),\ (132)\}$ — разбиение S_3 на сопряженные классы. Размеры этих классов (длины орбит) делят $6 = |S_3|$.

10.11. Каждая группа G действует транзитивно на множестве G/H левых смежных классов G по H.

10.12. Если G — транзитивная группа на $\Omega = \{1,\ \ldots,\ n\}$ и $i = g_i(1)$, то $G_i = g_i G_1 g_i^{-1}$ ($g_1 = e$), где G_i — стационарная подгруппа точки i, кроме того, элементы g_i можно выбрать в качестве представителей левых смежных классов G по G_1, т.е. $G = G_1 \cup g_2 G_1 \cup \ldots \cup g_n G_1$. В частности, $|\,G| = n|\,G_1|$.

10.13. Пусть $\Omega^{(k)}$ — совокупность упорядоченных k-элементных подмножеств. Группа G, действующая на Ω, индуцирует действие на $\Omega^{(k)}$; если при этом имеет место транзитивность на $\Omega^{(k)}$, то G называется *k-транзитивной* на Ω. Влечет ли $(k+1)$-транзитивность k-транзитивность?

Пусть G — транзитивная группа на Ω и $x \in \Omega$. Следующие условия равносильны:

а) G является $(k+1)$-транзитивной;

б) G_x действует k-транзитивно на множестве $\Omega \setminus \{x\}$, где G_x — стационарная подгруппа точки x.

10.14. Пусть G — конечная транзитивная группа на $\Omega = \{1,\ \ldots,\ n\}$, и для любого $g \in G$ пусть $N(g) = |\,\mathrm{Fix}(g)|$ — число точек в Ω, остающихся на месте при действии g. Тогда:

а) $\sum\limits_{g \in G} N(g) = |\,G|$;

б) если G есть 2-транзитивная группа, то $\sum\limits_{g \in G} N(g)^2 = 2|\,G|$.

10.15. Пусть группа G действует транзитивно на Ω, $x \in \Omega$ и H — подгруппа в G. Тогда:

а) H транзитивна (на Ω), если и только если $G_x H = G$;

б) H регулярна, если и только если $G_x H = G$ и $G_x \cap H = e$;

в) если H регулярна, то $|\,H| = |\,\Omega|$;

г) если H регулярна и конечно порождена, а G — 2-транзитивна на Ω, то $|\,\Omega| = p^k$ для некоторого простого числа p.

10.16. Пусть Ω — G-множество, $N \trianglelefteq G$ и N регулярна на Ω. Тогда $G = N \leftthreetimes G_x$ для всех $x \in \Omega$.

10.17. Пусть G — коммутативная транзитивная подгруппа в $S(\Omega)$. Тогда:

а) G регулярна;

б) G — максимальная коммутативная подгруппа в группе $S(\Omega)$.

10.18. Центр некоммутативной группы не транзитивен.

10.19. Пусть G — конечная транзитивная группа и $x \in \Omega$. Тогда $N_G(G_x)$ действует транзитивно на множестве $\mathrm{Fix}\,(G_x)$.

10.20. Пусть G — конечная группа, действующая на множестве Ω. Тогда $r\,(G : \Omega) = \frac{1}{|G|} \sum\limits_{g \in G} |\,\mathrm{Fix}(g)|$, где $r\,(G : \Omega)$ — число орбит группы G.

10.21. Пусть группа G действует транзитивно на Ω, H — подгруппа в G и $x \in \Omega$. Тогда:

а) если $G_x \subset H \subset G$ и $B = H(x)$, то $\{gB \,|\, g \in G\}$ есть система импримитивности группы G;

б) G примитивна, если и только если G_x — максимальная подгруппа в G.

10.22. Пусть H — подгруппа транзитивной группы перестановок G. Тогда если H транзитивна, регулярна или примитивна, то любая сопряженная с ней подгруппа H^g ($g \in G$) также транзитивна, регулярна или примитивна соответственно.

10.23. Если G — k-транзитивная подгруппа в S_n, то $|\,G|$ делится на $n(n-1)\ldots(n-k+1)$.

10.24. Покажите, что 2-транзитивная группа перестановок примитивна.

10.25. Если p — простое число, то любая транзитивная подгруппа группы S_p примитивна.

10.26. Пусть G — примитивная группа, действующая на Ω. Тогда если $e \subset N \trianglelefteq G$, то N транзитивна.

10.27. Группа, имеющая подгруппу индекса 2 (3 или 4), непроста.

10.28. Пусть коммутативная группа G действует на множестве Ω. Тогда если для некоторых $g \in G$ и $x_0 \in \Omega$ справедливо равенство $gx_0 = x_0$, то $gx = x$ для любой точки x, лежащей в одной орбите с x_0.

10.29. Каждое транзитивное действие группы G эквивалентно действию G на левых смежных классах по некоторой подгруппе H.

10.30. 1) Пусть группа $\mathrm{GL}(n, P)$ действует на векторном пространстве $M(n, P)$ матриц порядка n по правилу: $\Phi_A\colon X \to AX$ $(A \in \mathrm{GL}(n, P))$. Покажите, что $(\Phi, M(n, P))$ — вполне приводимое линейное представление Φ степени n^2, $\Phi = \Phi^{(1)} \oplus \ldots \oplus \Phi^{(n)}$, где $\Phi^{(i)} = \Phi \,|\, M_n^{(i)}$, а $M_n^{(i)}$ — подпространство матриц с единственным отличным от нуля i-м столбцом.

2) $\Phi_A : X \to A^{-1}XA$ также определяет линейное представление $\mathrm{GL}(n, P)$ на $M(n, P)$. Покажите, что множество $M^0(n, P)$ матриц с нулевым следом является инвариантным подпространством. Поэтому в случае поля нулевой характеристики имеет место разложение в прямую сумму $\mathrm{GL}(n, P)$-подпространств $M(n, P) = \langle E\rangle \oplus M^0(n, P)$ размерностей 1 и $n^2 - 1$, где E — единичная матрица.

3) Пусть предыдущем примере $P = \mathbb{R}$ и Φ — ограничение на ортогональную группу $O(n)$. Покажите, что получается линейное представление с разложением пространства представления $M(n, \mathbb{R})$ в прямую сумму $O(n)$-подпространств $M(n, \mathbb{R}) = \langle E\rangle \oplus M^+(n, \mathbb{R}) \oplus M^-(n, \mathbb{R})$ — одномерного пространства $\langle E\rangle$ скалярных матриц, $(n+2)(n-1)/2$-мерного пространства симметрических матриц с нулевым следом и $n(n-1)/2$-мерного пространства кососимметрических матриц. Хорошо известно взаимно однозначное соответствие между симметрическими (кососимметрическими) матрицами и соответствующими билинейными формами. Действие $O(n)$ на $\langle E\rangle \oplus M^+(n, \mathbb{R})$ и на $M^-(n, \mathbb{R})$ переносится на пространства соответствующих форм. Теорема о приведении квадратичной формы $f(x)$ к главным осям есть не что иное, как возможность выбора в $O(n)$-орбите, содержащей $f(x)$, диагональной формы $\sum_{i=1}^n \lambda_i x_i^2$ с вещественными λ_i, определенными однозначно с точностью до перестановки.

Заменяя $\mathbb{R}$ на $\mathbb{C}$ и $O(n)$ на унитарную группу, получаем разложение $M(n, \mathbb{C}) = \langle E\rangle \oplus M^+(n, \mathbb{C}) \oplus M^-(n, \mathbb{C})$.

10.31. Пусть G — группа перестановок, действующая на множестве Ω, $|\,\Omega| = n > 1$. Векторное пространство $V = \langle e_i \,|\, i \in \Omega\rangle$ над полем P нулевой характеристики с базисом, занумерованным элементами множества Ω, можно превратить в G-пространство, полагая $\Phi(g)(\sum\limits_{i\in\Omega} \lambda_i e_i) = \sum\limits_{i\in\Omega} \lambda_i e_{g(i)}$. Получается линейное представление степени n. Будет ли оно неприводимым?

10.32. 1) Эквивалентность двух одномерных представлений равносильна их совпадению, кроме того, представление степени 1 некоммутативной группы не является точным.

2) Одномерное представление циклической группы может быть неточным.

3) В случае $P = \mathbb{C}$ любая циклическая группа имеет точное одномерное представление.

4) Группа $\mathbb{Z}$ обладает неразложимыми комплексными представлениями сколь угодно высокой степени, не являющимися неприводимыми.

5) Циклическая группа $G = \langle a \,|\, a^n = e\rangle$ порядка n имеет ровно n попарно неэквивалентных неприводимых представлений над $\mathbb{C}$, все они одномерны и имеют вид $\Phi^{(m)}\colon a^k \mapsto \varepsilon^{mk}$, где $\varepsilon = e^{(2\pi\, i/n)}$ — примитивный корень степени n из 1, $m = 0, 1, \ldots, n-1$.

6) В случае циклической группы конечного порядка всякое комплексное линейное конечномерное представление вполне приводимо и $\Phi = \Phi^{(1)} \oplus \ldots \oplus \Phi^{(r)}$, где с точностью до эквивалентности $\Phi^{(m)}$ — одно из представлений из 5).

10.33. Пусть $G = \langle a \,|\, a^3 = e\rangle$ и $P = \mathbb{R}$. Двумерное представление (Φ, V), $V = \langle v_1, v_2\rangle$, заданное в указанном базисе матрицей $\Phi_a = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ неприводимо. Однако если рассматривать V над $\mathbb{C}$, то представление становится приводимым.

10.34. Пусть $P = \mathbb{R}$ и G — аддитивная группа вещественных чисел. Будут ли приводимыми двумерные представления, заданные в базисе $V = \langle v_1, v_2\rangle$ матрицами $\Phi(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ и $\Psi(t) = \begin{pmatrix} e^t & e^t - 1 \\ 0 & 1 \end{pmatrix}$?

10.35. Докажите теорему Машке в случае $P = \mathbb{C}$.

10.36. Всякое точное комплексное двумерное представление некоммутативной конечной группы неприводимо.

10.37. (Лемма Шура). Пусть (Φ, V), (Ψ, W) — два неприводимых комплексных представления группы G и $\sigma\colon V \to W$ — линейное отображение такое, что $\Psi(g)\,\sigma = \sigma\,\Phi(g)$ $(g \in G)$. Тогда:

а) если представления Φ, Ψ неэквивалентны, то $\sigma = 0$;

б) если $V = W$, $\Phi = \Psi$, то $\sigma = \lambda\, I$.

10.38. 1) Эквивалентные представления имеют равные характеры.

2) $\chi_\Phi(e) = \dim V$, кроме того, прямой сумме $\Phi = \Phi_1 \oplus \Phi_2$ представлений отвечает характер $\chi_\Phi = \chi_{\Phi_1} + \chi_{\Phi_2}$.

3) Характеры являются классовыми функциями.

4) Если $P = \mathbb{C}$, то $\chi_\Phi(g^{-1}) = \overline{\chi_\Phi(g)}$ (комплексная сопряженность) для любого $g \in G$ конечного порядка.

5) Элемент $g \in G$ конечного порядка сопряжен в G со своим обратным, если и только если $\chi_\Phi(g)$ — вещественное число.

6) Если χ — характер конечной группы G, то $(\chi, \chi) \leqslant \chi(1)^2$, причем $(\chi, \chi) = \chi(1)^2$, если и только если $\chi(1) = 1$.

10.39. Пусть G — конечная группа. Тогда:

а) если $V = V_1 \oplus \ldots \oplus V_k$ — разложение комплексного G-пространства V в прямую сумму неприводимых G-подпространств V_i, то для любого неприводимого G-пространства W с характером χ_W число слагаемых V_i, изоморфных W, равно $(\chi_V, \chi_W)_G$ и не зависит от способа разложения (*кратность вхождения* W в G-пространство V);

б) два комплексных представления группы G с одним и тем же характером изоморфны;

в) скалярный квадрат $(\chi_\Phi, \chi_\Phi)_G$ характера χ_Φ любого комплексного представления Φ является целым числом, равным 1 в точности тогда, когда Φ — неприводимое представление.

10.40. Центр конечной группы G, обладающей точным неприводимым представлением над $\mathbb{C}$, тривиален или циклический.

10.41. Каждое неприводимое представление конечной группы G над полем $\mathbb{C}$ входит в разложение регулярного представления ρ с кратностью, равной своей степени n_i, причем $\sum\limits_{i=1}^{r} n_i^2 = |G|$, где r — число классов сопряженности группы G.

Сведения о характерах неприводимых представлений записывают в виде таблицы, называемой *таблицей характеров*.

G	e	g_2	g_3	$\ldots$	g_r
χ_1	n_1	$\chi_1(g_2)$	$\chi_1(g_3)$	$\ldots$	$\chi_1(g_r)$
χ_2	n_2	$\chi_2(g_2)$	$\chi_2(g_3)$	$\ldots$	$\chi_2(g_r)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
χ_r	n_r	$\chi_r(g_2)$	$\chi_r(g_3)$	$\ldots$	$\chi_r(g_r)$

В верхней строке стоят представители всех r классов сопряженности группы G.

Например,

S_3	e	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

есть таблица характеров группы S_3.

10.42. Каждое неприводимое представление конечной коммутативной группы A над $\mathbb{C}$ имеет степень 1. Число таких попарно неэквивалентных представлений равно порядку $|A|$. Обратно, если каждое неприводимое представление группы A имеет степень 1, то A — коммутативная группа.

Пусть A — конечная коммутативная группа. Множество $\widehat{A} = \operatorname{Hom}(A, \mathbb{C}^*)$ гомоморфизмов группы A в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел, рассматриваемое вместе с поточечной операцией умножения $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ ($\chi_i \in \widehat{A}$, $a \in A$), называется *группой характеров* группы A над $\mathbb{C}$.

10.43. Группы A и $\widehat{A}$ изоморфны.

10.44. Пусть V_{2^n} — коммутативная группа порядка 2^n, порядок каждого неединичного элемента которой равен двум, χ — ее неприводимый комплексный характер такой, что $\chi(a) \neq 1$ для некоторого $a \in V_{2^n}$. Покажите, что $\operatorname{Ker}\chi = B \cong V_{2^{n-1}}$, и если $V_{2^n} = B \cup aB$ — разложение на смежные классы по B, то $\chi(a^i b) = (-1)^i$, $i = 0, 1$. Воспользовавшись этим, найдите таблицу характеров группы Клейна V_4.

10.45. Произведение конечного числа характеров группы G также есть характер этой группы. Кроме того, если $\chi, \gamma \in \operatorname{Irr} G$ и $\gamma(1) = 1$, то $\chi\gamma \in \operatorname{Irr} G$, причем условие $\gamma(1) = 1$ не может быть опущено.

10.46. Представления степени 1 конечной группы G находятся в биективном соответствии с неприводимыми представлениями факторгруппы G/G', где G' — коммутант группы G. Их число равно индексу $(G : G')$.

10.47. Пусть G — группа перестановок, действующая на множестве $\Omega = \{1, \ldots, n\}$, Φ — естественное представление группы G на пространстве $V = \langle e_1, \ldots, e_n \rangle$ с действием $\Phi(g)e_i = e_{g(i)}$.

Докажите, что естественное линейное представление (Φ, V) 2-транзитивной группы перестановок G над полем $\mathbb{C}$ является суммой единичного представления и еще одного неприводимого представления.

10.48. Пусть (Φ, V) — представление группы G и в V существует базис, в котором все операторы $\Phi(g)$ ($g \in G$) диагональны. Докажите, что $G' \subseteq \operatorname{Ker}\Phi$.

10.49. Пусть Φ — комплексное представление конечной группы G. Тогда каждый оператор $\Phi(g)$ $(g \in G)$ диагонализируем.

10.50. Всякое неприводимое неодномерное комплексное представление группы порядка p^3 является точным.

10.51. Найдите число неприводимых комплексных представлений некоммутативной группы порядка p^3 и их размерности.

10.52. Составьте таблицы характеров групп A_4, S_4, Q_8 и $\mathbb{Z}_n$.

10.53. Пусть A — конечная абелева группа. Тогда:

а) если A допускает точное комплексное неприводимое представление, то A — циклическая группа;

б) если B — подгруппа в A, то любой характер группы B продолжается до характера группы A и число таких продолжений равно индексу $(A : B)$.

10.54. 1) Если χ — характер группы G, то $\overline{\chi}$ также характер группы G, где $\overline{\chi}\colon g \mapsto \overline{\chi(g)}$.

2) Если $\chi \in \operatorname{Irr} G$, то $\overline{\chi} \in \operatorname{Irr} G$.

3) Если $\chi \in \operatorname{Irr} G$ и $\chi(1) = 2$, то группа G непроста.

4) Если H — подгруппа, а χ — характер группы G, причем $\chi|H \in \operatorname{Irr} H$, то $\chi \in \operatorname{Irr} G$.

10.55. Пусть Φ — n-мерное комплексное представление конечной группы G. Докажите, что $\chi_\Phi(g) = n$, если и только если $g \in \operatorname{Ker}\Phi$.

10.56. Пусть Φ — гомоморфизм группы G в $\mathrm{GL}(n, \mathbb{C})$. Тогда:

а) отображение $\Phi^*\colon g \mapsto (\Phi(g^{-1}))^t$ также является представлением группы G;

б) $\chi_\Phi(g) = \overline{\chi}_{\Phi^*}(g)$ для всякого $g \in G$;

в) представления Φ и Φ^* эквивалентны тогда и только тогда, когда значения характера χ вещественны.

10.57. Если Φ — представление группы G с характером χ, то $\{g \in G \mid \chi(g) = \chi(1)\} = \operatorname{Ker}\Phi \trianglelefteq G$.

10.58. Если $N \trianglelefteq G$, то обозначают $\operatorname{Irr}(G|N) = \{\chi \in \operatorname{Irr} G \mid N \subseteq \operatorname{Ker}\chi\}$. Покажите, что:

а) существует взаимно однозначное соответствие $\chi \mapsto \chi'$ из $\operatorname{Irr}(G|N)$ на $\operatorname{Irr}(G/N)$ такое, что $\chi'(gN) = \chi(g) = \chi(gn) = \chi(ng)$ для всех $g \in G$ и натуральных n;

б) $N = \bigcap\limits_{\chi \in \operatorname{Irr}(G\,|\,N)} \operatorname{Ker}\chi$;

в) $|\,C_G(g)| - |\,C_{G/N}(gN)| = \sum\limits_{\chi \in \operatorname{Irr} G \setminus \operatorname{Irr}(G\,|\,N)} |\chi(g)|^2$ для $g \in G$;

г) если $|\,C_N(g)| = 1$ для $g \in G$, то $|\,C_G(g)| = |\,C_{G/N}(gN)|$ и $\chi(g) = 0$ для всех $\chi \in \operatorname{Irr} G \setminus \operatorname{Irr}(G\,|\,N)$.

10.59. Пусть G — конечная группа, $g \in G$. Следующие условия равносильны:

а) $\chi(g) \in \mathbb{Q}$ для всех $\chi \in \operatorname{Irr} G$;

б) g сопряжен в G с любым элементом вида g^m, где m — такое натуральное число, что $(m, |G|) = 1$.

10.60. Все элементы таблицы характеров группы S_n — целые числа.

Глава III. Кольца

11 Общие свойства колец

Ассоциативным кольцом называется непустое множество R, на котором заданы две бинарные алгебраические операции $+$ и $\cdot$, удовлетворяющие следующим аксиомам:

1) $(R,+)$ — абелева группа;

2) $(R,\cdot)$ — полугруппа;

3) $(a+b)c=ac+bc$, $c(a+b)=ca+cb$ для всех $a,b,c\in R$ (умножение дистрибутивно по сложению).

Структура $(R,+)$ называется *аддитивной группой кольца* R, а $(R,\cdot)$ — его *мультипликативной полугруппой*. Если $(R,\cdot)$ — полугруппа с единицей (моноид), то говорят, что R — *кольцо с единицей* 1.

В дальнейшем все кольца, если специально не оговорено, предполагаются ассоциативными и с ненулевой единицей. При необходимости подчеркнуть роль единицы кольца R ее обозначают через 1_R. Будем говорить, что R — *кольцо без единицы* (или *предкольцо*), если наличие единичного элемента в R не предполагается. В таком случае единичный элемент игнорируется, даже если он существует.

Кольцо называется *коммутативным*, если $ab=ba$ для всех $a,b\in R$.

Если в вышеприведенном определении аксиома 2) устранена или заменена другой — в зависимости от конкретной задачи, — то говорят о *неассоциативных кольцах*.

Непустое подмножество K кольца R без единицы называется *подкольцом,* если из того, что $s,t\in K$, следует $s-t\in K$ и $st\in K$, т.е. если K — подгруппа аддитивной группы и подполугруппа мультипликативной полугруппы кольца. Для кольца R с единицей к этим двум условиям добавляется еще одно: $1\in K$.

Нейтральный элемент группы $(R,+)$ называется *нулем* кольца R и обозначается через 0. Если R состоит из одного элемента, то $0=1$, и в этом случае R называется *нулевым кольцом*.

Если $ab=0$ при $a\neq 0$ и $b\neq 0$ в кольце R, то a называется *левым,* а b — *правым* делителем нуля. Сам нуль в кольце $R\neq 0$ — тривиальный делитель нуля.

Элемент a кольца R называется *центральным*, если $ax=xa$ для всякого $x\in R$.

Кольцо, не имеющее ненулевых делителей нуля, называется *кольцом без делителей нуля* (*областью целостности*, или просто *областью*). Ненулевое коммутативное кольцо с единицей и без делителей нуля называется *коммутативной областью*.

Так же, как в полугруппах, элемент a кольца называется *идемпотентом*, если $a^2=a$.

Кольцо R с условием $a^2=a$ для любого $a\in R$ называется *булевым*.

Идемпотент $e\neq 0$ кольца называется *примитивным,* если e не может быть представлен в виде суммы двух ненулевых ортогональных идемпотентов. Говорят, что идемпотенты e и f кольца *ортогональны*, если $ef=fe=0$.

Кольцо называется *нормальным*, если все его идемпотенты центральны.

Элемент x кольца R называется *нильпотентным*, если $x^n=0$ для некоторого натурального числа n.

Кольцо без ненулевых нильпотентных элементов называется *редуцированным* кольцом.

Кольцо R называется *регулярным*, если каждый элемент его мультипликативной полугруппы регулярен.

Пусть R — кольцо с $1\neq 0$. Элемент $a\in R$ называется *обратимым* (или *делителем единицы*), если существует элемент $a^{-1}\in R$ со свойством $aa^{-1}=a^{-1}a=1$. Если $ab=1$ или $ba=1$, то говорят об элементах, *обратимых справа* или *слева*.

Кольцо, в котором каждый ненулевой элемент обратим, называется *кольцом с делением* или *телом*. Таким образом, в теле всегда $1\neq 0$. Коммутативное тело называется *полем*.

Если $(R,+,\cdot)$ и $(S,\oplus,\times)$ — два кольца, то они называются *изоморфными,* если существует биекция $f\colon R\to S$, сохраняющая операции, т.е. $f(a+b)=f(a)\oplus f(b)$, $f(a\cdot b)=f(a)\times f(b)$ для всех $a,b\in R$ и $f(1_R)=1_S$. Изоморфизм кольца на себя называется его *автоморфизмом*.

Задачи

11.1. Покажите, что в определении:

а) кольца аксиома коммутативности сложения выводится из остальных аксиом;

б) кольца без единицы аксиома коммутативности сложения не выводится из остальных аксиом;

в) кольца без единицы аксиома существования противоположного по сложению элемента не выводится из остальных аксиом.

11.2. Пусть $f\colon R \to S$ — изоморфизм колец. Проверьте, что:

а) если R — коммутативное, то и S — коммутативное и наоборот;

б) R не имеет делителей нуля тогда и только тогда, когда их не имеет S;

в) если v — обратимый элемент в R, то $f(v)$ обратим в S и $f\left(v^{-1}\right) = (f(v))^{-1}$.

11.3. 1) В любом кольце есть подкольцо, изоморфное одному из колец $\mathbb{Z}$, $\mathbb{Z}_n$.

2) Если в кольце R нет делителей нуля, то в R есть подкольцо, изоморфное одному из колец $\mathbb{Z}$, $\mathbb{Z}_p$ (p — простое число).

11.4. Пусть A — некоторое множество и a — произвольный его элемент. Определите кольцевые операции в A так, чтобы получилось кольцо (без единицы) и роль нуля в нем играл элемент a.

11.5. 1) Сколькими способами на множестве из двух элементов можно определить две бинарные операции «сложения» и «умножения» так, чтобы получилось кольцо без единицы?

2) Сколькими способами на множестве $\{a, b, c\}$ можно определить две бинарные операции «сложения» и «умножения» так, чтобы получилось кольцо без единицы, и роль нуля в нем играл элемент a?

3) Сколькими способами на множестве $\{a, b, c, d\}$ можно определить две бинарные операции «сложения» и «умножения» так, чтобы получились неизоморфные кольца без единицы?

11.6. Если R — кольцо и $r, s \in R$, то:

а) $0 \cdot r = r \cdot 0 = 0$; б) $(-r)s = r(-s) = -(rs)$;

в) $(-r)(-s) = rs$.

11.7. Если в кольце R каждое из уравнений $ax = b$, $ya = b$ ($a, b \in R$, $a \neq 0$) обладает хотя бы одним решением, то R является телом, причем если $1 \in R$, то достаточна разрешимость только одного уравнения.

11.8. 1) Во всяком кольце законы дистрибутивности выполняются и для разности, т.е. $(a-b)c = ac - bc$, $c(a-b) = ca - cb$, где полагаем $a - b = a + (-b)$.

2) В кольце с единицей и без делителей нуля каждый элемент, имеющий односторонний обратный, является обратимым.

11.9. Для элемента a кольца R и целого числа n положим

$$na = \begin{cases} \underbrace{a + \ldots + a}_{n}, & \text{если } n \geqslant 1; \\ 0 \text{ при } n = 0; \\ \underbrace{-a - \ldots - a}_{-n}, & \text{если } n \leqslant -1. \end{cases}$$

Покажите, что для любых $a, b \in R$ выполняются равенства $n(ab) = (na)b = a(nb)$.

11.10. Если элементы a и b кольца переставимы, то a переставим с $-b$, ab и b^{-1} (если последний существует). Если a переставим с b и c, то он переставим с элементами $b + c$ и bc.

Кольцо называется *чистым*, если каждый его элемент есть сумма идемпотентного и обратимого элемента.

11.11. Кольцо R локально (см. введение в § 13) тогда и только тогда, когда R чистое кольцо и не имеет идемпотентов, отличных от 0 и 1.

11.12. Пусть e — такой идемпотент кольца R, что eRe и $(1-e)R(1-e)$ чистые кольца. Тогда R — чистое кольцо.

11.13. Если R — чистое кольцо, то таково же кольцо матриц $M(n, R)$ для любого $n \geqslant 2$.

11.14. Любой элемент кольца R есть сумма n, $n > 1$, обратимых элементов тогда и только тогда, когда любой элемент факторкольца $R/J(R)$ есть сумма n обратимых элементов ($J(R)$ — радикал Джекобсона кольца R, см. введение в § 13).

11.15. Для любого кольца R всякая диагональная матрица над R порядка $\geqslant 2$ есть сумма двух обратимых матриц.

11.16. 1) Для любого кольца R любая $n \times n$ матрица над R, $n > 1$, есть сумма как трех, так и четырех обратимых матриц.

2) Существует кольцо R такое, что не всякая матрица порядка 2 над R есть сумма двух обратимых матриц.

11.17. Всякий линейный оператор векторного пространства V над полем F есть сумма двух обратимых линейных операторов, исключая случай, когда $\dim_F V = 1$ и $F = \mathbb{Z}_2$.

Кольцо R называется *n-чистым*, где n — фиксированное натуральное число, если каждый его элемент есть сумма идемпотента и n обратимых элементов. Упражнения 11.18 и 11.19 обобщают 11.12 и 11.13.

11.18. Пусть e — такой идемпотент кольца R, что eRe и $(1-e)R(1-e)$ — n-чистые кольца. Тогда R — n-чистое

кольцо.

11.19. Если R — n-чистое кольцо, то n-чистым будет кольцо матриц $M(k,R)$ для любого $k \geqslant 2$.

11.20. Все центральные элементы кольца R образуют подкольцо $Z(R)$. Оно называется *центром* кольца R.

11.21. Матрица A является центральным элементом в кольце $M(n,R)$ тогда и только тогда, когда A — скалярная матрица, т.е. $A = aE$ для некоторого $a \in Z(R)$ (E — единичная матрица порядка n). В частности, $Z(M(n,R)) \cong Z(R)$.

11.22. Определим *противоположное* (или *дуальное*) кольцо R° к заданному кольцу R. Множества элементов у колец R° и R совпадают, операции сложения в R° и R также совпадают. Операция $\circ$ умножения в R° определяется по операции умножения в R следующим образом: для любых $x, y \in R^\circ$ полагаем $x \circ y = yx$. Убедитесь, что R° действительно является кольцом.

11.23. Кольцо $M(n,\mathbb{R})$ $(n > 1)$ изоморфно своему противоположному кольцу.

Если R — кольцо, то можно рассмотреть всевозможные *многочлены*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \quad n \geqslant 0,$$

относительно *переменной* x ($x \notin R$) с *коэффициентами* $a_0, a_1, \ldots, a_n$ из R; если $a_n \neq 0$, то n называется *степенью* многочлена $f(x)$. Предполагается, что $ax = xa$ для любого $a \in R$. Если $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, то сумма $h(x) = f(x) + g(x)$ означает многочлен

$$h(x) = (a_0 + b_0) + (a_1 + b_1)\, x + \ldots + (a_k + b_k)\, x^k,$$

где $k = \max(n,m)$ и где коэффициенты a_i или b_i предполагаются равными 0, если индекс i больше, чем степень соответствующего многочлена.

Умножение $f(x)$ и $g(x)$ определяется по правилу: $q(x) = f(x)g(x) = \sum\limits_{r=0}^{n+m} c_r x^r$, где $c_r = \sum\limits_{i+j=r} a_i b_j$.

Над кольцом R можно также определить (формальные) *степенные ряды*

$$a_0 + a_1 x + \ldots + a_n x^n + \ldots = \sum_{n=0}^{\infty} a_n x^n (a_n \in R)$$

от переменной x. Определение операций с многочленов на степенные ряды переносится непосредственным образом:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n)\, x^n,$$

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{m=0}^{\infty} b_m x^m = \sum_{r=0}^{\infty} c_r x^r, \text{где } c_r = \sum_{n+m=r} a_n b_m.$$

Определим также (формальный) *ряд Лорана* от переменной x над кольцом R как выражение

$$a_n x^n + a_{n+1} x^{n+1} + \ldots + a_k x^k + \ldots = \sum_{k=n}^{\infty} a_k x^k \ (a_k \in R),$$

где n — любое целое, возможно, отрицательное число. Сложение и умножение рядов Лорана происходит аналогично сложению и умножению степенных рядов.

11.24. Множество всех многочленов образует кольцо $R[x]$, ассоциативно-коммутативное, если соответствующими свойствами обладает кольцо R. Аналогично определяется *кольцо многочленов* $R[x_1, \ldots, x_n]$ от *переменных* $x_1, \ldots, x_n$.

Множество всех степенных рядов с указанными сложением и умножением образует кольцо; оно называется *кольцом степенных рядов* от переменной x над кольцом R и обозначается через $R\,[[x]]$. Можно определить степенные ряды от нескольких переменных.

Множество всех рядов Лорана с указанными сложением и умножением образует кольцо, называемое *кольцом рядов Лорана* $R\langle x\rangle$ от переменной x над кольцом R.

11.25. 1) Многочлен с коэффициентами из коммутативного кольца R является нильпотентным элементом в кольце $R\,[x]$ тогда и только тогда, когда все его коэффициенты — нильпотентные элементы в R.

2) Приведите пример степенного ряда над кольцом R с нильпотентными коэффициентами, который не был бы нильпотентным в кольце $R\,[[x]]$.

11.26. Многочлен с коэффициентами из коммутативного кольца R обратим в $R\,[x]$ тогда и только тогда, когда его свободный член обратим в R, а остальные коэффициенты — нильпотентные элементы.

11.27. Кольцо рядов Лорана над полем является полем.

11.28. 1) Каждый элемент кольца $\mathbb{Z}_n$ либо обратим, либо является делителем нуля (см. 11.40 (г)).

2) $\mathbb{Z}_n$ является полем тогда и только тогда, когда $n = p$ — простое число.

3) $\mathbb{Z}_n$ содержит ненулевые нильпотентные элементы тогда и только тогда, когда n делится на квадрат натурального числа > 1.

11.29. Кольцо из 5 элементов с ненулевым умножением изоморфно $\mathbb{Z}_5$.

11.30. Если P — поле, то в кольце $M(n, P)$ вырожденные матрицы, и только они, являются делителями нуля.

11.31. Пусть R — кольцо, и $a, b \in R$. Докажите, что:

а) если элементы a и b обратимы, то элемент ab также обратим и $(ab)^{-1} = b^{-1}a^{-1}$;

б) если элементы ab и ba обратимы, то a и b также обратимы;

в) если R не имеет делителей нуля и произведение ab обратимо, то a и b обратимы, в общем же случае из обратимости элемента ab не следует обратимость a и b;

г) если обратим элемент $1 + ab$, то обратим и элемент $1 + ba$;

д) нильпотентность элемента a влечет обратимость элемента $1 + a$.

11.32. В бесконечном кольце R либо каждый ненулевой элемент обратим, либо число необратимых элементов бесконечно.

11.33. Пусть x — обратимый справа элемент некоторого кольца. Следующие условия эквивалентны:

а) x обладает более чем одним правым обратным;

б) x необратим;

в) x — левый делитель нуля.

11.34. Кольцо R будет телом тогда и только тогда, когда для любого $a \neq 1$ найдется элемент $b \in R$ такой, что $a + b - ab = b + a - ba = 0$.

11.35. Покажите, что матрицы $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$:

а) с $a, b \in F_3$ образуют поле из 9 элементов и что мультипликативная группа этого поля — циклическая порядка 8;

б) с вещественными a и b образуют поле, изоморфное полю комплексных чисел.

11.36. Матрицы $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a и b образуют поле, изоморфное полю $\mathbb{Q}(\sqrt{2})$.

11.37. Множество 2^M всех подмножеств множества M является коммутативным кольцом с 1, все элементы аддитивной группы которого имеют порядок два, относительно операций симметрической разности $A + B = A \Delta B$ и пересечения $AB = A \cap B$. Это кольцо называется *кольцом всех подмножеств множества* M.

11.38. Пусть R — произвольное кольцо, X — произвольное множество. Тогда через R^X обозначают *кольцо функций*. Его элементами являются функции $f\colon X \to R$, а операции сложения и умножения определяются следующим образом: если $f, g \in R^X$ и $x \in X$, то $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. Убедитесь, что R^X действительно кольцо.

11.39. Если все элементы коммутативного кольца имеют общий делитель a, то кольцо обладает единицей.

11.40. Пусть R — конечное кольцо (не обязательно с 1). Тогда:

а) если R не содержит делителей нуля, то оно является телом;

б) если R содержит единицу, то каждый его элемент, имеющий односторонний обратный, обратим;

в) если R имеет единицу, то всякий левый делитель нуля является правым делителем нуля;

г) если R имеет единицу, то всякий его элемент либо обратим, либо является делителем нуля;

д) если $|R| = n$, то $na = 0$ для каждого $a \in R$.

11.41. Каково наименьшее число n такое, что существует некоммутативное кольцо без единицы с n элементами?

Примером неассоциативного кольца служит кольцо векторов трехмерного евклидова пространства, в котором операциями служат обычные сложение и векторное произведение.

Хорошо известно, что в этом кольце для любых его элементов выполняются следующие соотношения:

(1) $a^2 = 0$ и (2) $(ab)\,c + (bc)\,a + (ca)\,b = 0$ — *тождество Якоби*. Всякое кольцо, удовлетворяющее условиям (1) и (2), называется *лиевым кольцом*.

11.42. 1) Из вышеприведенного условия (1) вытекает *закон антикоммутативности* $ba = -ab$.

2) Если R — произвольное ассоциативное кольцо, то, сохраняя аддитивную группу этого кольца, а операцию умножения xy заменяя *операцией коммутирования* $x \circ y = xy - yx$, получим лиево кольцо. Элемент $[x, y] = xy - yx$ часто называется *коммутатором* элементов x и y. Коммутатор $[x, y]$ является билинейной знакопеременной функцией от x, y. Это означает, что $[x, y] = -[y, x]$, так что тождество Якоби $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$

можно записать в виде $[[x,y],z]=[x,[y,z]]+[y,[z,x]]$. Тождество $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ также называют тождеством Якоби. Положим по индукции $[x_1,\dots,x_n]=[[x_1,\dots,x_{n-1}],x_n]$, при этом обозначении справедливо тождество $[x,y,z,t]+[y,x,t,z]+[z,t,x,y]+[t,z,y,x]=0$.

Покажите, что если кольцо R удовлетворяет тождеству $[x,y,z]=0$, то для любых натуральных чисел m,n,s,t в R справедливы тождества:

а) $[x^m,y]=mx^{m-1}[x,y]$;

б) $[x^ny^m,x^sy^t]=(nt-ms)x^{n+s-1}y^{m+t-1}[x,y]$;

в) $[x^ny^n,x^sy^s]=0$.

3) Для кольца R с единицей следующие условия эквивалентны:

а) $[a,b]\in Z(R)$ для любых $a,b\in R$;

б) $[[a,b],c]=[a,[b,c]]$ для любых $a,b,c\in R$;

в) $[a,b,c]=[a,c,b]$ для любых $a,b,c\in R$;

г) $[a,bc]=[a,cb]$ для любых $a,b,c\in R$;

д) $[[a,b]c,d]=[a,b][c,d]$ для любых $a,b,c,d\in R$.

4) Всякое лиево ненулевое кольцо является кольцом без единицы.

11.43. Если A — ненулевая абелева группа, то кольцо эндоморфизмов $\operatorname{End}(A\oplus A)$ некоммутативное.

11.44. В ассоциативном кольце R сохраним его аддитивную группу, а операцию умножения ab заменим *операцией симметрирования* $a\cdot b=ab+ba$. Покажите, что получается новое кольцо, в котором выполняются соотношения: (1) $a\cdot b=b\cdot a$ и (2) $[(a\cdot a)\cdot b]\cdot a=(a\cdot a)\cdot(b\cdot a)$ (кольцо, в котором выполняются (1) и (2), называется *йордановым*).

В общем случае йордановы кольца неассоциативны. Заметим, что все ассоциативно-коммутативные кольца являются йордановыми.

Пусть R — произвольное (не обязательно ассоциативное) кольцо. *Дифференцированием* кольца R называется всякое преобразование δ множества R, являющееся эндоморфизмом аддитивной группы R^+ кольца R, т.е. $\delta(a+b)=\delta a+\delta b$, и удовлетворяющее условию $\delta(ab)=(\delta a)b+a(\delta b)$, $a,b\in R$.

Элемент a кольца R называется *константой относительно дифференцирования* δ, если $\delta a=0$.

11.45. Покажите, что дифференцирования кольца R составляют лиево кольцо, а именно подкольцо лиева кольца эндоморфизмов аддитивной группы R^+ кольца R, т.е. проверьте, что:

а) нулевой эндоморфизм является дифференцированием;

б) если δ_1 и δ_2 — дифференцирования кольца R, то эндоморфизм его аддитивной группы $\delta_1+\delta_2$ также будет дифференцированием;

в) эндоморфизм $-\delta$, противоположный дифференцированию δ, сам будет дифференцированием;

г) лиево произведение $\delta_1\circ\delta_2=\delta_1\delta_2-\delta_2\delta_1$ дифференцирований δ_1 и δ_2 само будет дифференцированием.

Покажите, что константы составляют в R подкольцо, а в поле — подполе.

11.46. Найдите все дифференцирования колец:

а) $\mathbb{Z}$; б) $\mathbb{Z}[x]$; в) $\mathbb{Z}[x_1,\dots,x_n]$.

11.47. 1) Булево кольцо R коммутативно и его элементы a удовлетворяют тождеству $a+a=0$.

2) Коммутативное кольцо R является булевым тогда и только тогда, когда оно не имеет нильпотентных элементов и $(a+b)ab=0$ для всех $a,b\in R$.

3) Пусть $(B,+,\cdot,')$ — булева алгебра. Для $a,b\in B$ положим $a\oplus b=ab'+a'b$ и $a\circ b=ab$. Тогда $(B,\oplus,\circ)$ становится булевым кольцом.

4) Пусть $(R,\oplus,\circ)$ — булево кольцо. Положим $a+b=(a\oplus b)\oplus(a\circ b)$ и $ab=a\circ b$. Тогда R становится булевой алгеброй B. Кольцо, получаемое из алгебры B с помощью 3), совпадает с R. Применение описанной в 4) конструкции к кольцу, указанному в 3), приводит к исходной алгебре B.

Более широкий класс образуют *альтернативные кольца*, т.е. те кольца, в которых ассоциативны все подкольца, порожденные двумя элементами. Классический пример альтернативного кольца — алгебра Кэли (см. 12.75).

Если a,b,c — элементы некоторого кольца, то назовем *ассоциатором* этих элементов элемент $[a,b,c]=(ab)c-a(bc)$.

11.48. Всякое кольцо, все подкольца которого, порожденные тремя элементами, ассоциативны, само ассоциативно.

Ассоциатор дистрибутивен по каждому своему аргументу. Далее, равенство $[a,b,c]=0$ равносильно тому, что для элементов a,b,c выполняется закон ассоциативности $(ab)c=a(bc)$. Кроме того, следующие условия эквивалентны:

а) кольцо R альтернативно;

б) $[a,a,b]=0$, $[a,b,a]=0$, $[b,a,a]=0$ для любых $a,b\in R$;

в) в кольце R выполняются два тождества из трех, указанных в б).

Если в кольце элементы a, b, c подвергнуты некоторой перестановке, то ассоциатор $[a, b, c]$ не меняется, если эта перестановка четная, и меняет знак, если она нечетная.

11.49. Если e — идемпотент кольца R, то:

а) $1 - e$ — также идемпотент;

б) $t = e + (1 - e)xe$ — также идемпотент для любого $x \in R$; кроме того, для всякого такого t найдется $y \in R$ со свойством $e = t + (1 - t)yt$;

в) множество $eRe = \{ere \,|\, r \in R\}$ — кольцо относительно операции умножения, индуцированной соответствующей операцией кольца R;

г) e примитивен тогда и только тогда, когда кольцо eRe не содержит идемпотентов, отличных от 0 и e.

11.50. Все обратимые элементы кольца R образуют группу $U(R)$ относительно умножения. Найдите группу обратимых элементов следующих колец:

а) $\mathbb{Z}$; б) $\mathbb{Z}_n$; в) $\mathbb{Z}[i]$;

г) кольца верхних треугольных матриц над полем.

Будут ли группы $U(\mathbb{Z}_4)$, $U(\mathbb{Z}_6)$, $U(\mathbb{Z}_8)$ циклическими?

Покажите, что группа $U(\mathbb{Z}[\sqrt{3}])$ бесконечна.

11.51. Пусть элементы a и b кольца R таковы, что $ab = 1$ и $ba \neq 1$. Покажите, что:

а) элементы b^2a^2, $ba - b^2a^2$, $1 - ba + b^2a^2$ — идемпотенты;

б) в R при любом натуральном n можно указать n попарно ортогональных идемпотентов, т.е. таких идемпотентов $e_1, \ldots, e_n$, что $e_ie_j = 0$ при $i \neq j$.

11.52. Степенной ряд $f = \sum\limits_{k=0}^{\infty} a_kx^k$ обратим в кольце $R\,[[x]]$ в точности тогда, когда a_0 — обратимый элемент кольца R.

11.53. Числа ± 1, $\pm i$ суть корни уравнения $x^4 = 1$ над полем комплексных чисел. Рассмотрим уравнение $x^3 = 1$. Так как $x^3 - 1 = (x - 1)\left(x^2 + x + 1\right)$, то его корнями будут 1 и $(-1 \pm \sqrt{-3})/2$. Пусть $\omega = (-1 + \sqrt{-3})/2$. Нетрудно проверить, что $\omega^2 = (-1 - \sqrt{-3})/2$ и что $1 + \omega + \omega^2 = 0$. Покажите, что множество $\mathbb{Z}[\omega] = \{m + n\omega \,|\, m, n \in \mathbb{Z}\}$ образует коммутативную область относительно сложения и умножения.

Проверьте, что комплексно сопряженное число $\overline{\omega}$ совпадает с ω^2. Используя это, докажите, что кольцо $\mathbb{Z}[\omega]$ замкнуто относительно комплексного сопряжения.

Покажите, что всякое число $m+n\omega$ можно записать в более явном виде $m+n\omega = m+n\dfrac{-1+\sqrt{-3}}{2} = \dfrac{(2m-n)+n\sqrt{-3}}{2}$. Используя это, докажите, что:

а) кольцо $\mathbb{Z}[\omega]$ совпадает с кольцом чисел вида $\dfrac{p + q\sqrt{-3}}{2}$, где p и q — целые числа одинаковой четности;

б) $\mathbb{Z}[\sqrt{-3}]$ является подкольцом в $\mathbb{Z}[\omega]$;

в) число 3 не является простым в $\mathbb{Z}[\omega]$.

Пусть $\widehat{\mathbb{Z}}_p$ — множество формальных степенных рядов вида $\xi = s_0 + s_1p + \ldots + s_np^n + \ldots$, где p — некоторое фиксированное простое число, а $s_n = 0, 1, \ldots, p - 1$; ξ называется *целым p-адическим числом*. Если $\zeta = r_0 + r_1p + \ldots + r_np^n + \ldots$ — другое целое p-адическое число, то сумма $\xi + \zeta = q_0 + q_1p + \ldots + q_np^n + \ldots$, произведение $\xi\zeta = q'_0 + q'_1p + \ldots + q'_np^n + \ldots$ определяются так: $q_0 = s_0 + r_0 - k_0p$, $q_n = s_n + r_n + k_{n-1} - k_np$, $q'_0 = s_0r_0 - m_0p$, $q'_n = s_0r_n + s_1r_{n-1} + \ldots + s_nr_0 + m_{n-1} - m_np$ $(n = 1, 2, \ldots)$, где целые числа k_0, k_n, m_0, m_n однозначно определяются тем условием, что все числа q_0, q_n и q'_0, q'_n лежат между 0 и $p - 1$. Получающаяся так коммутативная область $\widehat{\mathbb{Z}}_p$ называется *кольцом целых p-адических чисел*. Отметим, что $|\widehat{\mathbb{Z}}_p| = 2^{\aleph_0}$.

11.54. 1) Противоположным к числу

$$\xi = s_np^n + s_{n+1}p^{n+1} + \ldots \quad (s_n \neq 0)$$

является число

$$-\xi = (p - s_n)p^n + (p - s_{n+1} - 1)p^{n+1} + \ldots .$$

2) Обратный элемент ξ^{-1} для $\xi = s_0 + s_1p + \ldots + s_np^n + \ldots$ существует если и только если $s_0 \neq 0$, его можно найти методом неопределенных коэффициентов, группа $U(\widehat{\mathbb{Z}}_p)$ состоит из всех таких чисел ξ.

3) Множество $\widehat{\mathbb{Z}}_{p^\infty}$ «дробных» p-адических чисел вида $\sum\limits_{n=-k}^{\infty} s_np^n$, $0 \leqslant s_n < p$, образует уже *поле p-адических чисел.*

Пусть R — кольцо, G — группа. Определим *групповое кольцо* RG группы G над кольцом R. Его элементами являются всевозможные формальные конечные суммы вида $\sum\limits_{g\in G} r_g g$, $r_g \in R$, а операции определяются формулами:

$$\sum_{g\in G} r_g g + \sum_{g\in G} s_g g = \sum_{g\in G} (r_g + s_g)\, g,$$

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{h\in G} s_h h\right) = \sum_{t\in G} u_t t, \text{ где } u_t = \sum_{gh=t} r_g s_h \in R.$$

11.55. Покажите, что RG является кольцом для любого кольца R и любой группы G, причем это утверждение остается справедливым, если G — произвольная полугруппа с единицей. Кольцо многочленов $R[x]$ является частным случаем этой конструкции (в качестве G нужно взять полугруппу, состоящую из всех неотрицательных степеней x).

Отображения $r \to re$, $r \in R$ (e — единичный элемент группы G), и $g \to 1g$, $g \in G$, являются, соответственно, вложением (см. § 12) кольца R в кольцо RG и вложением группы G в группу обратимых элементов кольца RG.

Элементы r и g отождествляют с их образами при указанных вложениях. Получается, что единичный элемент e является единицей в RG.

11.56. Групповое кольцо $\mathbb{Z}G$ называется *целочисленным*. Если G — циклическая группа порядка 2 или 3, то обратимые элементы целочисленного группового кольца $\mathbb{Z}G$ исчерпываются элементами $\pm g$ ($g \in G$). Это не так для группы G порядка 5.

11.57. Если G — конечная группа, то кольцо $\mathbb{Z}G$ имеет делители нуля и в нем нет идемпотентов, кроме 0 и 1.

11.58. Пусть G — конечная группа. Тогда если элемент $n \cdot 1$, где $n = |G|$, обратим в кольце R, то элемент $(n\cdot 1)^{-1} \sum\limits_{g\in G} g$ является идемпотентом в групповом кольце RG.

В упражнении 11.24 введено кольцо многочленов $R[x]$ от переменной x над кольцом R. В следующих трех упражнениях указываются новые операции умножения многочленов. При этом получаются другие кольца многочленов.

11.59. Пусть α — некоторый автоморфизм кольца R. Сохраним прежнее сложение многочленов и зададим новое умножение многочленов равенством $xa = \alpha(a)x$ ($a \in R$) и его следствиями (смысл этого поясняется ниже). Проверьте, что множество всех многочленов с данными операциями сложения и умножения образует кольцо. Оно называется *кольцом косых многочленов* от переменной x над кольцом R и обозначается $R[x,\alpha]$. Ясно, что для тождественного автоморфизма α кольцо $R[x,\alpha]$ совпадает с $R[x]$. Разберитесь, как умножаются многочлены в кольце $R[x,\alpha]$. В силу дистрибутивности для этого достаточно определить значение произведения $ax^m \cdot bx^n$. Проверьте, что оно равно $a\alpha^m(b)\, x^{m+n}$.

11.60. Пусть δ есть дифференцирование кольца R (см. 11.45). Тогда множество всех многочленов от переменной x над кольцом R является также кольцом относительно обычного сложения многочленов и умножения, которое определяется равенством $xa = ax + \delta(a)$ ($a \in R$) и его следствиями. Это кольцо называется *кольцом дифференциальных многочленов* и обозначается $R[x,\delta]$. Проверьте, что $R[x,\delta]$ действительно кольцо. Вычислите произведение ax^m на bx^n в этом кольце.

11.61. Конструкции колец многочленов из упражнений 11.59 и 11.60 можно объединить следующим образом. Пусть снова α — автоморфизм кольца R. Отображение $\delta\colon R \to R$ называется *α-дифференцированием* кольца R, если $\delta(a+b) = \delta(a) + \delta(b)$ и $\delta(ab) = \delta(a)\alpha(b) + a\delta(b)$ для любых $a, b \in R$. Докажите, что получится кольцо многочленов, обозначаемое $R[x,\alpha,\delta]$, если сохранить то же сложение, а умножение задать равенством $xa = \alpha(a)x + \delta(a)$ ($a \in R$) и его следствиями. Если α — тождественный автоморфизм, то приходим к кольцу дифференциальных многочленов $R[x,\delta]$, а при $\delta = 0$ получаем кольцо косых многочленов $R[x,\alpha]$. Выясните, как перемножаются в кольце $R[x,\alpha,\delta]$ $\quad ax^m$ и bx^n.

12 Факторкольца и гомоморфизмы

Подмножество I кольца R (с единицей или без единицы) называется *левым* (соответственно, *правым*) *идеалом*, если $a-b \in I$ и $ra \in I$ (соответственно, $a-b \in I$ и $ar \in I$) для любых $a, b \in I$ и $r \in R$. Подразумевая один из этих идеалов, говорят *односторонний идеал*. *Двусторонним идеалом* или просто *идеалом* кольца R называют подмножество I, являющееся одновременно левым и правым идеалом, т.е. справедливы включения $a - b \in I$ и $ra, ar \in I$ при всех $a, b \in I$ и $r \in R$. В кольце без единицы каждый односторонний идеал является подкольцом.

Пересечение любого семейства левых (правых, двусторонних) идеалов кольца R (с единицей или без единицы) снова является идеалом того же вида. Поэтому для каждого непустого подмножества $A \subseteq R$ существуют три наименьших идеала, порожденных множеством A: левый, правый и двусторонний. В случае конечности A, эти идеалы называются *конечно порожденными*. Если A состоит из одного элемента a, то соответствующие идеалы

называют *главным левым* (соответственно, *правым* и *двусторонним*) *идеалом*, порожденным a. Идеал, порожденный подмножеством A, обозначают (A). Если A состоит из одного элемента a, то пишут (a).

Коммутативная область, все идеалы которой главные, называется *коммутативной областью главных идеалов*.

Кольцо, в котором каждый правый (левый) идеал главный, называется *кольцом главных правых* (*левых*) идеалов. Кольцо, в котором каждый правый и левый идеал главный, называется *кольцом главных* идеалов.

Кольцо R, не имеющее двусторонних идеалов, отличных от 0 и R, называется *простым*.

Всякий идеал I кольца R определяет факторкольцо R/I. На множестве идеалов кольца R определены операции: *сумма* $I+J=\{a+b\,|\,a\in I, b\in J\}$, *пересечение* $I\cap J$ и *произведение* $IJ=\{\sum\limits_{i=1}^{n} a_ib_i\,|\,a_i\in I, b_i\in J, n\in\mathbb{N}\}$. Всегда $IJ\subseteq I\cap J$.

Отображение f кольца R в кольцо S (кольца без единицы) называется *кольцевым гомоморфизмом*, если $f(a+b)=f(a)+f(b)$ и $f(ab)=f(a)f(b)$ для всех $a,b\in R$. Для колец с единицей добавляется условие $f(1_R)=1_S$. Сюръективный гомоморфизм называют иногда *наложением*, а инъективный — *мономорфизмом* или *вложением*. Гомоморфизм кольца в себя называется его *эндоморфизмом*.

Пусть R — декартово произведение колец $R_1,\dots,R_m$. Определим в R операции $+$ и $\cdot$ по правилам:

$$(r_1,\dots,r_m)+(s_1,\dots,s_m)=(r_1+s_1,\dots,r_m+s_m),$$

$$(r_1,\dots,r_m)\cdot(s_1,\dots,s_m)=(r_1s_1,\dots,r_ms_m).$$

Тогда R становится кольцом, называемым *внешней прямой суммой колец* и обозначаемым через $R=R_1\oplus\ldots\oplus R_m$ или $R=\bigoplus\limits_{i=1}^{m} R_i$. Пишут также $R=R_1\times\ldots\times R_m=\prod\limits_{i=1}^{m} R_i$ и говорят, что R — *прямое произведение* колец $R_1,\dots,R_m$.

Если $I_1,\dots,I_m$ — идеалы кольца R со свойствами $R=I_1+\ldots+I_m$ и $I_j\cap(\sum\limits_{k\neq j} I_k)=0$, то в этом случае говорят, что R является (*внутренней*) *прямой суммой* своих идеалов $I_1,\dots,I_m$, и пишут $R=I_1\oplus\ldots\oplus I_m$. Различие между внутренними и внешними прямыми суммами колец — чисто теоретико-множественное, так как если $R=R_1\oplus\ldots\oplus R_m$, то $I_j=\{(0,\dots,x_j,\dots,0)\,|\,x_j\in R_j\}\cong R_j$, I_j — идеал в R и $R=I_1\oplus\ldots\oplus I_m$. И наоборот, если $R=I_1\oplus\ldots\oplus I_m$, то, записав $1=e_1+\ldots+e_m$ ($e_j\in I_j$), получаем, что I_j — кольцо с единицей e_j $(j=1,\dots,m)$ и R изоморфно внешней прямой сумме колец $I_1,\dots,I_m$. Действительно, любой элемент $r\in R$ единственным образом представляется в виде суммы $r=x_1+\ldots+x_m$, где $x_j\in I_j$. Указанный изоморфизм сопоставляет элементу r элемент $(x_1,\dots,x_m)$. Понятие прямого произведения колец можно распространить на произвольное бесконечное множество колец R_i, $i\in I$. Если $R=\prod\limits_{i\in I} R_i$, то каждый элемент $r\in R$ представим в виде $r=(\dots,r_i,\dots)$, $r_i\in R_i$; для каждого $i\in I$ определено наложение $\pi_i\colon R\to R_i$, $\pi_i(r)=r_i$; π_i называется *канонической проекцией* кольца R на прямой множитель R_i. Если $R=\prod\limits_{i\in I} R_i$ и $f_i\colon R_i\to S_i$ — кольцевые гомоморфизмы, то $f(\dots,x_i,\dots)=(\dots,f(x_i),\dots)$ — кольцевой гомоморфизм $f\colon R\to\prod\limits_{i\in I} S_i$, f называется *прямым произведением* гомоморфизмов f_i, $i\in I$, и обозначается $f=(\dots,f_i,\dots)$.

Если S — непустое подмножество в кольце R, то его *централизатор* $C_R(S)=\{x\in R\,|\,xy=yx,\ y\in S\}$ является подкольцом в R; через $r_R(S)=\{x\in R\,|\,Sx=0\}$ и $\ell_R(S)=\{x\in R\,|\,xS=0\}$ обозначается, соответственно, *правый* и *левый аннуляторы* подмножества S в кольце R (индексы иногда опускаются). Правый (соответственно, левый) идеал I называется *аннуляторным*, если $I=r(S)$ (соответственно, $I=\ell(S)$) для некоторого подмножества S кольца R.

Элемент a кольца R называется *регулярным справа* (*слева*) в R, если $r(a)=0$ ($\ell(a)=0$).

Алгеброй (линейной) K над полем P называют кольцо K, являющееся векторным пространством над полем P, при этом умножение на скаляры (элементы из поля P) и умножение в кольце переставимы: $\alpha(a\cdot b)=(\alpha a)\cdot b=a\cdot(\alpha b)$, $\alpha\in P$, $a,b\in K$. Алгебра называется *конечномерной*, если она конечномерна как векторное пространство.

Если K — конечномерная алгебра над полем P с базисом $u_1,\dots,u_n$, то умножение слева на каждый элемент $t\in K$ является линейным оператором векторного P-пространства K. Определитель $|T|$ матрицы этого оператора, как известно, не зависит от выбора базиса, и называется *нормой* элемента t: $N(t)=|T|$. След $S(T)$ матрицы, тоже не зависящий от выбора базиса, называется *следом* $S(t)$ элемента t. Итак, $S(t)=S(T)=\sum\limits_{i=1}^{n} t_{ii}$.

Теорема 12.1 (основная теорема о гомоморфизмах). *Каждый идеал I кольца K определяет структуру кольца на фактормножестве K/I, причем K/I является гомоморфным образом кольца K с ядром I. Обратно, каждый гомоморфный образ $f(K)$ кольца K изоморфен факторкольцу $K/\operatorname{Ker} f$.*

Теорема 12.2 (первая теорема об изоморфизме). *Пусть K — кольцо, L — подкольцо, I — идеал в K. Тогда $L+I=\{x+y\,|\,x\in L,\ y\in I\}$ — подкольцо в K, содержащее I в качестве идеала, $L\cap I$ — идеал в L. Отображение*

$$\varphi\colon\ x+I\mapsto x+(L\cap I),\ x\in L,$$

осуществляет изоморфизм колец: $(L+I)/I \cong L/(L\cap I)$.

Теорема 12.3 (вторая теорема об изоморфизме). *Пусть K — кольцо, L — его подкольцо, а I — идеал в K и $I\subset L$. Тогда $\overline{L}=L/I$ — подкольцо в $\overline{K}=K/I$ и соответствие $L\to\overline{L}$ является биекцией множества подколец в K, содержащих I, на множество всех подколец кольца $\overline{K}$. Кроме того, L — идеал в K тогда и только тогда, когда $\overline{L}$ — идеал в $\overline{K}$, причем $K/L\cong\overline{K}/\overline{L}=(K/I)/(L/I)$.*

Теорема 12.4 (китайская теорема об остатках). *Если K — кольцо, $I_1,\dots,I_n$ — его идеалы со свойством $I_i+I_j=K$ для $1\leqslant i\neq j\leqslant n$, то отображение $\varphi\colon x\mapsto(x+I_1,\dots,x+I_n)$ является сюръективным гомоморфизмом кольца K в $S=K/I_1\oplus\ldots\oplus K/I_n$ с ядром $\operatorname{Ker}\varphi=I_1\cap\ldots\cap I_n$.*

Если K — коммутативная область и $a_1,\dots,a_n$ — ее попарно взаимно простые элементы, т.е. $a_iK+a_jK=K$ при $i\neq j$, то из теоремы 12.4 следует, что для любых $x_1,\dots,x_n\in K$ найдется элемент $x\in K$ со свойством $x\equiv x_i\pmod{a_i}$, $i=1,\dots,n$, где под сравнением $x\equiv x_i\pmod{a_i}$ понимается, что $x-x_i\in a_iK$.

Говорят, что кольцо R является *подпрямым произведением* колец R_i, $i\in I$, если существует вложение $f\colon R\to S=\prod\limits_{i\in I}R_i$, для которого $\pi_i\circ f$ — наложения для всех $i\in I$, $\pi_i\colon S\to R_i$ — каноническая проекция.

Задачи

12.1. Изоморфны ли поля $\mathbb{Q}$ и $\mathbb{R}$, $\mathbb{R}$ и $\mathbb{C}$, $\mathbb{Q}$ и $\mathbb{Q}(\sqrt{2})$?

12.2. Распространите понятие суммы и произведения идеалов на любое (в том числе и бесконечное) семейство идеалов кольца R.

12.3. Проверьте выполнение аксиом кольца и гомоморфные свойства проекций для прямого произведения колец.

12.4. 1) Объединение двух идеалов является идеалом тогда и только тогда, когда один из них содержится в другом.

2) Если идеал I содержится в объединении идеалов J и L, то либо $I\subseteq J$, либо $I\subseteq L$.

3) Вполне инвариантные подгруппы группы R^+ являются идеалами в кольце R.

12.5. Объединение линейно упорядоченного семейства подколец (идеалов) кольца снова является подкольцом (идеалом) этого кольца.

12.6. Пусть R — прямая сумма колец $R_1,\dots,R_m$ без единицы.

1) При каких условиях R коммутативно, имеет единицу, не имеет делителей нуля?

2) Найдите в R все обратимые элементы, все делители нуля, все нильпотентные элементы.

12.7. Всякое кольцо без единицы R изоморфно вкладывается в кольцо с единицей. Если при этом кольцо R ассоциативно или коммутативно, то его можно вложить, соответственно, в ассоциативное или коммутативное кольцо с единицей.

12.8. Кольцо линейных операторов конечномерного векторного пространства является простым.

12.9. Если числа k и l взаимно простые, то $\mathbb{Z}_{kl}\cong\mathbb{Z}_k\oplus\mathbb{Z}_l$.

12.10. В кольце матриц $M(n,R)$ над кольцом R идеалами являются в точности множества матриц, элементы которых принадлежат фиксированному идеалу кольца R.

Кольцо матриц над полем является простым (см. 12.8).

12.11. 1) Если идеал содержит обратимые элементы, то этот идеал совпадает со всем кольцом.

2) Если кольцо является суммой некоторого семейства идеалов, то оно является конечной суммой некоторых из них.

12.12. Множество I_S непрерывных функций, обращающихся в 0 на фиксированном подмножестве $S\subseteq[a,b]$, является идеалом в кольце функций, непрерывных на $[a,b]$.

Верно ли, что всякий идеал этого кольца имеет вид I_S для некоторого $S\subseteq[a,b]$?

12.13. Докажите, что ненулевое коммутативное кольцо R, не имеющее нетривиальных идеалов, является полем. Существенно ли для этого утверждения наличие единицы?

12.14. 1) Кольцо R без нетривиальных односторонних идеалов, в котором для каждого $0\neq a\in R$ найдутся такие $b,c\in R$, что $ab\neq 0$ и $ca\neq 0$, является телом (наличие единицы в кольце изначально не предполагается).

2) Кольцо с 1 и без делителей нуля, в котором всякая убывающая цепочка левых идеалов конечна, является телом.

12.15. Пусть $n>1$ и $1\leqslant k\leqslant n$. Покажите, что:

а) матрицы с нулевой k-й строкой образуют правый, но не левый идеал кольца $M(n,\mathbb{R})$;

б) матрицы с нулевым k-м столбцом образуют левый, но не правый идеал кольца $M(n,\mathbb{R})$.

12.16. На множестве $\{a,b,c,d\}$ определите операции сложения и умножения так, чтобы получилось кольцо (без единицы) и множеством его идеалов было:

а) $I_1=\{a\}$, $I_2=\{a,b\}$, $I_3=\{a,c\}$, $I_4=\{a,d\}$, $I_5=\{a,b,c,d\}$;

б) $I_1 = \{b\}$, $I_2 = \{b, c\}$, $I_3 = \{b, d\}$, $I_4 = \{a, b, c, d\}$;

в) $I_1 = \{d\}$, $I_2 = \{a, b, c, d\}$.

12.17. Любой идеал прямой суммы $R_1 \oplus R_2$ колец R_1 и R_2 имеет вид $I_1 \oplus I_2$, где I_1 — идеал кольца R_1, I_2 — идеал кольца R_2.

12.18. Если в коммутативном кольце R пересечение всех ненулевых идеалов отлично от нуля, то множество делителей нуля в нем образует идеал.

12.19. Приведите пример кольца с такими идеалами A и B, что $AB \neq A \cap B$.

12.20. Для идеалов I и J кольца установите равенства $r(I + J) = r(I \cup J) = r(I) \cap r(J)$.

12.21. Если X — произвольное подмножество кольца, то $r(\ell(r(X))) = r(X)$. В частности, правый идеал I является аннуляторным тогда и только тогда, когда $I = r(\ell(I))$.

12.22. Пусть M — множество тех идеалов A кольца R, для которых существует правый идеал B такой, что $A = r(B)$. Тогда:

а) $0, R \in M$;

б) если $A_1, A_2 \in M$, то $A_1 \cap A_2 \in M$;

в) для любых $A_1, A_2 \in M$ в частично упорядоченном относительно включения множестве M существует точная верхняя грань.

12.23. Приведите пример некоммутативного кольца, в котором есть коммутативный идеал, факторкольцо по которому коммутативно.

12.24. Покажите, построив соответствующий пример, что класс $a + I$ факторкольца может быть:

а) центральным элементом; б) идемпотентом;

в) нильпотентным элементом; г) делителем нуля;

д) обратимым элементом, даже если элемент $a \in R$ не обладает соответствующим свойством.

12.25. Докажите, что в коммутативном кольце R множество всех нильпотентных элементов образует идеал W, а факторкольцо R/W не содержит ненулевых нильпотентных элементов. Приведите пример некоммутативного кольца, в котором нильпотентные элементы не образуют ни левый, ни правый идеал.

12.26. 1) Норма $N(a + bi)$ комплексного числа $a + bi$ равна $a^2 + b^2$, а след $S(a + bi)$ равен $2a$.

2) Норма $N(A)$ матрицы $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ в алгебре матриц $M(2, P)$ над полем P равна квадрату определителя $(ad - bc)^2$.

3) Норма произведения равна произведению норм, а след суммы равен сумме следов.

Вычислите норму элемента $a + b\sqrt{d}$ в расширении $\mathbb{Q}(\sqrt{d})$.

12.27. Если I, J, L — такие идеалы кольца, что $J \subseteq I$, то верно равенство $I \cap (J + L) = J + (I \cap L)$ (модулярное тождество).

12.28. Приведите пример кольца и в нем идеалов I, J, L таких, что $I \cap (J + L) \neq (I \cap J) + (I \cap L)$.

12.29. Ненулевые элементы a, b коммутативной области порождают один и тот же идеал в точности тогда, когда существует обратимый элемент u со свойством $b = au$.

12.30. Идеал коммутативного кольца R, порожденный подмножеством $M \subseteq R$, состоит из всех конечных сумм вида:

а) $(M) = \{\sum r_i a_i \,|\, r_i \in R,\ a_i \in M\}$, если R имеет единицу;

б) $(M) = \{\sum r_i a_i + \sum n_j a_j \,|\, r_i \in R;\ a_i, a_j \in M;\ n_j \in \mathbb{Z}\}$, если R не имеет единицы.

12.31. 1) Левый аннулятор любого подмножества является в кольце левым идеалом.

2) Левый аннулятор левого идеала является двусторонним идеалом.

3) Левый аннулятор правого идеала кольца, порожденного идемпотентом, также порождается (как левый идеал) некоторым идемпотентом.

12.32. Если $I = I_1 \oplus I_2$ — прямая сумма идеалов, то произведение любого элемента из I_1 на любой элемент из I_2 равно нулю.

12.33. Пусть $R = I_1 \oplus I_2$ — разложение кольца R в прямую сумму ненулевых идеалов. Тогда если $1 = e_1 + e_2$, где $e_1 \in I_1$, $e_2 \in I_2$, то e_1, e_2 будут единицами, соответственно, в I_1, I_2, но не в R.

12.34. Пусть A, B — идеалы кольца R. Тогда отображение

$$R/(A \cap B) \to R/A \oplus R/B, \quad x + (A \cap B) \mapsto (x + A, x + B),$$

где $x \in R$, есть гомоморфизм колец. Найдите условие, при котором этот гомоморфизм будет изоморфизмом.

12.35. Конечная сумма левых идеалов, порожденных попарно ортогональными идемпотентами, также порождается идемпотентом.

12.36. Факторкольца $\mathbb{R}[x]/(x^2+1)$ и $\mathbb{R}[x]/(x^2+x+1)$ изоморфны полю $\mathbb{C}$.

12.37. Если $f\colon P \to R$ — гомоморфизм тела P (в частности, поля) в кольцо R, то f является мономорфизмом.

12.38. 1) Факторкольцо $\mathbb{Z}[i]/(2)$ содержит делители нуля.

2) Факторкольцо $\mathbb{Z}[i]/(3)$ является полем из 9 элементов.

12.39. Пусть R — коммутативное кольцо и N — некоторое множество его элементов, не являющихся делителями нуля.

1) Подполугруппа S мультипликативной полугруппы кольца R, порожденная N, не содержит ни нуля, ни делителей нуля.

2) Отношение $\sim$ на $R \times S$, при котором $(a,b) \sim (c,d)$ в точности тогда, когда $ad = bc$, является отношением эквивалентности; класс, содержащий (a,b), обозначается через $\dfrac{a}{b}$ и называется *дробью* элементов a и b.

3) Операции $\dfrac{a}{b}\cdot\dfrac{c}{d} = \dfrac{ac}{bd}$ и $\dfrac{a}{b}+\dfrac{c}{d} = \dfrac{ad+bc}{bd}$ превращают множество дробей в коммутативное кольцо Q, в котором обратимы все дроби вида $\dfrac{s}{t}$, где $s,t \in S$.

4) Отображение $R \ni a \mapsto \dfrac{a}{1}$ является вложением R в Q.

В частности, если R — область, а $S = R \setminus \{0\}$, то в Q обратимы все ненулевые элементы из R; Q в этом случае называется *кольцом* (*полем*) *частных* кольца R.

Говорят, что кольцо R удовлетворяет *правому условию Оре* (или, что R — *правое кольцо Оре*), если для любых $a,b \in R$, где b — неделитель нуля, существуют элементы $c,d \in R$, где c — неделитель нуля, со свойством $ac = bd$.

Говорят, что кольцо R обладает *правым кольцом частных* Q, если существует такое вложение $h\colon R \to Q$, что $h(x)$ обратим в Q для всех неделителей нуля $x \in R$ и что $Q = \{h(a)h(b)^{-1} \mid a \in R,\ b$ — неделитель нуля в $R\}$. С точностью до отождествления $R \subseteq Q$ и $Q = \{ab^{-1} \mid a \in R,\ b$ — неделитель нуля в $R\}$.

5) Кольцо R обладает правым кольцом частных в точности тогда, когда R — правое кольцо Оре.

12.40. Любое коммутативное кольцо, заключенное между коммутативной областью главных идеалов R и ее кольцом частных Q, само является областью главных идеалов.

12.41. Пусть $P[x,y]$ — кольцо многочленов от двух переменных x и y над полем P, I — множество всех многочленов без свободных членов. Докажите, что:

а) I является идеалом, но не главным;

б) $P[x,y]/I \cong P$.

12.42. Если P — поле и $f \in P[x]$ имеет степень n, то размерность P-алгебры $P[x]/(f)$ равна n.

12.43. При каком $a \in F_7$ факторкольцо $F_7[x]/(x^2+a)$ является полем?

12.44. Если $f(x)$ — неприводимый многочлен степени n из кольца $\mathbb{Z}_p[x]$, то факторкольцо $\mathbb{Z}_p[x]/(f(x))$ является полем из p^n элементов.

12.45. Лежат ли:

а) $x^5 - 3x^2 + x - 7$ и $x^4 + 5$;

б) $\left(x^2+1\right)x$ и $\left(x^2+1\right)(x+1)$;

в) $ax+b$ и $cx+d$ при $a \neq c$

в одном смежном классе кольца $\mathbb{R}[x]$ по идеалу (x^2+1)?

12.46. Делителями нуля в кольце $\mathbb{Q}[x]/(x^2-4)$ будут смежные классы с представителями $ax-2a$ и $ax+2a$ при $0 \neq a \in \mathbb{Q}$.

12.47. Есть ли в кольце $\mathbb{Q}[x]/(x^2-4)$:

а) идемпотенты, отличные от $\overline{0}$ и $\overline{1}$;

б) ненулевые нильпотентные элементы?

12.48. Идеал $I = (x) + (2)$ кольца $\mathbb{Z}[x]$ состоит из многочленов с четными свободными членами и $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$.

12.49. Установите изоморфизмы:

а) $\mathbb{Q}[x]/(x^2-1) \cong \mathbb{Q} \oplus \mathbb{Q}$; б) $\mathbb{Q}[x]/(x^2-3) \cong \mathbb{Q}(\sqrt{3})$.

12.50. Множество $\operatorname{End} R$ всех эндоморфизмов кольца R является полугруппой относительно композиции отображений. Она называется *полугруппой эндоморфизмов* кольца R.

12.51. Множество $\mathrm{Aut}\ R$ всех автоморфизмов кольца R образует группу относительно композиции отображений. Она называется *группой автоморфизмов* кольца R.

12.52. Пусть v — фиксированный обратимый элемент кольца R. Покажите, что отображение $x \mapsto v^{-1}xv$ $(x \in R)$ есть автоморфизм кольца R, называемый *внутренним*. Множество всех внутренних автоморфизмов является нормальной подгруппой в группе $\mathrm{Aut}\ R$.

12.53. Кольца $\mathbb{Z}_n$, $\mathbb{Z}$, $\mathbb{Q}_p$, $\widehat{\mathbb{Z}}_p$ не имеют неединичных автоморфизмов.

12.54. Все автоморфизмы кольца $M(n,\mathbb{R})$ являются внутренними.

12.55. Приведите пример кольца R, в котором:

а) есть автоморфизмы, не являющиеся внутренними;

б) группа автоморфизмов $\mathrm{Aut}\ R$ двухэлементна;

в) $\mathrm{Aut}\ R \cong S_n$;

г) $\mathrm{Aut}\ R$ изоморфна мультипликативной группе поля вещественных чисел.

12.56. Не существует ненулевых гомоморфизмов:

а) из $\mathbb{Z}_n$ в $\mathbb{Z}$; б) из $\mathbb{Q}$ в $\mathbb{Z}$;

в) из $\mathbb{R}$ в $\mathbb{Q}$; г) из $M(n,\mathbb{R})$ в $\mathbb{R}$ $(n > 1)$.

12.57. Построить вложение:

а) из $\mathbb{R}$ в $\mathbb{C}$; б) из $\mathbb{Q}_p$ в $\widehat{\mathbb{Z}}_p$;

в) из $\mathbb{R}$ в $M(n,\mathbb{R})$; г) из $M(2,\mathbb{R})$ в $M(2n,\mathbb{R})$;

д) из R в $R \oplus R$, где R — произвольное кольцо.

12.58. Покажите, что кольца R и S не изоморфны:

а) $R = \mathbb{Z}$, $S = \mathbb{Z} \oplus \mathbb{Z}$; б) $R = \mathbb{Z}$, $S = \mathbb{Z}[x]$;

в) $R = \mathbb{Z}$, $S = M(2,\mathbb{Z})$; г) $R = \mathbb{Z}_4$, $S = \mathbb{Z}_2 \oplus \mathbb{Z}_2$;

д) $R = M(2,\mathbb{R})$, $S = M(3,\mathbb{R})$.

12.59. Найдите все подкольца поля $\mathbb{Q}$, содержащие 1.

12.60. Кольцо $P(\{1,2,3\})$ изоморфно кольцу $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

12.61. 1) Приведите пример таких колец R, S, T, что $R \oplus S \cong R \oplus T$ и $S \ncong T$.

2) Приведите пример такого кольца R, что $R \cong R \oplus R$.

12.62. Пусть n — натуральное число с каноническим разложением $n = p_1^{m_1} \dots p_r^{m_r}$. Используя теорему 12.4, докажите, что:

а) $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{m_r}}$ (прямая сумма колец);

б) $U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{m_1}}) \times \dots \times U(\mathbb{Z}_{p_r^{m_r}})$ (прямое произведение групп).

12.63. Используя п. б) предыдущей задачи, докажите справедливость:

а) формулы Эйлера $\varphi(n) = n\left(1 - \dfrac{1}{p_1}\right) \dots \left(1 - \dfrac{1}{p_r}\right)$;

б) теоремы Эйлера $a^{\varphi(n)} \equiv 1 \pmod{n}$ для любого целого числа a, взаимно простого с n.

12.64. Из 12.62 следует, что для полного изучения групп $U(\mathbb{Z}_n)$ достаточно разобрать случай $n = p^m$. Покажите, что если p — нечетное простое число, то $U(\mathbb{Z}_{p^m})$ — циклическая группа. Легко видеть, что $U(\mathbb{Z}_{2^l})$ при $l = 1, 2$ является циклической группой порядка 1 и 2 соответственно. При $l \geqslant 3$ эта группа является прямым произведением циклической группы порядка 2 и циклической группы порядка 2^{l-2}.

12.65. Пусть R — кольцо, G, H — группы, и существует вложение групп $G \to H$. Постройте вложение групповых колец $RG \to RH$.

12.66. Покажите, что в ассоциативной алгебре A с 1 размерности n над полем P каждый элемент $a \in A$ является корнем некоторого унитарного многочлена степени $\leqslant n$ (такой многочлен наименьшей степени называется *минимальным многочленом* $\mu_a(x)$ элемента a). Элемент a обратим в точности тогда, когда $\mu_a(0) \neq 0$, это эквивалентно тому, что a не является делителем нуля. Если в A нет делителей нуля, то A — алгебра с делением. Если при этом поле P алгебраически замкнуто, то $A = P$.

12.67. Конечномерная алгебра с 1 и без делителей нуля над полем $\mathbb{C}$ изоморфна $\mathbb{C}$.

12.68. Перечислите с точностью до изоморфизма все коммутативные двумерные алгебры над $\mathbb{R}$ (над $\mathbb{C}$):

а) с единицей;

б) не обязательно с единицей.

12.69. *Алгеброй вещественных кватернионов* называется четырехмерная ассоциативная алгебра $\mathbb{H}$ над $\mathbb{R}$ с базисными элементами $1, i, j, k$ и с таблицей умножения

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

1) $\mathbb{H}$ — некоммутативная алгебра с 1 и с центром $Z(\mathbb{H}) = \mathbb{R}$.

2) $\mathbb{H}$ является алгеброй с делением, т.е. телом.

3) Отображение $u = a+bi+cj+dk \mapsto \overline{u} = a-bi-cj-dk$ является антиавтоморфизмом (переставляющим множители) алгебры $\mathbb{H}$.

12.70. Докажите, что нельзя построить ассоциативную алгебру с делением A над $\mathbb{R}$ размерности 3, содержащую $\mathbb{C}$ в качестве подалгебры.

Теорема Фробениуса утверждает, что над $\mathbb{R}$ существуют лишь три конечномерные ассоциативные алгебры с делением: $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$. Для произвольных (не обязательно ассоциативных) алгебр над $\mathbb{R}$ доказано, что существуют лишь алгебры с размерностью 1, 2, 4 и 8.

12.71. Всякая альтернативная конечномерная алгебра без делителей нуля над полем является алгеброй с делением.

12.72. Если $\alpha = a + (bi + cj + dk)$, то a называется *вещественной частью кватерниона* α и обозначается $a = \operatorname{Re}\alpha$, а $bi + cj + dk = \operatorname{Im}\alpha$ называется его *мнимой частью*. Через $N(\alpha) = a^2 + b^2 + c^2 + d^2$ обозначают норму кватерниона α. Покажите, что:

а) всякий кватернион α удовлетворяет квадратному уравнению

$$x^2 - (2\operatorname{Re}\alpha)x + N(\alpha) = 0$$

с вещественными коэффициентами;

б) если $g(x) = x^2 + 2tx + s$ — квадратный многочлен с отрицательным дискриминантом, то любой кватернион β, для которого $\operatorname{Re}\beta = -t$, $N(\beta) = s$, является корнем многочлена $g(x)$. Таких кватернионов, обращающих в нуль многочлен $g(x)$, континуум;

в) решите в $\mathbb{H}$ уравнение $x^2 + 1 = 0$.

12.73. 1) Является ли алгебра кватернионов $\mathbb{H}$ алгеброй над полем $\mathbb{C}$, если умножение на скаляр $\alpha \in \mathbb{C}$ понимать как левое умножение на $\alpha \in \mathbb{H}$?

2) Отображение

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

индуцирует изоморфизм алгебры $\mathbb{H}$ на подалгебру матриц вида

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

в алгебре матриц $M(2, \mathbb{C})$ над $\mathbb{R}$.

3) Отображение $z \mapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$ является вложением поля $\mathbb{C}$ в алгебру $\mathbb{H}$, реализованную как в 2) в виде подалгебры алгебры матриц $M(2, \mathbb{C})$ над $\mathbb{R}$.

12.74. Алгебра вещественных матриц вида

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

изоморфна алгебре кватернионов.

12.75. Алгебра Кэли. Это вещественная алгебра $\mathcal{C}a$, состоящая из элементов вида $\{\alpha + \beta e \mid \alpha, \beta \in \mathbb{H}\}$, с операциями

$$(\alpha + \beta e) + (\gamma + \delta e) = (\alpha + \gamma) + (\beta + \delta)\, e,$$
$$(\alpha + \beta e)(\gamma + \delta e) = \left(\alpha\gamma - \overline{\delta}\beta\right) + \left(\delta\alpha + \beta\overline{\gamma}\right) e.$$

Проверьте, что $\mathcal{C}a$ является восьмимерной вещественной алгеброй с базисом $\{1, i, j, k, e, ie, je, ke\}$ и с таблицей умножения

	1	i	j	k	e	ie	je	ke
1	1	i	j	k	e	ie	je	ke
i	i	-1	k	$-j$	ie	$-e$	$-ke$	je
j	j	$-k$	-1	i	je	ke	$-e$	$-ie$
k	k	j	$-i$	-1	ke	$-je$	ie	$-e$
e	e	$-ie$	$-je$	$-ke$	-1	i	j	k
ie	ie	e	$-ke$	je	$-i$	-1	$-k$	j
je	je	ke	e	$-ie$	$-j$	k	-1	$-i$
ke	ke	$-je$	ie	e	$-k$	$-j$	i	-1

Элементы вида $\alpha = \alpha + 0e$ составляют в алгебре Кэли подалгебру, изоморфную алгебре кватернионов. Алгебра Кэли не является ни коммутативной, ни ассоциативной.

Если $\xi = \alpha + \beta e \in \mathcal{C}a$, то элемент $\overline{\xi} = \overline{\alpha} - \beta e$ называется *сопряженным* к ξ. $N(\xi) = \xi\overline{\xi}$ — норма элемента ξ. Проверьте следующие свойства сопряжения:

$$\overline{\xi\zeta} = \overline{\zeta}\,\overline{\xi}, \quad \overline{\xi + \zeta} = \overline{\xi} + \overline{\zeta}, \quad \xi\overline{\xi} = \overline{\xi}\xi = \alpha\overline{\alpha} + \beta\overline{\beta} = N(\alpha) + N(\beta),$$
$$\xi\overline{\xi} \geqslant 0 \quad \text{и} \quad \xi\overline{\xi} = 0 \iff \xi = 0.$$

Элемент $1 = 1 + 0e$ является единицей алгебры $\mathcal{C}a$. Проверьте, что алгебра Кэли является (неассоциативным) телом. Докажите, что алгебра Кэли альтернативна.

Доказано, что алгебра Кэли является единственной конечномерной вещественной альтернативной, но не ассоциативной алгеброй с делением. Объединение этой теоремы с теоремой Фробениуса называется *обобщенной теоремой Фробениуса*.

Пусть A — алгебра с 1 над $\mathbb{R}$. Пусть на A задана операция сопряжения $a \mapsto \overline{a}$, обладающая свойствами $\overline{\overline{a}} = a$, $\overline{ab} = \overline{b}\,\overline{a}$. Если снабдить пространство $A \oplus A = \{(a, b) \,|\, a, b \in A\}$ билинейной операцией умножения

$$(a, b)(u, v) = (au - \overline{v}b, b\overline{u} + va),$$

то получится алгебра, называемая *удвоением* алгебры A.

12.76. $\mathbb{C}$ — удвоение алгебры $\mathbb{R}$, $\mathbb{H}$ — удвоение алгебры $\mathbb{C}$, алгебра Кэли $\mathcal{C}a$ — удвоение алгебры $\mathbb{H}$.

12.77. Пусть K — коммутативная область. Покажите, что число корней многочлена $f(x) \in K[x]$, рассматриваемых вместе с их кратностями, не превышает степени $f(x)$. Пример многочлена $x^3 \in \mathbb{Z}_8[x]$, имеющего 4 корня в $\mathbb{Z}_8$, показывает, что условие «K — область» существенно. Покажите, что условие коммутативности K также существенно.

Кольцо *комплексно-косых* многочленов $\mathbb{C}[x, ^-]$ состоит из многочленов от x с комплексными коэффициентами, для которых выполняется равенство $xa = \overline{a}x$, где $\overline{a}$ — комплексное число, сопряженное к a.

12.78. 1) Центром кольца $\mathbb{C}[x, ^-]$ является кольцо $\mathbb{R}[x^2]$, т.е. кольцо вещественных многочленов от x^2.

2) Кольцо вычетов кольца $\mathbb{C}[x, ^-]$ по модулю $x^2 + 1$, т.е. факторкольцо $\mathbb{C}[x, ^-]/(x^2 + 1)$, изоморфно телу $\mathbb{H}$.

13 Специальные идеалы

На множестве всех левых идеалов кольца R (с единицей или без единицы) можно ввести частичный порядок $\leqslant$, если для левых идеалов A и B считать, что $A \leqslant B$ в точности тогда, когда $A \subseteq B$. Говорят, что $\leqslant$ — *порядок относительно включения* (см. § 1). Получаем частично упорядоченное множество левых идеалов кольца R. Аналогично (т.е. относительно включения) определяется частичный порядок на множестве всех правых идеалов и всех идеалов кольца R.

Идеал I называется *нильпотентным*, если существует число $n \in \mathbb{N}$ такое, что для всех наборов элементов $a_1, \ldots, a_n \in I$ выполняется $a_1 \cdot \ldots \cdot a_n = 0$. Наименьшее такое n называют *индексом нильпотентности* идеала I.

Идеал кольца R называется *минимальным* (соответственно, *максимальным*), если он является минимальным (соответственно, максимальным) элементом в частично упорядоченном множестве ненулевых идеалов (соответственно, собственных идеалов) кольца R.

Идеал I кольца R называется *ниль-идеалом*, если каждый элемент a из I нильпотентен, т.е. $a^n = 0$ для некоторого $n \in \mathbb{N}$ (n зависит от a).

Рассматривают также левые или правые специальные идеалы. Так, заменив в приведенных выше определениях понятие «идеал» на понятие «левый идеал» (соответственно, «правый идеал»), получим определение минимального, максимального, нильпотентного левого (соответственно, правого) идеала, а также левого (соответственно, правого) ниль-идеала.

Говорят, что R — кольцо *с условием обрыва убывающих цепей* левых (соответственно, правых) идеалов, если любая последовательность $I_1 \supseteq I_2 \supseteq \ldots$ левых (соответственно, правых) идеалов, где $I_m \neq I_n$ при $m \neq n$, конечна. Говорят также, что R — кольцо *с условием обрыва возрастающих цепей* левых (соответственно, правых) идеалов,

если любая последовательность $I_1 \subseteq I_2 \subseteq \dots$ левых (соответственно, правых) идеалов, где $I_m \neq I_n$ при $m \neq n$, конечна.

Кольца с условием обрыва убывающих цепей левых (правых) идеалов называют еще *артиновыми слева* (*справа*); кольца с условием обрыва возрастающих цепей левых (правых) идеалов — *нетеровыми слева* (*справа*).

Идеал I кольца R называется *примитивным справа*, если I — наибольший идеал, содержащийся в некотором максимальном правом идеале.

Кольцо называется *примитивным* (*справа*), если примитивен его нулевой идеал. Из правой примитивности не следует левая, но, тем не менее, иногда прилагательное «правый» опускается.

Кольцо называется *полупримитивным* (справа), если пересечение его примитивных справа идеалов равно 0. Полупримитивные слева кольца определяются симметрично. Правая полупримитивность кольца эквивалентна его левой полупримитивности (15.78).

Идеал $I \neq R$ кольца R называется *первичным*, если для любых идеалов A и B кольца R из включения $AB \subseteq I$ следует, что либо $A \subseteq I$, либо $B \subseteq I$ (в коммутативном кольце такой идеал называется *простым*).

Пересечение всех первичных идеалов кольца R называется его *первичным радикалом* и обозначается $\operatorname{rad} R$.

Элемент $a \in R$ называется *строго нильпотентным*, если все члены последовательности $a_0, a_1, \dots$ такой, что $a_0 = a$, $a_{n+1} \in a_n R a_n$, начиная с некоторого номера равны нулю. Строго нильпотентный элемент является нильпотентным. Если кольцо коммутативно, то каждый его нильпотентный элемент строго нильпотентен.

Первичный радикал совпадает с множеством всех строго нильпотентных элементов кольца.

Пересечение всех максимальных правых, эквивалентно — левых (см. 13.58), идеалов кольца R называется *радикалом Джекобсона* $J(R)$ кольца R.

Кольцо R называется *полупервичным*, если 0 — его единственный нильпотентный идеал. В этом случае говорят, что R *не имеет нильпотентных идеалов*. Кольцо R называется *первичным*, если произведение двух ненулевых его идеалов является ненулевым идеалом. Коммутативное кольцо первично тогда и только тогда, когда оно является областью целостности. Первичное кольцо полупервично.

Кольцо R называется *локальным*, если в R есть единственный максимальный левый идеал, или, равносильно, в R есть единственный максимальный правый идеал (см. 13.60).

В упражнениях, касающихся простых идеалов, кольца предполагаются коммутативными. Если M — множество, то под кольцом $R = P(M)$ понимается кольцо $(P(M), \triangle, \cap)$.

Задачи

13.1. Образуют ли идеал необратимые элементы колец:

а) $\mathbb{Z}$; б) $\mathbb{C}[x]$; в) $\mathbb{R}[x]$; г) $\mathbb{Z}_n$?

Найдите максимальные идеалы в этих кольцах.

13.2. Пусть R — кольцо непрерывных функций на отрезке $[0, 1]$, $I_c = \{f(x) \in R \mid f(c) = 0\}$ $(0 \leqslant c \leqslant 1)$. Докажите, что:

а) I_c — максимальный идеал в R;

б) всякий максимальный идеал кольца R совпадает с I_c для некоторого c.

13.3. В коммутативной области главных идеалов простыми идеалами являются те, которые порождаются простыми (см. § 14) элементами кольца, причем каждый ненулевой простой идеал максимален.

13.4. Каждый собственный (правый) идеал кольца содержится в максимальном собственном (правом) идеале.

13.5. 1) Идеал (p) кольца $\mathbb{Z}_{p^n}$ является нильпотентным индекса нильпотентности n.

2) Если A — идеал кольца R, то A/A^n — нильпотентный идеал кольца R/A^n индекса нильпотентности $\leqslant n$.

3) Если A и B — нильпотентные идеалы индекса нильпотентности n и m соответственно, то $A + B$ — нильпотентный идеал индекса нильпотентности $\leqslant n + m$.

13.6. Если идеалы A_i $(i \in I)$ нильпотентны, то:

а) идеал $\sum\limits_{i \in I} A_i$ является ниль-идеалом;

б) если множество I конечно, то идеал $\sum\limits_{i \in I} A_i$ нильпотентен.

13.7. Если I — минимальный правый идеал кольца R, то либо $I = eR$ для некоторого идемпотента $e \in R$, либо $I^2 = 0$.

13.8. Пусть R — коммутативное кольцо. Докажите, что:

а) минимальный идеал I в R всегда главный и $I^2 = 0$ или $I^2 = I$;

б) если R — кольцо без ненулевых нильпотентных элементов, то всякий его минимальный идеал порождается идемпотентом;

в) если I — минимальный идеал, порожденный идемпотентом, то кольцо I является полем.

13.9. Собственный идеал I коммутативного кольца R максимален в точности тогда, когда для любого $r \in R \setminus I$ найдется $x \in R$ со свойством $1 - rx \in I$.

13.10. В коммутативном кольце R собственный идеал P прост тогда и только тогда, когда для любых элементов $a, b \in R$ таких, что $ab \in P$, справедливо хотя бы одно из включений $a \in P$ или $b \in P$.

13.11. Факторкольцо R/I коммутативного кольца является полем (соответственно, областью), если и только если I — максимальный (соответственно, простой) идеал в R.

Максимальный идеал коммутативного кольца является простым.

13.12. 1) Нулевой идеал максимален в коммутативном кольце тогда и только тогда, когда это кольцо есть поле.

2) Центр простого кольца является полем.

13.13. Приведите пример коммутативного кольца без единицы, в котором нулевой идеал максимален, однако кольцо полем не является.

13.14. Идеал P коммутативного кольца R простой тогда и только тогда, когда P — ядро гомоморфизма из R в некоторое поле.

Пусть R — коммутативное кольцо с 1 и $T \subseteq R$ — такое подмножество, что $xy \in T$ при $x, y \in T$. Подмножество с таким свойством называется *мультипликативно замкнутым.*

13.15. 1) Если $1 \in T$, $0 \notin T$ и T — мультипликативно замкнутое подмножество коммутативного кольца R, то любой идеал P, максимальный среди идеалов, не пересекающихся с T, прост.

2) Идеал P прост тогда и только тогда, когда множество $R \setminus P$ мультипликативно замкнуто.

3) Элемент $x \in R$ нильпотентен тогда и только тогда, когда он лежит во всяком простом идеале кольца R, т.е. множество нильпотентных элементов кольца R совпадает с пересечением всех простых идеалов этого кольца.

13.16. Если I — максимальный идеал в $\mathbb{Z}[x]$, то $\mathbb{Z}[x]/I$ — конечное поле.

Для элемента a кольца R (с единицей или без единицы) введем следующие обозначения: $Ra = \{ra \,|\, r \in R\}$, $aR = \{ar \,|\, r \in R\}$ и $RaR = \{\sum\limits_{i=1}^{n} r_i a s_i \,|\, r_i, s_i \in R, n \in \mathbb{N}\}$.

13.17. Ra, aR и RaR — соответственно, левый, правый и двусторонний идеалы кольца R.

13.18. Пусть R — кольцо с единицей и $a \in R$. Тогда:

а) левый идеал Ra является главным левым идеалом, порожденным элементом a;

б) правый идеал aR является главным правым идеалом, порожденным элементом a;

в) идеал RaR является главным идеалом, порожденным элементом a.

13.19. Приведите такие примеры кольца R без единицы и элемента a, чтобы:

а) левый идеал Ra не совпадал с главным левым идеалом, порожденным элементом a;

б) правый идеал aR не совпадал с главным правым идеалом, порожденным элементом a.

13.20. Приведите пример кольца R без единицы такого, чтобы R не являлся главным идеалом.

13.21. Главный идеал коммутативного кольца, порожденный необратимым элементом, является собственным. Приведите такой пример кольца R без единицы и необратимого элемента $a \in R$, что главный идеал (a) совпадает с R.

13.22. Покажите, что идеал I кольца R является главным:

а) $I = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, $R = \mathbb{Z}_{12}$;

б) $I = \left\{ \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$, $a \in \mathbb{Z}$; $R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \right\}$, $a, b, c \in \mathbb{R}$;

в) $I = \{\varnothing, \{1\}, \{3\}, \{1, 3\}\}$, $R = P(\{1, 2, 3\})$.

13.23. Какие элементы входят в главный правый идеал aR, если:

а) $a = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $R = M(3, \mathbb{R})$; б) $a = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $R = M(3, \mathbb{R})$;

в) $a = \{0, 2, 4\}$, $R = P(\{0, 1, 2, 3, 4, 5\})$.

13.24. Сколько элементов содержит главный идеал $a\mathbb{Z}_{24}$ кольца $\mathbb{Z}_{24}$, если:

а) $a = \overline{5}$; б) $a = \overline{6}$?

13.25. Проверьте равенство главных идеалов, порожденных элементами a и b кольца R:

а) $a = \overline{4}$, $b = \overline{1}$, $R = \mathbb{Z}_{15}$;

б) $a = 2x + 1$, $b = 4x + 2$, $R = \mathbb{R}[x]$;

в) $a = 6/7$, $b = 2$, $R = \mathbb{Q}_2$.

13.26. Проверьте, что каждый конечно порожденный идеал кольца 2^M является главным.

В следующих упражнениях 13.27 — 13.32 покажите, что идеал I кольца R не является главным.

13.27. I состоит из конечных подмножеств бесконечного множества M, $R = 2^M$.

13.28. I состоит из функций, обращающихся в нуль вне некоторого (для каждой функции своего) отрезка, $R = \mathbb{R}^{\mathbb{R}}$.

13.29. I состоит из последовательностей, в которых лишь конечное число ненулевых элементов, $R = \mathbb{R}^{\mathbb{N}}$.

13.30. $R = \mathbb{Z}[\sqrt{5}\,i] = \{m + n\sqrt{5}\,i \,|\, m, n \in \mathbb{Z}\}$, $I = (a, b)$, $a = 3$, $b = 1 + 2\sqrt{5}\,i$.

13.31. $R = T\,[[x]]$, $I = J + (x)$, где J — нетривиальный идеал кольца T.

13.32. $R = \mathbb{Z}[x]$, $I = (2) + (x)$.

13.33. Пусть R — кольцо A и такое его подкольцо, что $[x, a] = xa - ax \in A$ для любых $x \in R$ и $a \in A$. Тогда если $a, b \in A$, то $R(ab - ba)R \subseteq A$.

13.34. Если D — тело, то для каждого $f \in D^X$ существует идемпотент $e \in D^X$ такой, что $(f) = (e)$.

13.35. Если e — идемпотент кольца R, то для главных правых идеалов $I_1 = eR$, $I_2 = (1 - e)\,R$ справедливы соотношения: $I_1 \cap I_2 = 0$, $I_1 + I_2 = R$.

13.36. Пусть e — центральный идемпотент кольца R. Докажите, что:

а) $1 - e$ — также центральный идемпотент кольца R, ортогональный к e;

б) eR — идеал кольца R и в то же время eR — кольцо с единицей e;

в) R является прямой суммой идеалов: $R = eR \oplus (1 - e)\,R$.

13.37. Следующие утверждения эквивалентны:

а) кольцо R изоморфно прямой сумме колец R_i $(i = 1, \ldots, n)$;

б) существуют ортогональные идемпотенты $e_i \in Z\,(R)$ со свойствами $e_1 + \ldots + e_n = 1$ и $R = e_1R \oplus \ldots \oplus e_nR$, причем кольца e_iR и R_i изоморфны $(i = 1, \ldots, n)$;

в) кольцо R является прямой суммой идеалов $R = I_1 \oplus \ldots \oplus I_n$, причем кольца I_i и R_i изоморфны.

13.38. Найдите все идеалы кольца:

а) $\mathbb{Z}$; б) $P[x]$, где P — поле.

13.39. Кольцо многочленов $K[x]$ является коммутативной областью главных идеалов в точности тогда, когда K — поле.

13.40. Покажите, что R — коммутативное кольцо главных идеалов:

а) $R = 2^M$, если M — конечное множество;

б) $R = P\,[[x]]$, где P — некоторое поле;

в) R — кольцо целых p-адических чисел $\widehat{\mathbb{Z}}_p$.

13.41. Покажите, что кольцо R не является кольцом главных идеалов:

а) $R = \mathbb{Z}[x]$; б) $R = \mathbb{R}^{\mathbb{R}}$;

в) $R = 2^M$, если M — бесконечное множество (см. 13.27).

13.42. Покажите, что в кольце R идеал I максимален:

а) $R = \mathbb{Z}$, $I = 3\mathbb{Z}$;

б) $R = \mathbb{Z}_{14}$, $I = \{0, \overline{7}\}$;

в) $R = 2^{\mathbb{R}}$, $I = \{A \subseteq \mathbb{R} \,|\, 0 \notin A\}$;

г) $R = \mathbb{Q}^{(2)}$, $I = (12)$;

д) $R = M(2, \mathbb{Z})$, $I = M(2, 2\mathbb{Z})$;

е) $R = P\,[x]$ (P — некоторое поле), $I = (x)$.

13.43. Идеал (4) не максимален в кольце $\mathbb{Q}_2$.

13.44. Найдите все максимальные идеалы кольца $\mathbb{Z}_{36}$.

13.45. Матрицы вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ (соответственно, $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$) образуют максимальный правый (соответственно, левый) идеал кольца $M(2, \mathbb{R})$.

13.46. Кольцо матриц $M(2,P)$ над бесконечным полем P содержит бесконечное множество минимальных правых идеалов.

13.47. Идеал кольца 2^M, состоящий из конечных подмножеств бесконечного множества M, не является максимальным в 2^M.

13.48. Какие идеалы максимальны в $\mathbb{Z} \oplus \mathbb{Z}$?

13.49. Максимальный идеал кольца 2^M, содержащий все конечные подмножества бесконечного множества M, не является главным (ср. с 13.27).

13.50. Идеал I кольца $P[x]$ над полем P максимален тогда и только тогда, когда он имеет вид $I = (f(x))$, где:

а) если $P = \mathbb{C}$, то $f(x)$ — многочлен первой степени;

б) если $P = \mathbb{R}$, то $f(x)$ — многочлен первой степени или многочлен второй степени, не имеющий вещественных корней.

13.51. Для каждого максимального (соответственно, простого) идеала I кольца R идеал $\{a_0 + a_1x + \ldots + a_nx^n \mid a_0 \in I\}$ будет максимальным (соответственно, простым) идеалом в $R[x]$.

В упражнениях 13.52 — 13.57 R обозначает кольцо, a — элемент кольца R.

13.52. При каком условии для максимального правого идеала M кольца R выполняется соотношение $1 \notin aR + M$?

13.53. Используя упражнение 13.52, покажите, что элемент $1 - ax$ будет обратим справа для любого $x \in R$ тогда и только тогда, когда a лежит в пересечении всех максимальных правых идеалов.

13.54. Пусть $r, s \in R$ таковы, что $(1 - ar)\, s = 1$. Найдите $t \in R$, для которого $(1 - ra)\, t = 1$.

13.55. Используя упражнение 13.54, покажите, что если элемент $1 - ar$ обратим справа для любого $r \in R$, то и элемент $1 - ra$ обратим справа для любого $r \in R$.

13.56. Используя упражнения 13.53 и 13.55, покажите, что пересечение $J(R)$ всех максимальных правых идеалов кольца R есть двусторонний идеал.

13.57. Используя упражнение 13.53 и обратимость $1 - a$ для каждого нильпотентного элемента a, покажите, что каждый нильпотентный идеал содержится в пересечении всех максимальных правых идеалов.

13.58. Используя упражнения 13.52 — 13.56, покажите, что пересечение всех максимальных правых идеалов $J(R)$ кольца R совпадает с пересечением всех максимальных левых идеалов.

13.59. Используя упражнения 13.52 — 13.56, покажите, что многочлен с коэффициентами из коммутативного кольца лежит в пересечении всех максимальных идеалов тогда и только тогда, когда он нильпотентен.

13.60. Следующие утверждения о кольце R эквивалентны:

а) R — локальное кольцо;

б) для любого элемента $r \in R$ либо r, либо $1 - r$ — обратимый слева элемент;

в) для любого элемента $r \in R$ либо r, либо $1 - r$ — обратимый элемент;

г) множество необратимых элементов I кольца R замкнуто относительно сложения;

д) все необратимые элементы кольца R образуют идеал;

е) все необратимые элементы кольца R лежат в некотором собственном идеале;

ж) все необратимые элементы кольца R образуют единственный максимальный левый идеал.

Утверждение остается справедливым, если б) и ж) заменить на их правые аналоги.

13.61. Покажите, что кольцо R локально, и укажите максимальные идеалы:

а) $R = P\,[[x]]$, где P — некоторое поле;

б) $R = \mathbb{Z}_{p^n}$, где p — простое число, $n > 1$;

в) $R = \mathbb{Q}_p$;

г) R — кольцо целых p-адических чисел.

13.62. Для любого коммутативного кольца R существует локальное кольцо L и вложение R в L.

13.63. Факторкольцо локального кольца локально.

13.64. Покажите, что кольцо R не локально:

а) $R = \mathbb{Z}$; б) $R = \mathbb{Z}_6$;

в) $R = P\,[x]$ для любого поля P;

г) $R = \mathbb{Z}\,[[x]]$.

13.65. Покажите, что в кольце R идеал I является простым:

а) $R = \mathbb{Z}$, $I = (p)$ (p — простое число);

б) $R=\mathbb{Z}_n$, $I=(p)$, где $n>1$ и p делит n;

в) $R=\mathbb{R}[x]$, $I=(x)$;

г) $R=\mathbb{R}^{\mathbb{R}}$, $I=(x+1)$;

д) $R=\mathbb{R}[x]$, $I=\left(x^2+1\right)$;

е) $R=2^M$, где $M=\{1,2,3,4\}$, $I=\{A\subseteq M\mid 3\notin A\}$;

ж) $R=\mathbb{R}\oplus\mathbb{R}$, $I=\{(a,0)\mid a\in\mathbb{R}\}$;

з) $R=\mathbb{Z}[x]$, $I=(2)+(x)$.

13.66. Покажите, что идеал I не является простым в кольце R:

а) $R=\mathbb{C}[x]$, $I=\left(x^2+1\right)$;

б) $R=\mathbb{R}[x]$, $I=\left(x^2-1\right)$;

в) $R=2^M$, где $M=\{0,1,2,3,4\}$, $I=\{A\subseteq M\mid 1,3\in A\}$;

г) $R=2^M$, где M — бесконечное множество, I — идеал, состоящий из конечных подмножеств (см. 13.47).

13.67. Доказано, что если каждый элемент кольца удовлетворяет уравнению $x^n=x$ ($n\geqslant 2$, n для каждого x свое), то кольцо является коммутативным. Используя этот факт, покажите, что любой простой идеал P в этом кольце максимален.

13.68. В булевом кольце каждый простой идеал максимален.

13.69. Коммутативное кольцо содержит единственный простой идеал тогда и только тогда, когда каждый необратимый элемент нильпотентен.

13.70. В коммутативном кольце множество всех делителей нуля содержит простой идеал.

13.71. Если идеал содержится в конечном объединении простых идеалов, то он содержится в одном из них.

13.72. Частично упорядоченное множество простых идеалов кольца содержит минимальные элементы.

13.73. Идеал $(4)+(x)$ кольца $\mathbb{Z}[x]$ не прост и не является произведением простых идеалов.

В упражнениях 13.74 — 13.76 R обозначает коммутативное кольцо; $\operatorname{Spec}(R)$ — множество простых идеалов кольца R (*спектр* R); если A — подмножество в R, то $\Gamma(A)=\{P\in\operatorname{Spec}(R)\mid A\not\subseteq P\}$.

13.74. $\Gamma(R)=\operatorname{Spec}(R)$, $\Gamma(0)=\varnothing$. А для $A\subseteq R$ можно записать $\Gamma(A)=\bigcup\limits_{a\in A}\Gamma(a)$.

13.75. Если A_i ($i\in I$) — некоторое семейство идеалов кольца R, то $\bigcup\limits_{i\in I}\Gamma(A_i)=\Gamma\left(\sum\limits_{i\in I}A_i\right)$.

13.76. Если $a,b\in R$ и A, B — идеалы кольца R, то $\Gamma(a)\cap\Gamma(b)=\Gamma(ab)$, $\Gamma(A)\cap\Gamma(B)=\Gamma(AB)$.

13.77. Кольцо $\mathbb{Z}$ нетерово, но не артиново.

13.78. Пусть $f\colon R\to S$ — сюръективный кольцевой гомоморфизм. Тогда если R — артиново (нетерово) справа кольцо, то кольцо S также артиново (нетерово) справа.

13.79. Подкольцо артинова (нетерова) кольца не обязательно артиново (нетерово).

13.80. 1) Кольцо главных правых идеалов нетерово справа.

2) Нетерова справа область целостности является правым кольцом Ope.

13.81. Кольцо R нетерово и артиново справа в точности тогда, когда в R найдется конечная цепочка правых идеалов $0=I_0\subset I_1\subset\ldots\subset I_n=R$ таких, что каждый идеал I_j максимален в I_{j+1}, $j=0,1,\ldots,n-1$.

13.82. Кольцо всех матриц вида $\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}$, где $a\in\mathbb{Z}$, $b,c\in\mathbb{Q}$, нетерово справа, но не слева. (В связи с 17.14 заметим, что кольца $\begin{pmatrix} \mathbb{Z} & \mathbb{Q}\\ 0 & \mathbb{Q}\end{pmatrix}$ и $\begin{pmatrix} \mathbb{Q} & \mathbb{Q}\\ 0 & \mathbb{Z}\end{pmatrix}$ антиизоморфны.)

13.83. Пусть R и K — поля, причем R — бесконечное расширение K (например, $\mathbb{R}$ и $\mathbb{Q}$), а S — кольцо всех матриц вида $\begin{pmatrix} k & r_1\\ 0 & r_2\end{pmatrix}$, где $k\in K$, $r_1,r_2\in R$. Покажите, что S не является ни нетеровым, ни артиновым слева, но S — артиново и нетерово справа кольцо.

13.84. В коммутативном нетеровом кольце каждый ниль-идеал нильпотентен (см. 16.29).

13.85. Пусть R — артиново слева кольцо. Предположим, что для каждого правого идеала I существует левый идеал J такой, что $I=r(J)$. Тогда R — нетерово справа кольцо.

13.86. Если в кольце R для каждого левого идеала I существует элемент $x\in R$ такой, что $I=\ell(xR)$, и для каждого правого идеала J существует левый идеал L такой, что $J=r(L)$, то R артиново слева.

13.87. Пусть в кольце R для каждого левого идеала I существует конечное множество X и для каждого правого идеала J существует конечное множество Y со свойством $I=\ell(X)$, $J=r(Y)$. Тогда R артиново слева и справа и

нетерово слева и справа.

13.88. В коммутативном артиновом кольце каждый простой идеал максимален (см. 16.29 и 16.33).

13.89. Коммутативная артинова область является полем.

13.90. Коммутативное артиново кольцо имеет лишь конечное число простых идеалов.

14 Разложение на простые множители

Пусть K — коммутативная область. Говорят, что элемент $b \in K$ *делится* на $a \in K$, если существует такой элемент $c \in K$, что $b = ac$, в этом случае пишут $a \mid b$. Если $a \mid b$ и $b \mid a$, то a и b называются *ассоциированными* элементами. Кольцо K распадается на классы ассоциированных элементов.

Элемент $p \in K$ называется *простым* (или *неприводимым*), если p необратим и его нельзя представить в виде $p = ab$, где a, b — необратимые элементы. В поле каждый ненулевой элемент обратим, и в нем нет простых элементов.

Говорят, что коммутативная область K — *кольцо с разложением на простые множители*, если любой элемент $a \neq 0$ из K можно представить в виде $(*)$: $a = up_1 \dots p_r$, где u — обратимый элемент, а $p_1, \dots, p_r$ — простые элементы (не обязательно попарно различные). Если из существования другого такого разложения $a = vq_1 \dots q_s$ следует, что $r = s$ и при надлежащей перенумерации элементов p_i и q_i будет $q_1 = u_1 p_1, \dots, q_r = u_r p_r$, где $u_1, \dots, u_r$ — обратимые элементы, то кольцо K называется *кольцом с однозначным разложением на простые множители* или *факториальным*. Приняв в $(*)$ $r = 0$, допускают, что обратимые элементы в K также имеют разложение на простые множители. Иногда в литературе под простым элементом кольца понимается такой элемент p, что из $p \mid ab$ вытекает делимость на p хотя бы одного из множителей a, b. В факториальных кольцах понятия неприводимого и простого элементов совпадают (см. 14.2), поэтому в таких кольцах вместо термина «неприводимый» часто используется «простой». Однако для многочленов, как правило, принято использовать только термин «неприводимый».

Теорема 14.1. *Если K — коммутативная область с разложением на простые множители, то таковым является и кольцо многочленов $K[x]$. Если к тому же K факториально, то факториально и $K[x]$.*

Пусть K — коммутативная область. Под *наибольшим общим делителем* элементов $a, b \in K$ понимается элемент $d \in K$, обозначаемый $d = (a, b)$ и определяемый с точностью до ассоциированности, со свойствами: 1) $d \mid a, b$; 2) условие $c \mid a, b$ влечет $c \mid d$. Под *наименьшим общим кратным* $[a,\ b]$ элементов a, b понимается элемент m, также определяемый с точностью до ассоциированности, со свойствами: 1) $a, b \mid m$; 2) условие $a, b \mid c$ влечет $m \mid c$.

Пусть, далее, на K задана такая функция $\delta\colon K \backslash \{0\} \to \mathbb{N} \cup \{0\}$, что: 1) $\delta(ab) \geqslant \delta(a)$ для всех $0 \neq a, b \in K$; 2) для всех $a, b \in K$, $b \neq 0$, найдутся $q, r \in K$ со свойством $a = bq + r$, где $\delta(r) < \delta(b)$ или $r = 0$. Тогда K называется *евклидовым кольцом*, а функция δ — *евклидовой нормой*. В евклидовом кольце K выполнен *алгоритм Евклида*, позволяющий находить наибольший общий делитель элементов этого кольца. Кроме того, каждое евклидово кольцо является областью главных идеалов, а все коммутативные области главных идеалов факториальны.

Пусть K — факториальное кольцо. *Содержанием многочлена* $f(x) \in K[x]$ называется наибольший общий делитель $d(f)$ всех его коэффициентов. Если $d(f)$ — обратимый элемент в K, то говорят, что $f(x)$ — многочлен с содержанием 1 (иногда в этом случае $f(x)$ называют еще *примитивным* многочленом; отметим, что в § 30 рассматривается другое понятие примитивного многочлена).

Лемма 14.2 (Гаусс). *Пусть K — факториальное кольцо и $f, g \in K[x]$. Тогда $d(fg) = d(f)d(g)$. В частности, произведение двух многочленов с содержанием* 1 *снова будет многочленом с содержанием* 1 (равенство понимается с точностью до ассоциированности).

Задачи

Все кольца в упражнениях данного параграфа предполагаются коммутативными.

14.1. Приведите пример кольца с ненулевым умножением, не являющегося полем и не имеющего простых элементов.

14.2. Если K — кольцо с разложением на простые множители, то однозначность разложения, т.е. факториальность кольца K, имеет место тогда и только тогда, когда любой простой элемент $p \in K$, делящий произведение $a \cdot b \in K$, делит по крайней мере один из множителей a, b.

14.3. Пусть K — область. Главные идеалы (a) и (b) совпадают в точности тогда, когда элементы a и b ассоциированы.

14.4. Если K — область и идеал I, порождаемый элементами $a_1, \dots, a_n$, является главным, $I = (d)$, то d — НОД$\{a_1, \dots, a_n\}$, причем d представим в виде линейной комбинации этих элементов.

14.5. В факториальном кольце для любых $a, b \in K$ существуют (a, b) и $[a, b]$, причем $(a + b,\ [a, b]) = (a, b)$.

14.6. Пусть для элементов a, b области K существуют (a, b) и $[a, b] = m$. Покажите, что:

а) $m = 0$, если и только если $a = 0$ или $b = 0$;

б) $m \mid ab$, причем если $ab = dm$ для $a, b \neq 0$, то $d = (a, b)$.

14.7. 1) Покажите, что если $a, b \in K$ имеют $[a, b]$, то они имеют и (a, b). Рассмотрите подкольцо кольца $\mathbb{Z}[x]$, состоящее из многочленов с четным коэффициентом при x, и убедитесь, что обратное к предыдущему утверждению неверно.

2) Любые два элемента кольца K обладают НОК тогда и только тогда, когда любые два его элемента обладают НОД.

14.8. 1) Произведение двух главных идеалов области является главным идеалом.

2) Всякая возрастающая цепочка $I_1 \subseteq I_2 \subseteq \ldots$ идеалов кольца главных идеалов обрывается.

3) $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$, $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$, $n\mathbb{Z} \cdot m\mathbb{Z} = (nm)\mathbb{Z}$, $(n\mathbb{Z} + m\mathbb{Z})(n\mathbb{Z} \cap m\mathbb{Z}) = (nm)\mathbb{Z}$.

14.9. Если R — область главных идеалов, то $aR \cap bR = [a, b]\, R$ для $a, b \in R$.

14.10. Пусть $\pi = \{p_1, \ldots, p_n\}$ — произвольный конечный набор простых чисел. Покажите, что:

а) $\mathbb{Q}^{(\pi)}$ образует факториальное кольцо, множество классов простых ассоциированных элементов которого бесконечно;

б) $\mathbb{Q}_\pi$ образует факториальное кольцо, содержащее ровно n классов простых ассоциированных элементов.

14.11. Пусть K — евклидово кольцо с нормой δ. Тогда:

а) если a и b — ассоциированные элементы, то $\delta(a) = \delta(b)$;

б) если a делит b и $\delta(a) = \delta(b)$, то a и b — ассоциированные элементы;

в) $\delta(a) = \delta(1)$ в точности тогда, когда $a \in U(K)$;

г) если $a \in U(K)$, то $\delta(a) \leqslant \delta(b)$ и $\delta(ab) = \delta(b)$ для любого $0 \neq b \in K$;

д) если $0 \neq b \in K \backslash U(K)$, то $\delta(b) > \delta(1)$;

е) если $0 \neq b \in K \backslash U(K)$, то $\delta(b) < \delta\left(b^2\right) < \ldots < \delta\left(b^n\right) < \ldots$, поэтому множество значений евклидовой нормы бесконечно.

14.12. Пусть K — евклидово кольцо, $0 \neq a, b \in K$. Докажите, что:

а) если $a = bc$, где b и c необратимы, то $\delta(b), \delta(c) < \delta(a)$;

б) если $a = bq + r$, то $(a, b) = (b, r)$;

в) существуют (a, b) и $[a, b]$, причем найдутся $u, v \in K$ со свойством $(a, b) = au + bv$;

г) a, b взаимно просты в точности тогда, когда существуют $u, v \in K$, для которых $au + bv = 1$;

д) если $(a, b) = 1$ и $(a, c) = 1$, то $(a, bc) = 1$;

е) если $b \mid a$, $c \mid a$ и $(b, c) = 1$, то $bc \mid a$;

ж) если $a \mid bc$ и $(a, b) = 1$, то $a \mid c$.

14.13. Пусть δ — евклидова норма в евклидовом кольце K. Тогда:

а) для любого $n \in \mathbb{N}$ функция $n\delta$ также является евклидовой нормой в K;

б) если функция $f\colon \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$ монотонно возрастает, то композиция $(f \circ \delta)(x) = f(\delta(x))$ также является евклидовой нормой в кольце K.

14.14. 1) Простое число $p \in \mathbb{Z}$ остается простым в $\mathbb{Z}[i]$ тогда и только тогда, когда $p = 4k - 1$.

2) Всякое простое число $p = 4k + 1$ представимо в виде $p = m^2 + n^2$ для некоторых $m, n \in \mathbb{Z}$.

3) Если простое число $p \in \mathbb{Z}$ допускает нетривиальное разложение в $\mathbb{Z}[i]$, то $p = (m + in)(m - in) = m^2 + n^2$.

4) Число $l \in \mathbb{Z}$ представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда в каноническом разложении числа l на простые множители каждый простой делитель $p = 4k - 1$ входит с четным показателем.

14.15. Факторкольцо $\mathbb{Z}[i]/(n)$, где n — натуральное число, является полем в точности тогда, когда n — простое число, не равное сумме двух квадратов целых чисел.

14.16. Если $p = 4k - 1$ — простое число, то многочлен $x^2 + 1$ неприводим над полем $\mathbb{Z}_p$.

14.17. Ненулевой элемент p факториального кольца K является простым в точности тогда, когда $K/(p)$ — область.

14.18. Пусть K — евклидово кольцо с нормой δ, $0 \neq a \in K$. Покажите, что $K/(a) = \{\overline{b} = b + (a) \mid b = 0$ или $\delta(b) < \delta(a)\}$.

14.19. Построить факторкольца:

а) $\mathbb{Z}[i]/(1 + i)$, $\mathbb{Z}[i]/(1 + 2i)$;

б) $\mathbb{Z}\left[\sqrt{-2}\right]/(2)$, $\mathbb{Z}\left[\sqrt{-2}\right] / \left(1 + \sqrt{-2}\right)$;

в) $\mathbb{Q}[x]/(x)$, $\mathbb{Q}[x]/\left(x^2 + 1\right)$, $\mathbb{Q}[x]/\left(x^2 - 2\right)$;

г) $F_2[x]/\left(x^2\right)$, $F_2[x]/(x^2+1)$, $F_2[x]/(x^2+x+1)$.

14.20. Будут ли идеалы I в указанных ниже кольцах, порожденные элементами:

а) n и $x_1, \ldots, x_m$ в $\mathbb{Z}[x_1, \ldots, x_m]$, $n \in \mathbb{N}$, б) $x_1, \ldots, x_m$ в $P[x_1, \ldots, x_m]$ над полем P,

главными? Найдите $\mathbb{Z}[x_1, \ldots, x_m]/I$ и $P[x_1, \ldots, x_m]/I$ (см. 12.41, 12.48 и 13.32).

14.21. Покажите, что все конечные суммы вида $\sum a_i 2^{r_i}$ с целыми коэффициентами a_i и неотрицательными рациональными r_i, знаменатели которых — степени данного простого числа p, образуют кольцо относительно обычных операций сложения и умножения чисел. Какие элементы этого кольца являются простыми? Выполняется ли в этом кольце условие разложимости на простые множители?

14.22. Является ли кольцо $\mathbb{Z}[\sqrt{-5}]$ кольцом с разложением на простые множители? Будет ли оно факториальным? Покажите, что, например, числа $a = 9$ и $b = 6 + 3\sqrt{-5}$ в этом кольце не имеют НОД.

14.23. Докажите евклидовость следующих колец и найдите группы их обратимых элементов:

а) $\mathbb{Z}[i]$; б) $\mathbb{Z}[\omega]$ (см. 11.53); в) $\mathbb{Z}[\sqrt{-2}]$.

Покажите, что подкольцо $\mathbb{Z}[\sqrt{-3}]$ кольца $\mathbb{Z}[\omega]$ является кольцом с разложением на простые множители, но не факториальным.

14.24. Покажите евклидовость колец:

а) $\mathbb{Q}^{(p)}$ с нормой $\delta(ap^t) = |a|$, где $a, t \in \mathbb{Z}$ и p не делит a;

б) $\mathbb{Q}_p$ с нормой $\delta(\frac{a}{b}p^t) = p^t$, где $a, b, t \in \mathbb{Z}$, $a \neq 0$, $t \geqslant 0$ и p не делит ab.

14.25. Многочлен $f(x) \in K[x]$ положительной степени, неприводимый над факториальным кольцом K, неприводим также над его полем частных Q.

14.26. Докажите критерий неприводимости Эйзенштейна. Пусть $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$, где простое число $p \,|\, a_1, \ldots, a_n$, но $p^2 \nmid a_n$. Тогда $f(x)$ неприводим над $\mathbb{Q}$.

Используя этот критерий, докажите, что $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ неприводим над $\mathbb{Q}$ при любом простом p.

14.27. Разложение на простые множители в $\mathbb{Z}_8[x]$ неоднозначно.

14.28. В области главных идеалов всякий собственный идеал является произведением конечного числа простых идеалов.

14.29. Пусть K — факториальное кольцо и S — его мультипликативное подмножество ($0 \notin S$). Покажите, что подмножество $S^{-1}K = \{x/s \,|\, x \in K, s \in S\}$ в кольце частных кольца K является факториальным кольцом и что простые элементы в $S^{-1}K$ — это те же простые $p \in K$, для которых $(p) \cap S = \varnothing$.

14.30. Пусть K — область с разложением на простые множители. Если группа $U(K)$ обратимых элементов кольца K конечна или множество $U(K) \cup \{0\}$ образует подгруппу аддитивной группы кольца K, то множество классов простых ассоциированных элементов в кольце K бесконечно.

Среди факториальных колец K, в каждом из которых множество $U(K) \cup \{0\}$ бесконечно и не образует в K^+ подгруппы, существуют кольца, содержащие как любое конечное число классов простых ассоциированных элементов, так и бесконечное множество этих классов. Так, $\mathbb{Q}_\pi$, где $\pi = \{p_1, \ldots, p_n\}$, факториально и содержит точно n классов простых ассоциированных элементов. Кольцо $\mathbb{Q}^{(2)}$ факториально и число его классов простых ассоциированных элементов бесконечно (см. 14.10).

Пусть k — целое число, отличное от 1, и свободное от квадратов. Функция $n(a+b\sqrt{k}) = a^2 - kb^2$ называется *нормой поля* $\mathbb{Q}(\sqrt{k})$.

Напомним, что алгебраические числа и целые алгебраические числа определены в Предварительных сведениях.

14.31. Покажите, что норма является полной мультипликативной функцией, т.е. для любых $r, s \in \mathbb{Q}(\sqrt{k})$ справедливо равенство $n(rs) = n(r)n(s)$.

Пусть $D(k)$ — кольцо целых чисел в $\mathbb{Q}(\sqrt{k})$. Можно показать, что $D(k) = \mathbb{Z}[k]$ при $k \equiv 2, 3 \pmod 4$;

$$D(k) = \left\{ \frac{a}{2} + \frac{b}{2}\sqrt{k} \,\middle|\, a, b \in \mathbb{Z},\ 2|(a-b) \right\} \text{ при } k \equiv 1 \pmod 4.$$

В последнем случае $D(k) = \mathbb{Z} + \mathbb{Z}((-1+\sqrt{k})/2)$ (см. также 28.17–28.23).

Покажите, что $D(k)$ является кольцом с разложением. Кольца $D(k)$ называются *квадратичными*. Доказано, что евклидовых вещественных квадратичных колец насчитывается семнадцать и для них k = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97. Евклидовых мнимых квадратичных колец существует только пять (при $k = -1, -2, -3, -7, -11$). При $k = -1, -2, -3, -7, -11, -19, -43, -67, -163$ кольца $D(k)$ будут факториальными.

14.32. Выполнить деления с остатком в следующих кольцах относительно указанных норм δ.

1) $\mathbb{Z}[i]$: $40 + i$ на $3 - i$, $15 + 16i$ на $7 + i$, $\delta(a + bi) = a^2 + b^2$.

2) $\mathbb{Z}[\sqrt{-2}]$: $20 - 7\sqrt{-2}$ на $6 + \sqrt{-2}$, 100 на $17 + 5\sqrt{-2}$, $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.

3) $\mathbb{Z}[\sqrt{2}]$: $17 + 11\sqrt{2}$ на $8 - 5\sqrt{2}$, $23 + 9\sqrt{2}$ на $7 - 5\sqrt{2}$, $\delta(a + b\sqrt{2}) = |a^2 - 2b^2|$.

4) $\mathbb{Z}[\sqrt{3}]$: $40-11\sqrt{3}$ на $7+5\sqrt{3}$, $28+11\sqrt{3}$ на $10-8\sqrt{3}$, $\delta(a+b\sqrt{3})=|a^2-3b^2|$.

14.33. Выполнить деления с остатком в следующих кольцах.

1) $\mathbb{Q}^{(5)}$: 1100 на 1000, 91 на 17.

2) $\mathbb{Q}_2$: $\dfrac{320}{7}$ на $\dfrac{146}{5}$, 60 на $\dfrac{40}{37}$.

14.34. Выполнить деления с остатком в следующих кольцах многочленов.

1) $\mathbb{Q}[x]$: $\dfrac{2}{3}x^4+x^3-\dfrac{1}{4}x^2+1$ на $x^2-x+\dfrac{1}{2}$.

2) $F_2[x]$: $x^5+x^3+x^2+x+1$ на x^2+x+1, $x^5+x^4+x^2+x+1$ на x^3+x^2+1.

3) $F_3[x]$: x^6-x^5-1 на x^2-1, $x^5-x^4+x^3-x^2+1$ на x^2-x-1.

14.35. Найдите НОД в следующих кольцах относительно соответствующих евклидовых норм.

1) $\mathbb{Q}^{(5)}$: 7585 и $\dfrac{2501}{5}$, $\dfrac{121}{125}$ и $\dfrac{36}{25}$.

2) $\mathbb{Q}_3$: 630 и $\dfrac{69}{77}$, 165 и $\dfrac{189}{13}$.

3) $\mathbb{Z}[\sqrt{2}]$: $9-5\sqrt{2}$ и $6+2\sqrt{2}$, $17-3\sqrt{2}$ и $25+\sqrt{2}$.

4) $\mathbb{Z}[\sqrt{3}]$: $4+7\sqrt{3}$ и $2+\sqrt{3}$, $15+2\sqrt{3}$ и $7-\sqrt{3}$.

5) $\mathbb{Z}[i]$: $15-2i$ и $17+3i$, $12-5i$ и $10+i$.

6) $\mathbb{Z}[\sqrt{-2}]$: $14-3\sqrt{-2}$ и $8+5\sqrt{-2}$, $7+\sqrt{-2}$ и $17+\sqrt{-2}$.

7) $F_2[x]$: $x^6+x^4+x^3+x^2+x+1$ и x^4+x^3+1, $x^5+x^3+x^2+1$ и x^2+x+1.

8) $F_3[x]$: $x^6-x^4-x^3-x^2+x+1$ и x^3-x^2-1, $x^5-x^4+x^2-x+1$ и x^2+x-1.

14.36. Пользуясь свойством НОК и НОД из упражнения 14.6 б), вычислите НОК для элементов из упражнения 14.35.

Глава IV. Модули

15 Основные понятия теории модулей

Пусть R — ассоциативное кольцо с 1. *Левый модуль* ${}_RM$ — это аддитивная абелева группа M и такое отображение $R\times M\to M$, обозначаемое ra ($r\in R$, $a\in M$), что $r(a+b)=ra+rb$, $(r+s)a=ra+sa$, $r(sa)=(rs)a$ и $1\cdot a=a$ для всех $r,s\in R$ и $a,b\in M$. Говорят также, что M — левый модуль над кольцом R. Отображение $R\times M\to M$ называется *модульным умножением* на M. Само кольцо R иногда называют *кольцом скаляров*, а его элементы — *скалярами*. Правые R-модули определяются аналогично. Именно правый R-модуль N_R — это аддитивная абелева группа N и такое отображение $N\times R\to N$, обозначаемое ar ($a\in N$, $r\in R$), что $(a+b)r=ar+br$, $a(r+s)=ar+as$, $(ar)s=a(rs)$ и $a\cdot 1=a$ для всех $a,b\in N$ и $r,s\in R$. Конкретные модули могут быть левыми или правыми. Нет канонического способа превращения левого модуля в правый (над одним кольцом) и наоборот. Однако в общей теории можно ограничиться модулями одного вида. Существует переход от левых модулей к правым и наоборот, основанный на том, что любой левый R-модуль можно рассматривать как правый над противоположным кольцом R° (см. 15.3). Поэтому есть соответствие между утверждениями о левых модулях и утверждениями о правых модулях.

Под *подмодулем* A левого R-модуля M понимается подгруппа A в M со свойством $ra\in A$ для всех $r\in R$ и $a\in A$. Факторгруппу M/A можно рассматривать как R-модуль, если положить $r(m+A)=rm+A$ для каждого смежного класса $m+A\in M/A$ и $r\in R$. Этот модуль называется *фактормодулем* и обозначается ${}_RM/A$ или просто M/A.

Пересечение любого семейства подмодулей также является подмодулем. Поэтому для всякого подмножества $S\subseteq {}_RM$ определен наименьший по включению подмодуль $\langle S\rangle$, порожденный подмножеством S. Модуль называется *циклическим*, если он порождается одним элементом. Каждый модуль порождается некоторым множеством элементов. Если m — кардинальное число, то модуль называется *m-порожденным*, если он порождается не более чем m элементами.

Отображение $R\times R\to R$, $(r,s)\to rs$ определяет на аддитивной группе R^+ структуру левого R-модуля ${}_RR$ и правого R-модуля R_R. Подмодули модуля ${}_RR$ (соответственно, R_R) — это в точности левые (соответственно, правые) идеалы кольца R.

Множество всех подмодулей модуля M обозначим через $L(M)$. Относительно теоретико-множественного включения подмодулей $L(M)$ образует частично упорядоченное множество. На самом деле в соответствии с § 1, имеем решетку подмодулей. Точной нижней гранью для $A,B\in L(M)$ является пересечение $A\cap B$, а точной верхней гранью — сумма $A+B$, где $A+B=\{a+b\,|\,a\in A, b\in B\}$.

Аннулятором модуля ${}_RM$ называется множество $\operatorname{Ann} M=\{r\in R\,|\,rM=0\}$. Модуль ${}_RM$ называется *точным*, если $\operatorname{Ann} M=0$.

Если $m\in M$ и M — левый (правый) R-модуль, то $\ell(m)=\{a\in R\,|\,am=0\}$ ($r(m)=\{a\in R\,|\,ma=0\}$). Иногда $\ell(m)$ ($r(m)$) обозначают через $\operatorname{Ann}(m)$.

Модуль M называется *дистрибутивным*, если решетка $L(M)$ его подмодулей дистрибутивна, т.е. $A\cap(B+G)=A\cap B+A\cap G$ для любых $A,B,G\in L(M)$.

Подмодуль A модуля M называется *малым* в M, если для любого подмодуля $B\subseteq M$ равенство $A+B=M$ влечет совпадение B с M. Правый идеал A кольца R называется *малым*, если A_R — малый подмодуль в R_R.

Подмодуль модуля M называется *существенным* (или *большим*), если его пересечение с любым ненулевым подмодулем модуля M отлично от нуля.

Ненулевой модуль M называется *простым* (или *неприводимым*), если он содержит только тривиальные подмодули.

Подмодуль фактормодуля модуля M называется *подфактором* модуля M.

Если M — модуль, то его *цоколем* $\operatorname{Soc} M$ называется сумма всех его простых подмодулей. Если таких подмодулей нет, то $\operatorname{Soc} M=0$.

Модуль называется *равномерным*, если любые два его ненулевых подмодуля имеют ненулевое пересечение.

Под *гомоморфизмом* модулей (кратко *R-гомоморфизмом*) понимается гомоморфизм абелевых групп $f\colon M\to N$, для которого $f(rx)=rf(x)$ при всех $r\in R$, $x\in M$. Гомоморфизм $f\colon M\to M$ называется *эндоморфизмом* модуля M. Тождественный эндоморфизм модуля M обозначается через 1_M.

Эпиморфизм (мономорфизм) $f\colon M\to N$ модулей называется *расщепляющимся*, если $\operatorname{Ker} f$ ($\operatorname{Im} f$) — прямое слагаемое в M (в N).

Множество всех эндоморфизмов $\operatorname{End}_R M$ модуля ${}_RM$ является подкольцом кольца эндоморфизмов $\operatorname{End} M$ абелевой группы M. Кольцам эндоморфизмов абелевых групп посвящен § 26.

Модуль ${}_RT$ над кольцом R называется *кообразующим*, если для любого ненулевого модуля ${}_RM$ существует ненулевой гомоморфизм $M\to T$.

Подмодуль $A^\bullet \subseteq M$ называется *аддитивным дополнением*, сокращенно а.д., для подмодуля A в M, если $A^\bullet$ — минимальный подмодуль в M со свойством $A + A^\bullet = M$.

Подмодуль $A' \subseteq M$ называется *дополнением по пересечению*, сокращенно д.п., (или просто *дополнением*) для подмодуля A в M, если A' — максимальный подмодуль в M со свойством $A \cap A' = 0$.

Подмодуль H модуля M называется *дополнительным*, если H — дополнение некоторого подмодуля модуля M; *вполне инвариантным*, если $f(H) \subseteq H$ для всякого эндоморфизма f модуля M.

Последовательность модульных гомоморфизмов $A \xrightarrow{f} B \xrightarrow{g} C$ называется *точной*, если $\operatorname{Im} f = \operatorname{Ker} g$. С подмодулем N модуля M ассоциируется точная последовательность $0 \to N \to M \to M/N \to 0$, где отображение $N \to M$ есть вложение, а $M \to M/N$ — канонический эпиморфизм, $x \mapsto x + N$, $x \in M$.

Если M и X — R-модули, то через $\operatorname{Hom}_R(M, X)$ обозначается множество всех R-гомоморфизмов модуля M в X. Тогда $\operatorname{Hom}_R(M, X)$ есть абелева группа относительно поточечного сложения гомоморфизмов. Если R — коммутативное кольцо, то $\operatorname{Hom}_R(M, X)$ можно превратить в R-модуль, полагая $(af)(x) = a(f(x))$, $a \in R$.

Пусть Y — R-модуль и $M \xrightarrow{f} X$ — R-гомоморфизм. Тогда имеем индуцированные гомоморфизмы

$$f^* = \operatorname{Hom}_R(f, 1_Y) : \operatorname{Hom}_R(X, Y) \to \operatorname{Hom}_R(M, Y),$$
$$f_* = \operatorname{Hom}_R(1_Y, f) : \operatorname{Hom}_R(Y, M) \to \operatorname{Hom}_R(Y, X),$$

задаваемые правилами $g \mapsto g \circ f$ и $g \mapsto f \circ g$ соответственно.

Если A_i $(i \in I)$ — некоторое семейство левых R-модулей, то декартово произведение $M = \prod\limits_{i \in I} A_i$ естественным образом можно рассматривать как левый R-модуль, если модульные операции определить покомпонентно (говорят также «покоординатно»):

$$(\dots, a_i, \dots) + (\dots, b_i, \dots) = (\dots, a_i + b_i, \dots) \text{ и } r(\dots, a_i, \dots) = (\dots, ra_i, \dots)$$

для любых $(\dots, a_i, \dots), (\dots, b_i, \dots) \in M$ и $r \in R$. В этом случае модуль $M = \prod\limits_{i \in I} A_i$ называется *прямым произведением семейства* A_i $(i \in I)$. Подмодуль в $\prod\limits_{i \in I} A_i$, состоящий из элементов $(\dots, a_i, \dots)$, у которых множество индексов $i \in I$ с $a_i \neq 0$ конечно, называется *внешней прямой суммой семейства* A_i $(i \in I)$; обозначение: $\bigoplus\limits_{i \in I} A_i$. Если все $A_i \cong A$ $(i \in I)$, то говорят о прямом произведении (соответственно, прямой сумме) из I *изоморфных копий* модуля A, и пишут $\prod\limits_{|I|} A$ или $A^{|I|}$ (соответственно, $\bigoplus\limits_{|I|} A$).

Если M_i $(i \in I)$ — семейство подмодулей модуля M со свойствами $M = \sum\limits_{i \in I} M_i$ и $M_i \cap (\sum\limits_{j \neq i} M_j) = 0$, то в этом случае говорят, что M является (*внутренней*) *прямой суммой* своих подмодулей M_i $(i \in I)$, и пишут $M = \bigoplus\limits_{i \in I} M_i$; подмодули M_i называются *прямыми слагаемыми* модуля M. Как и в случае колец, различие между внутренней и внешней прямой суммой — чисто теоретико-множественное. Действительно, если $M = \bigoplus\limits_{i \in I} A_i$ — внешняя прямая сумма как выше, то соответствие $a_i \mapsto (\dots, 0, a_i, 0, \dots)$ является изоморфизмом между модулем A_i и подмодулем A_i' модуля M всех векторов $(\dots, 0, a_i, 0, \dots)$. Модули A_i' $(i \in I)$ порождают внутри M модуль A, являющийся прямой суммой подмодулей A_i', и $M = A$. Если $M = \prod\limits_{i \in I} M_i$ (соответственно, $M = \bigoplus\limits_{i \in I} M_i$), то эпиморфизм $\pi_i \colon M \to M_i$, $\pi_i(\dots, a_i, \dots) = a_i \in M_i$, называется *канонической проекцией* модуля M на прямой множитель (соответственно, прямое слагаемое) M_i.

Модуль M называется *неразложимым*, если 0 и M — единственные подмодули, являющиеся прямыми слагаемыми в M.

Модуль M называется *строго неразложимым*, если все фактормодули модуля M являются неразложимыми.

Модуль M называется *регулярным*, если каждый его циклический подмодуль является прямым слагаемым в M.

Элемент a модуля ${}_RM$ называется *периодическим*, если $\ell(a)$ содержит элемент, не являющийся делителем нуля в R. Множество $t(M)$ всех периодических элементов модуля M называется его *периодической частью*. Говорят, что M — *модуль без кручения* (в смысле Леви), если $t(M) = 0$.

Пусть ${}_RM$ — ненулевой модуль и S — подмножество в M. Говорят, что S — *базис модуля* M, если $S \neq \varnothing$, S порождает M и линейно независимо, т.е. из $r_1 m_1 + \dots + r_n m_n = 0$, $r_i \in R$, $m_i \in M$, следует $r_i = 0$ (i=1, … ,n). Всякое кольцо с 1, рассматриваемое как модуль над собой, обладает базисом, состоящим из 1.

Пусть I — непустое множество и пусть ${}_RR_i = {}_RR$ для каждого $i \in I$. Модуль $F = \bigoplus\limits_{i \in I} R_i$ обладает базисом, состоящим из элементов e_i, i-й компонентой которых является единичный элемент из R_i, а все другие компоненты равны 0.

Левый модуль M над кольцом R называется *свободным циклическим*, если ${}_RM \cong {}_RR$ (т.е. существует такой $m \in M$, что $M = Rm$ и $\ell(m) = 0$; в этом случае m называется *свободным образующим* модуля M).

Под ненулевым *свободным* модулем понимается модуль, обладающий базисом, т.е. ненулевой свободный модуль является прямой суммой свободных циклических модулей.

Модуль M называется *конечно точным*, если существует такое $n \in \mathbb{N}$, что модуль M^n содержит свободный циклический модуль.

Пересечение $J(M)$ ядер всех гомоморфизмов модуля M в простые модули называется *радикалом Джекобсона* модуля M; $J(M) = M$, если в M нет максимальных подмодулей, $J(M)$ совпадает с пересечением всех максимальных подмодулей модуля M, если они существуют.

Модуль называется *полупримитивным*, если $J(M) = 0$.

Модуль называется *цепным*, если все его подмодули образуют цепь.

Модуль называется *модулем Безу* или *локально циклическим*, если каждый его конечно порожденный подмодуль является циклическим. Модуль называется *вполне циклическим*, если все его подмодули являются циклическими модулями.

Модуль называется *конечномерным* (в смысле Голди), если он не содержит бесконечных прямых сумм ненулевых подмодулей.

Модуль M, являющийся левым R-модулем и правым S-модулем одновременно, причем $(rm)s = r(ms)$ для $r \in R$, $s \in S$, $m \in M$, называется *R-S-бимодулем*. В этом случае используется обозначение ${}_RM_S$.

Задачи

15.1. а) Пусть M — абелева группа, R — кольцо и $f\colon R \to \operatorname{End} M$ — кольцевой гомоморфизм. Операция $ra = f(r)(a)$ ($r \in R$, $a \in M$) превращает M в левый R-модуль.

б) Каждый левый R-модуль M может быть реализован с помощью указанного в а) способа, причем единственным образом.

в) Сформулируйте и докажите аналогичные а) и б) утверждения для кольцевых антигомоморфизмов $f\colon R \to \operatorname{End} M$ и правых R-модулей M. *Кольцевой антигомоморфизм* f — это такой аддитивный гомоморфизм, что $f(rs) = f(s)f(r)$ для всех $r, s \in R$.

15.2. Пусть в ситуации упр. 15.1, а) f и g — кольцевые гомоморфизмы $R \to \operatorname{End} M$. Соответствующие им два R-модуля M изоморфны в точности тогда, когда $g = \phi f$ для некоторого внутреннего автоморфизма ϕ кольца $\operatorname{End} M$ (внутренние автоморфизмы определяются в 12.52).

15.3. Пусть M — левый R-модуль. Полагая $ar = ra$ ($r \in R$, $a \in M$), получаем структуру правого модуля на M над кольцом R°, противоположным к R (см. 11.22). Таким образом, каждый левый модуль над коммутативным кольцом R можно считать правым R-модулем и наоборот.

15.4. Пусть M — левый R-модуль и $S = \operatorname{End}_R M$. Для любых двух эндоморфизмов f и g из S определим произведение $f \circ g$, положив $(f \circ g)(a) = g(f(a))$ для всех $a \in M$. Относительно этого нового умножения все эндоморфизмы модуля M образуют еще одно кольцо эндоморфизмов S°. Кольца S и S° противоположны в смысле 11.22.

15.5. Пусть V — векторное пространство размерности n над полем F. В соответствии с 15.4 имеем два кольца операторов пространства V. Каждое из них известным способом изоморфно кольцу всех $n \times n$-матриц над полем F. Какое из этих колец соответствует записи матриц «по столбцам», какое — «по строкам»?

15.6. Пусть A — R-модуль. Для любого R-модуля B каждый аддитивный изоморфизм $A \to B$, не являющийся R-модульным, дает структуру R-модуля на A, отличную от исходной. При этом, «новый» R-модуль A изоморфен R-модулю B. Наоборот, если на A имеется еще одна R-модульная структура с тем же сложением, то существует аддитивный изоморфизм модуля A на какой-то R-модуль B, не являющийся R-модульным.

R-модуль A называется *модулем с однозначным модульным умножением* или, кратко, *UM-модулем*, если на группе A нельзя задать другого R-модульного умножения, т.е. имеющаяся на A структура R-модуля единственна.

15.7. Следующие свойства R-модуля A эквивалентны:

а) A — UM-модуль;

б) существует единственный гомоморфизм колец $R \to \operatorname{End} A$;

в) для любого R-модуля B всякий аддитивный изоморфизм A на B является R-модульным.

Аддитивный гомоморфизм $\delta\colon R \to M$, где M — некоторый R-R-бимодуль, называется *дифференцированием* (со значениями в M), если $\delta(rs) = r\delta(s) + \delta(r)s$ для всех $r, s \in R$ (ср. с 11.45).

15.8. Пусть A и B — R-модули.

1) $f\colon A \to B$ — аддитивный, но не R-модульный гомоморфизм. Тогда на группе $B \oplus A$ существует R-модульное умножение, отличное от естественного умножения $r(b + a) = rb + ra$ ($r \in R$, $b \in B$, $a \in A$), имеющегося в прямой сумме $B \oplus A$.

2) Группа $\mathrm{Hom}\,(A,B)$ является R-R-бимодулем, где модульные произведения rf и fr ($r\in R$, $f\in \mathrm{Hom}\,(A,B)$) задаются равенствами $(rf)(a)=rf(a)$ и $(fr)(a)=f(ra)$, $a\in A$.

3) Любой аддитивный гомоморфизм $f\colon A\to B$ дает дифференцирование $\delta_f\colon R\to \mathrm{Hom}\,(A,B)$, где $\delta_f(r)=rf-fr$, $r\in R$. δ_f — *внутреннее дифференцирование*, определяемое f; оно отлично от нуля в точности тогда, когда f — не R-модульный гомоморфизм.

15.9. (См. 15.8). Пусть $\delta\colon R\to \mathrm{Hom}\,(A,B)$ — ненулевое дифференцирование. В таком случае на группе $B\oplus A$ существует R-модульное умножение, отличное от естественного умножения, имеющегося в прямой сумме $B\oplus A$.

15.10. Пусть даны кольца S и R и кольцевой гомоморфизм $e\colon S\to R$. На всяком левом R-модуле A можно задать структуру левого S-модуля по правилу $sa=e(s)a$ для всех $s\in S$, $a\in A$. Этот S-модуль A называется *притягивающим* S-модулем. Аналогично, правый R-модуль можно превратить в правый S-модуль. В частности, R является притягивающим левым и правым S-модулем.

15.11. Пусть $e\colon S\to R$ — гомоморфизм колец и A — R-модуль. Тогда:

а) всякий R-подмодуль в A будет S-подмодулем;

б) если $f\colon A\to B$ — гомоморфизм R-модулей, то f будет гомоморфизмом S-модулей;

в) если e — сюръективный гомоморфизм, то всякий S-подмодуль в A будет R-подмодулем и любой S-гомоморфизм будет R-гомоморфизмом.

Кольцо R называется *кольцом с однозначным сложением*, или *UA-кольцом*, если на R нельзя задать другого сложения так, чтобы R было кольцом относительно этого нового сложения и старого умножения.

15.12. 1) Если существует мультипликативный изоморфизм колец R и S (т.е. изоморфизм их мультипликативных полугрупп), не являющийся аддитивным, то на R можно так определить другое сложение, что R становится кольцом. Таким образом, R не UA-кольцо. Верно и обратное.

2) R есть UA-кольцо в точности тогда, когда любой мультипликативный изоморфизм $R\to S$ является кольцевым.

15.13. 1) Для любого кольца R и натурального числа $n\geqslant 2$ кольцо всех $n\times n$-матриц и кольцо всех нижних треугольных $n\times n$-матриц над кольцом R являются UA-кольцами.

2) Прямое произведение UA-колец есть UA-кольцо.

R-модуль M называется *модулем с однозначным сложением* (кратко, *UA-модулем*), если на M нельзя задать другой операции сложения так, чтобы M был модулем над кольцом R относительно нового сложения и прежнего модульного умножения.

Отображение $f\colon M\to N$ левых R-модулей называется *R-однородным*, если $f(rx)=rf(x)$ при всех $r\in R$, $x\in M$.

15.14. Пусть M и N — R-модули и f — R-однородная биекция M на N, не являющаяся изоморфизмом. С помощью f на M можно задать другое сложение так, что M остается R-модулем со старым R-модульным умножением. При этом, «новый» R-модуль M изоморфен R-модулю N. Обратно, если на M имеются две структуры R-модуля с различными операциями сложения, то существует R-однородная биекция M на какой-то модуль N, не являющаяся изоморфизмом.

15.15. R-модуль M есть UA-модуль в точности тогда, когда любая R-однородная биекция $M\to N$ является изоморфизмом.

15.16. Если все R-модули являются UA-модулями, то R есть UA-кольцо. Обратное не всегда верно.

15.17. Пусть R — кольцо всех $n\times n$-матриц ($n\geqslant 2$) над некоторым кольцом и M — произвольный R-модуль. Тогда каждое R-однородное отображение $M\to M$ есть эндоморфизм.

15.18. Пусть V — конечномерное векторное пространство над полем F и α — некоторый его оператор. Проверить, что V есть модуль над кольцом многочленов $F[x]$. Соответствующее модульное умножение определяется формулой $f(x)\cdot a=f(\alpha)(a)$ ($f(x)\in F[x]$, $a\in V$). Что представляют собой подмодули этого модуля? В терминах минимального многочлена оператора α выяснить, когда V — неразложимый модуль.

15.19. Всякая абелева группа является модулем над кольцом целых чисел $\mathbb{Z}$. Обратно, если A — $\mathbb{Z}$-модуль с модульным умножением $\circ$, то $k\circ a=ka$ для всех $k\in\mathbb{Z}$ и $a\in A$. Таким образом, $\mathbb{Z}$-модули и абелевы группы можно считать одними и теми же объектами.

15.20. Если R — локальное кольцо, то $J(R)$ — единственный его максимальный левый (соответственно, правый) идеал, и состоит он из всех необратимых элементов кольца R.

15.21. Для любого левого R-модуля A справедлив изоморфизм левых R-модулей $\mathrm{Hom}_R(R,A)\cong A$. Найдите обратный изоморфизм.

15.22. Пусть R — кольцо, $R_n=M(n,R)$ и $n\geqslant 1$. Следующие кольца изоморфны:

а) $\mathrm{End}_R\,(R^n)$ и R_n; б) $\mathrm{End}_{R_n}\,(R^n)$ и R.

15.23. 1) Пусть $\overline{f}$ — любое отображение базиса $\{p_i\}_{i\in I}$ свободного модуля ${}_RP$ в произвольный модуль ${}_RM$. Тогда правилом $f(\sum a_ip_i)=\sum a_i\overline{f}(p_i)$, где $a_i\in R$, корректно определен гомоморфизм $f\colon P\to M$.

2) Пусть m — кардинальное число, ${}_RM$ — m-порожденный модуль, P — свободный модуль с базисом мощности m. Тогда существует эпиморфизм $f\colon P \to M$. Следовательно, каждый модуль является гомоморфным образом свободного модуля.

15.24. Если M — максимальный правый идеал кольца R и $s \in R\backslash M$, то $s^{-1}M = \{r \in R \,|\, sr \in M\}$ также является максимальным правым идеалом и $R/s^{-1}M \cong R/M$.

15.25. Если R — коммутативная область главных идеалов и M — свободный R-модуль с базисом, содержащим более одного элемента, то каждый эндоморфизм модуля M есть сумма двух его автоморфизмов (ср. с 11.17).

15.26. Для модуля M_R равносильны следующие условия:

а) M — дистрибутивный модуль;

б) $(A+B)\cap(A+G) = A + B\cap G$ для любых $A, B, G \in L(M)$;

в) $(m+n)\,R = mR \cap (m+n)\,R + nR \cap (m+n)\,R$ для любых $m, n \in M$.

15.27. Дистрибутивность модуля M равносильна как дистрибутивности всех его подфакторов, так и дистрибутивности всех его 2-порожденных подмодулей.

15.28. Для модуля M_R равносильны следующие условия:

а) M — дистрибутивный модуль;

б) для любых $m, n \in M$ существует такой $a \in R$, что $maR + n\,(1-a)\,R \subseteq mR \cap nR$;

в) для любых $m, n \in M$ существуют такие $a, b, c, d \in R$, что $1 = a + b$, $ma = nc$ и $nb = md$;

г) для любых $m, n \in M$ существует такой правый идеал B кольца R, что $(m+n)\,R = mB + nB$.

15.29. Пусть M_R — дистрибутивный модуль. Тогда:

а) если $m, n \in M$ и $mR \cap nR = 0$, то существует такой $a \in R$, что $ma = n\,(1-a) = 0$;

б) $\mathrm{Hom}_R(G, H) = 0$ для всех таких $G, H \in L(M)$, что $G \cap H = 0$;

в) $\mathrm{Hom}_R\left(G/\left(G\cap H\right), H/\left(G\cap H\right)\right) = 0$ для любых $G, H \in L(M)$;

г) $\mathrm{Hom}_R\left(M/H, M/G\right) = 0$ для любых таких $G, H \in L(M)$, что $G + H = M$.

15.30. Следующие условия равносильны:

а) любые два подмодуля модуля M сравнимы по включению (т.е. M — цепной модуль);

б) любые два циклических подмодуля модуля M сравнимы по включению.

15.31. Для модуля M_R равносильны следующие условия:

а) M — модуль Безу;

б) каждый 2-порожденный подмодуль модуля M является циклическим;

в) для любых $m, n \in M$ существуют такие $a, b, c, d \in R$, что $m = (ma + nb)\,c$ и $n = (ma + nb)\,d$.

Пусть даны кольца R, S и R-S-бимодуль M. Обозначим через $\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ множество всех матриц вида $\begin{pmatrix} r & m \\ 0 & s \end{pmatrix}$, где $r \in R$, $s \in S$, $m \in M$. Относительно обычного матричного сложения и умножения, выполняемого по правилу

$$\begin{pmatrix} r_1 & m_1 \\ 0 & s_1 \end{pmatrix}\begin{pmatrix} r_2 & m_2 \\ 0 & s_2 \end{pmatrix} = \begin{pmatrix} r_1r_2 & r_1m_2 + m_1s_2 \\ 0 & s_1s_2 \end{pmatrix},$$

$\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ является кольцом, называемым *кольцом обобщенных (треугольных) матриц*.

15.32. Радикал Джекобсона кольца $\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ равен $\begin{pmatrix} J(R) & M \\ 0 & J(S) \end{pmatrix}$.

15.33. Кольцо $\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$ артиново слева (справа) тогда и только тогда, когда R и S — артиновы слева (справа) кольца и M — артинов R-модуль (S-модуль). Аналогичное утверждение верно для свойства нетеровости кольца (ср. с 13.82, 13.83).

15.34. Эпиморфизм $f\colon M \to N$ модулей расщепляется в точности тогда, когда существует такой гомоморфизм $g\colon N \to M$, что $fg = 1_N$.

Идемпотентный эндоморфизм e модуля M называется *проекцией* M на $e(M)$.

15.35. 1) Для подмодуля N модуля M равносильны следующие условия:

а) N является прямым слагаемым модуля M;

б) существует проекция модуля M на N;

в) существует такой эпиморфизм $h\colon M \to N$, что $h(x) = x$ для всех $x \in N$;

г) существуют такие гомоморфизмы $f\colon M \to N$, $g\colon N \to M$, что $fg = 1_N$ — тождественный автоморфизм модуля N.

2) Для проекций e, t ненулевого модуля ${}_RM$ имеет место равенство $\operatorname{Im} e = \operatorname{Im} t$ в точности тогда, когда $t = e + (1 - e)fe$ для некоторого $f \in \operatorname{End}_R M$.

15.36. Пусть $M = A \oplus B$ — прямое разложение модуля M. Покажите, что фактормодуль M/A изоморфен модулю B.

15.37. Пусть A — модуль и $M = A \oplus A = \{x + y \,|\, x, y \in A\}$. Положим $D = \{a + a \,|\, a \in A\}$. Докажите, что D — подмодуль в M и $M = A \oplus D$.

15.38. Пусть модуль $M = A \oplus B$ и N — подмодуль в M, причем $A \subseteq N$. Тогда $N = A \oplus (N \cap B)$.

15.39. Пусть модуль $M = A \oplus B$ и N — такой подмодуль в M, что $N = X \oplus Y$, где $X \subseteq A$, $Y \subseteq B$. Тогда $M/N \cong A/X \oplus B/Y$.

15.40. Для подмодулей A и B модуля M докажите существование:

а) вложения $M/(A \cap B) \to M/A \oplus M/B$;

б) точной последовательности $0 \to A \cap B \to A \oplus B \to A + B \to 0$.

15.41. Пусть

$$\begin{array}{ccccccc} 0 \to & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \to 0 \\ & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & \\ 0 \to & X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z & \to 0 \end{array}$$

— коммутативная диаграмма модулей с точными строками, причем α, β, γ — мономорфизмы. Тогда β является изоморфизмом в точности тогда, когда α и γ — изоморфизмы.

15.42. Пусть $S = \operatorname{End}_R M$. Следующие условия эквивалентны:

а) ${}_RM$ неразложим;

б) S_S неразложим;

в) ${}_SS$ неразложим;

г) 0 и 1 — единственные идемпотенты в S.

15.43. Пусть $R = \mathbb{Z}^{\aleph_0}$. Найдите в модуле R_R подмодуль M, не имеющий конечной системы образующих. Значит, подмодуль циклического модуля может не быть циклическим, а подмодуль конечно порожденного модуля может не быть конечно порожденным.

15.44. 1) Периодическая часть модуля над коммутативным кольцом является его подмодулем.

2) Если M — правый модуль над правым кольцом Ope R, то его периодическая часть $t(M)$ является является подмодулем в M.

15.45. 1) Любой подмодуль в модуле M конечно порожден тогда и только тогда, когда M удовлетворяет условию максимальности для подмодулей.

2) Модуль M конечно порожден тогда и только тогда, когда множество собственных его подмодулей *индуктивно*, т.е. объединение произвольной цепи собственных подмодулей модуля M снова является собственным подмодулем в M. В частности, всякий подмодуль модуля M содержится в некотором максимальном.

15.46. Расширение конечно порожденного модуля при помощи конечно порожденного модуля снова есть конечно порожденный модуль.

15.47. Аннулятор $\operatorname{Ann} M$ левого R-модуля M является двусторонним идеалом кольца R, и операция $(r + \operatorname{Ann} M)x = rx$, $r \in R$, $x \in M$, наделяет M структурой точного $R/\operatorname{Ann} M$-модуля.

15.48. Пусть Y — R-модуль. Докажите, что:

а) для всякой точной последовательности $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ R-модулей индуцированная (см. введение к § 15) последовательность

$$0 \to \operatorname{Hom}_R(C, Y) \xrightarrow{g^*} \operatorname{Hom}_R(B, Y) \xrightarrow{f^*} \operatorname{Hom}_R(A, Y)$$

точна;

б) для всякой точной последовательности $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ R-модулей индуцированная последовательность

$$0 \to \operatorname{Hom}_R(Y, A) \xrightarrow{f_*} \operatorname{Hom}_R(Y, B) \xrightarrow{g_*} \operatorname{Hom}_R(Y, C)$$

точна.

15.49. Пусть $(*)$: $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ — точная последовательность модулей. Эквивалентны следующие условия:

а) существует гомоморфизм $h\colon C \to B$ со свойством $g \circ h = 1_C$;

б) существует гомоморфизм $d\colon B \to A$ со свойством $d \circ f = 1_A$.

При выполнении этих условий имеют место соотношения:

$$B = \operatorname{Ker} g \oplus \operatorname{Im} h,\ B = \operatorname{Im} f \oplus \operatorname{Ker} d,\ B \cong A \oplus C.$$

Если выполнены условия этого упражнения, то говорят, что последовательность $(*)$ *расщепляется*.

15.50. Если B — ненулевой подмодуль модуля M и A — максимальный подмодуль среди подмодулей, имеющих нулевое пересечение с B, то $B + A$ — существенный подмодуль в M.

15.51. Пусть M_R, N_R — модули над кольцом R. Тогда:

а) если I — правый идеал кольца R, $f\colon I \to M$ — гомоморфизм, то f продолжается до некоторого гомоморфизма $g\colon R_R \to M$, если и только если существует такой $m \in M$, что $f(x) = mx$ для всех $x \in I$;

б) если $A \in L(N)$, $h \in \operatorname{Hom}_R(A, M)$, то существует такой существенный подмодуль B модуля N и такой гомоморфизм $f \in \operatorname{Hom}_R(B, M)$, что $A \subseteq B$, h продолжается до f и $f(B) = h(A)$.

Пусть A — правый идеал кольца R с 1. Его *идеализатором* называется множество $I(A) = \{r \in R \mid ra \in A,\ a \in A\}$.

15.52. 1) Идеализатор $I(A)$ — наибольшее подкольцо в R, содержащее A в качестве идеала.

2) Отображение $f \mapsto f(1 + A)$ является кольцевым изоморфизмом $\operatorname{End}_R(R/A) \cong I(A)/A$.

3) Если A — максимальный аннуляторный правый идеал, то $\operatorname{End}_R(R/A)$ не имеет делителей нуля.

15.53. 1) Модуль ${}_RM$ прост в точности тогда, когда $M = Ra$ для любого $0 \neq a \in M$.

2) (Лемма Шура) Если U и V — простые R-модули и $f \in \operatorname{Hom}_R(U, V)$, то или $f = 0$, или f — изоморфизм.

3) Кольцо эндоморфизмов простого модуля является телом.

4) Если U_i $(i = 1, \ldots, n)$ — конечное множество попарно неизоморфных простых R-модулей, то кольцо эндоморфизмов их прямой суммы изоморфно прямому кольцевому произведению тел $D_i = \operatorname{End}_R U_i$ $(i = 1, \ldots, n)$.

15.54. Пусть F — поле и $R = M(2,F)$. Тогда $G = \begin{pmatrix} F & 0 \\ F & 0 \end{pmatrix}$ — простой левый R-модуль.

15.55. Простые модули над кольцом матриц над полем изоморфны между собой.

15.56. Модуль M называется *полупростым* (или *вполне приводимым*), если он удовлетворяет следующим эквивалентным условиям:

а) каждый подмодуль в M является суммой простых подмодулей;

б) M — сумма простых подмодулей;

в) M — прямая сумма простых подмодулей;

г) каждый подмодуль в M является прямым слагаемым.

15.57. Модуль полупрост тогда и только тогда, когда он не содержит собственных существенных подмодулей.

Решетка подмодулей $L(A)$ модуля A называется *решеткой с дополнениями*, если для любого подмодуля B модуля A найдется подмодуль C такой, что $B \cap C = 0$ и $A = B \oplus C$ (см. § 1). Подмодуль C в этом случае называется *дополнительным прямым слагаемым* (кратко, *д.п.с.*) к B.

15.58. 1) Если $L(A)$ — решетка с дополнениями и B — подмодуль в A, то $L(B)$ — также решетка с дополнениями.

2) Если $L(A)$ — решетка с дополнениями, то $J(A) = 0$.

3) Модуль A полупрост в точности тогда, когда $L(A)$ — решетка с дополнениями.

15.59. 1) Сумма полупростых модулей полупроста.

2) Всякий модуль над кольцом матриц над полем является полупростым.

3) Приведите пример модуля M с подмодулем U такого, что M не полупрост, но M/U и U полупросты.

15.60. 1) $\operatorname{Soc} M$ является прямой суммой некоторого множества простых подмодулей модуля M.

2) Цоколь — вполне инвариантный подмодуль модуля M.

3) $M = \operatorname{Soc} M$ в точности тогда, когда M полупрост.

4) $\operatorname{Soc} M$ является наибольшим полупростым подмодулем в M и совпадает с пересечением всех существенных подмодулей модуля M.

15.61. 1) Если $f\colon A \to M$ — эпиморфизм, а B — существенный подмодуль модуля M, то $f^{-1}(B)$ — существенный подмодуль модуля A, где $f^{-1}(B) = \{a \in A \mid f(a) \in B\}$.

2) Если $A \subseteq B \subseteq C$, то A — существенный подмодуль модуля C в точности тогда, когда A — существенный подмодуль модуля B, а B — существенный подмодуль модуля C.

3) Если B и C — существенные подмодули модуля A, то $B \cap C$ — также существенный подмодуль в A.

15.62. Приведите пример модуля, не имеющего существенных максимальных подмодулей.

15.63. Для кольца R эквивалентны следующие условия:

а) каждый левый R-модуль полупрост;

б) ${}_RR$ — полупростой модуль;

в) R_R — полупростой модуль;

г) каждый правый R-модуль полупрост.

Кольцо R называется *классически полупростым* (иногда просто *полупростым*), если оно удовлетворяет одному из условий а) — г) (см. теорему 16.4).

15.64. Пусть R — такое кольцо, что факторкольцо $R/J(R)$ классически полупросто. Покажите, что каждый простой правый (соответственно, левый) R-модуль изоморфен некоторому подмодулю в $(R/J(R))_R$ (соответственно, ${}_R(R/J(R))$).

15.65. Если кольцо R является прямой суммой минимальных правых идеалов A_j $(j \in J)$, то каждый идеал кольца R является прямой суммой некоторых RA_j.

15.66. Пусть e — идемпотент кольца R. Покажите, что:

а) $\mathrm{End}_R(eR) \cong eRe$;

б) если кольцо R полупервично, то eR — минимальный правый идеал в R в точности тогда, когда eRe — тело;

в) если кольцо R полупервично, то eR является минимальным правым идеалом в точности тогда, когда Re — минимальный левый идеал.

15.67. Пусть $e = e^2 \in R$ и $f = f^2 \in R$. Покажите, что:

а) имеет место изоморфизм аддитивных групп $\mathrm{Hom}_R(eR, fR) \cong fRe$, где $fRe = \{fxe \,|\, x \in R\}$;

б) $eR \cong fR$ в точности тогда, когда $vu = e$ и $uv = f$ для некоторых $u, v \in R$;

в) $eR \cong fR$ в точности тогда, когда $Re \cong Rf$.

15.68. Каждый минимальный правый идеал полупервичного кольца R имеет вид eR, где $e = e^2 \in R$.

15.69. Если R — полупервичное кольцо, то цоколи модулей R_R и ${}_RR$ совпадают.

15.70. 1) Коммутативное кольцо является примитивным тогда и только тогда, когда оно поле.

2) Кольцо R примитивно справа тогда и только тогда, когда существует точный простой модуль M_R.

3) Идеал I кольца R примитивен справа тогда и только тогда, когда R/I — примитивное кольцо; это эквивалентно тому, что I — аннулятор простого правого R-модуля.

15.71 (Теорема плотности). Пусть R — примитивное кольцо, M_R — точный простой модуль. Тогда $D = \mathrm{End}_R M$ является телом, а кольцо R канонически вкладывается в кольцо $E = \mathrm{End}_D M$ таким образом, что для любого $e \in E$ и любого конечно порожденного подмодуля G в ${}_DM$ существует элемент $r \in R$, для которого $G(e - r) = 0$ (эндоморфизм e левого D-модуля M записан справа).

15.72. 1) Собственный идеал I кольца R первичен в точности тогда, когда R/I — первичное кольцо.

2) Собственный идеал I кольца R первичен в точности тогда, когда для любых элементов $a, b \in R$ из включения $aRb \subseteq I$ следует, что либо $a \in I$, либо $b \in I$.

3) Примитивный идеал первичен.

15.73. Если M — максимальный правый идеал кольца R, то ассоциированный примитивный идеал $I = \{r \in R \,|\, Rr \subseteq M\}$ совпадает с пересечением всех правых идеалов вида $s^{-1}M$, где $s \in R \backslash M$, $s^{-1}M = \{r \in R \,|\, sr \in M\}$.

15.74. Первичное кольцо, обладающее минимальным правым идеалом, является примитивным справа.

15.75. Модуль M_R называется *подпрямо неразложимым*, если он содержит наименьший ненулевой подмодуль A. Покажите, что в таком случае $\mathrm{Ann}\, A$ является примитивным идеалом кольца R.

15.76. Следующие условия на кольцо R эквивалентны:

а) R — полупервичное кольцо;

б) $\mathrm{rad}\, R = 0$;

в) если A, B — идеалы кольца R и $AB = 0$, то $A \cap B = 0$.

Первичный радикал кольца R является наименьшим среди идеалов K, для которых R/K — полупервичное кольцо.

15.77. Радикал Джекобсона $J(R)$ кольца R:

а) совпадает с множеством всех таких элементов $r \in R$, что при всех $x \in R$ элемент $1 - rx$ обратим справа;

б) является наибольшим среди его идеалов K таких, что $1 - r$ — обратимый элемент при всех $r \in K$;

в) совпадает с пересечением всех максимальных левых идеалов, т.е. $J(R_R) = J({}_RR) = J(R)$;

г) совпадает с пересечением всех примитивных идеалов;

д) совпадает с пересечением правых (левых) аннуляторов всех простых правых (левых) R-модулей;

е) содержит все правые и левые ниль-идеалы кольца R.

15.78. 1) Следующие условия на кольцо R эквивалентны:

а) R полупримитивно справа;

б) $J(R) = 0$;

в) R полупримитивно слева.

2) Кольцо R полупервично (полупримитивно) тогда и только тогда, когда R является подпрямым произведением первичных (примитивных) колец.

15.79 (Лемма Накаямы). Для правого идеала A кольца R равносильны следующие условия:

а) $A \subseteq J(R)$;

б) $(1 - a)\, R = R$ для каждого $a \in A$;

в) A — малый правый идеал кольца R;

г) $MA \neq M$ для любого ненулевого конечно порожденного модуля M_R.

15.80. 1) Если A_i, $i = 1, \ldots, n$, — малые подмодули в M, то $\sum\limits_{i=1}^{n} A_i$ — малый подмодуль в M.

2) Если A — малый подмодуль в M и f — гомоморфизм M в модуль N, то $f(A)$ — малый подмодуль в N.

3) Для элемента $a \in M_R$ подмодуль aR не является малым в M в точности тогда, когда существует максимальный подмодуль C в M такой, что $a \notin C$. В частности, подмодуль aR является малым в M тогда и только тогда, когда $a \in J(M)$.

15.81. Докажите, что $J(M(n, R)) = M(n, J(R))$.

15.82. 1) $J(M)$ — вполне инвариантный подмодуль модуля M, $J(M)$ совпадает с суммой всех малых подмодулей модуля M и совпадает с пересечением ядер гомоморфизмов модуля M в полупростые модули, $M/J(M)$ — полупримитивный модуль.

2) Если $N \in L(M)$ и $J(M/N) = 0$, то $J(M) \subseteq N$.

3) $J(\bigoplus\limits_{i \in I} M_i) = \bigoplus\limits_{i \in I} J(M_i)$.

4) Если M — ненулевой конечно порожденный модуль, то $J(M)$ является наибольшим малым подмодулем модуля M, в частности, $M \neq J(M)$ и $J(R_R)$ — малый идеал в R.

5) Если $f\colon M_R \to N_R$ — гомоморфизм R-модулей, то $f(J(M)) \subseteq J(N)$, причем, если $\operatorname{Ker} f$ — малый подмодуль в M, а f — эпиморфизм, то $f(J(M)) = J(N)$ и $J(M) = f^{-1}(J(N)) = \{m \in M \mid f(m) \in J(N)\}$.

6) $MJ(R) \subseteq J(M)$.

Приведите пример, когда $MJ(R) \neq J(M)$.

15.83. 1) $\operatorname{Soc}(\bigoplus\limits_{i \in I} M_i) = \bigoplus\limits_{i \in I} \operatorname{Soc}(M_i)$.

2) Если $f\colon M_R \to N_R$ — гомоморфизм R-модулей, то $f(\operatorname{Soc}(M)) \subseteq \operatorname{Soc}(N)$, причем, если $\operatorname{Im} f$ — существенный подмодуль в M, а f — мономорфизм, то $f(\operatorname{Soc}(M)) = \operatorname{Soc}(N)$ и $\operatorname{Soc}(M) = f^{-1}(\operatorname{Soc}(N)) = \{m \in M \mid f(m) \in \operatorname{Soc}(N)\}$.

15.84. Пусть $R/J(R)$ — классически полупростое кольцо (см. 15.63). Тогда для всякого модуля M_R:

а) $J(M) = MJ(R)$;

б) $\operatorname{Soc} M = \{m \in M \mid mJ(R) = 0\}$.

15.85. Для кольца R следующие условия эквивалентны:

а) для каждого семейства M_i $(i \in I)$ правых R-модулей $\operatorname{Soc}(\prod\limits_{i \in I} M_i) = \prod\limits_{i \in I} \operatorname{Soc} M_i$;

б) прямое произведение любого числа полупростых правых R-модулей полупросто;

в) каждый правый R-модуль с нулевым радикалом полупрост;

г) кольцо $R/J(R)$ классически полупросто.

15.86. Для левого идеала $U \subseteq {}_R R$ следующие условия эквивалентны:

а) $(\prod\limits_{i \in I} M_i)\, U = \prod\limits_{i \in I} (M_i U)$ для каждого семейства M_i $(i \in I)$ правых R-модулей;

б) ${}_R U$ конечно порожден.

15.87. Если кольцо R коммутативно и нетерово, то для любого семейства M_i ($i \in I$) правых R-модулей $J(\prod\limits_{i\in I} M_i) = \prod\limits_{i\in I} J(M_i)$.

Говорят, что идемпотенты кольца R могут быть *подняты* по модулю идеала $I \subseteq R$, если для любого элемента $u \in R$ со свойством $u^2 - u \in I$ существует такой идемпотент $e \in R$, что $e - u \in I$.

15.88. Идемпотенты могут быть подняты по модулю любого ниль-идеала кольца R. В частности, идемпотенты могут быть подняты по модулю первичного радикала.

15.89. Пусть A — подмодуль модуля M. Покажите, что:

а) $M = A \oplus B$ в точности тогда, когда подмодуль B является одновременно а.д. и д.п. для A;

б) а.д. определено не всегда;

в) д.п. определено для любого подмодуля A, причем, если $A \cap B = 0$, то существует д.п. C для A, содержащее подмодуль B.

15.90. 1) Пусть $M = A + B$. Тогда B — а.д. для A в M в точности тогда, когда $A \cap B$ — малый подмодуль в B.

2) Если $A^\bullet$ — а.д. для A в M и $A^{\bullet\bullet}$ — а.д. для $A^\bullet$ в M, то $A^\bullet$ — также а.д. для $A^{\bullet\bullet}$ в M.

3) Если $A^\bullet$ — а.д. для A в M и $A^{\bullet\bullet}$ — а.д. для $A^\bullet$ в M, причем $A^{\bullet\bullet} \subseteq A$, то подмодуль $A/A^{\bullet\bullet}$ мал в $M/A^{\bullet\bullet}$.

15.91. 1) Если A и B — подмодули модуля M со свойством $A \cap B = 0$, то B — д.п. для A в M в точности тогда, когда $(A + B)/B$ — существенный подмодуль в M/B.

2) Если C — д.п. для A в M и D — д.п. для C в M, то C — также д.п. для D в M.

3) Если C — д.п. для A в M и D — д.п. для C в M, для которого $A \subseteq D$, то A — существенный подмодуль в D.

Множество $\operatorname{sing} M = \{m \in M \mid r(m)$ — существенный подмодуль в $R_R\}$ определяет подмодуль модуля M_R, $\operatorname{sing} M$ называется *сингулярным подмодулем* модуля M.

15.92. 1) $\operatorname{sing} M$ — вполне инвариантный подмодуль модуля M.

2) $\operatorname{sing} R$ — идеал кольца R.

15.93. $\operatorname{End}_R M$ — нормальное кольцо в точности тогда, когда каждое прямое слагаемое модуля M является его вполне инвариантным подмодулем.

16 Локальные, нетеровы и артиновы модули

Модуль M_R называется *локальным* при выполнении следующих равносильных условий:

1) M конечно порожден и имеет единственный максимальный подмодуль;

2) $M/J(M)$ — простой модуль и $J(M)$ — малый подмодуль в M;

3) $M \neq J(M)$ и $M = mR$ для любого $m \in M \backslash J(M)$.

Напомним, что согласно § 13, кольцо R локально, если локален модуль R_R, это эквивалентно локальности модуля ${}_RR$.

Теорема 16.1 (Крулля-Шмидта). *Если $M_R = \bigoplus\limits_{i\in I} M_i$, причем кольца $\operatorname{End} M_i$ локальны для всех $i \in I$, и $M_R = \bigoplus\limits_{j\in J} N_j$, где N_j — неразложимые ненулевые модули, то существует биекция $\alpha\colon I \to J$ такая, что $M_i \cong N_{\alpha(i)}$ для всех $i \in I$.*

Модуль M называется *артиновым*, если M не имеет бесконечных строго убывающих цепей подмодулей, это равносильно тому, что каждое непустое множество его подмодулей содержит минимальный (по включению) элемент.

Модуль M называется *нетеровым*, если M не имеет бесконечных строго возрастающих цепей подмодулей, это равносильно тому, что каждое непустое множество его подмодулей содержит максимальный элемент.

Ясно, что кольцо R нетерово справа, соответственно, артиново справа, если модуль R_R нетеров, соответственно, артинов (см. § 13). Нетеровость (артиновость) справа кольца не влечет соответствующее левое свойство этого кольца и наоборот.

Теорема 16.2 (Гильберта о базисе). *Если кольцо R нетерово справа, то кольцо многочленов $R[x]$ также нетерово справа.*

Цепи подмодулей $0 = A_0 \subset A_1 \subset \ldots \subset A_k = M$ и $0 = B_0 \subset B_1 \subset \ldots \subset B_n = M$ модуля M называются *изоморфными*, если $k = n$ и существует перестановка δ на $I = \{1, \ldots, k\}$ такая, что $A_i/A_{i-1} \cong B_{\delta(i)}/B_{\delta(i)-1}$, $i \in I$. Вторая цепь называется *уплотнением* первой, если первая получается из второй удалением некоторых B_j. Цепь $0 = A_0 \subset A_1 \subset \ldots \subset A_k = M$ называется *композиционным рядом*, если каждый подмодуль A_{i-1} максимален в A_i. Модуль M называется *модулем конечной длины*, если $M = 0$ или он обладает композиционным рядом.

Теорема 16.3 (Жордана-Гельдера-Шрайера). *Любые две конечные цепи данного модуля имеют изоморфные уплотнения.*

Модуль M называется *конечно копорожденным*, если в каждом множестве $\{A_i \mid i \in I\}$ его подмодулей, удовлетворяющем условию $\bigcap\limits_{i\in I} A_i = 0$, существует такое конечное подмножество $J \subseteq I$, что $\bigcap\limits_{j\in J} A_j = 0$.

Теорема 16.4 (Веддерберна-Артина). *Для кольца R равносильны следующие условия:*

а) R — артиново справа полупервичное кольцо;

б) R — полупервичное кольцо с условием минимальности для главных правых идеалов;

в) R — полупервичное кольцо с условием максимальности для главных правых идеалов вида eR, $e = e^2$, и $\operatorname{Soc} R_R$ — существенный правый идеал;

г) R — полупримитивное артиново справа кольцо;

д) R — полупростое справа кольцо (т.е. R — классически полупростое кольцо, см. 15.63);

е) все правые R-модули являются полупростыми;

ж) каждый максимальный правый идеал кольца R является прямым слагаемым модуля R_R;

з) R — конечное прямое произведение простых артиновых колец;

и) R изоморфно конечному прямому произведению колец матриц над телами.

Задачи

16.1. Если кольцо $S = \operatorname{End}_R M$ локально, то модуль M_R неразложим.

16.2. Для кольца R равносильны следующие условия:

а) R — локальное кольцо;

б) $R/J(R)$ — тело;

в) ${}_RR$ — локальный модуль;

г) R_R — локальный модуль;

д) $R = aR$ для любого $a \in R\backslash J(R)$;

е) $R = Ra$ для любого $a \in R\backslash J(R)$;

ж) $J(R)$ совпадает с множеством всех необратимых элементов кольца R;

з) для любых таких $a, b \in R$, что $a + b = 1$, хотя бы один из элементов a, b обратим в кольце R.

16.3. Пусть R — локальное кольцо. Тогда:

а) каждый циклический R-модуль является локальным;

б) все факторкольца кольца R являются локальными;

в) все простые правые R-модули изоморфны модулю $(R/J(R))_R$.

16.4. Если M — артинов или полупростой модуль, то каждый его подмодуль обладает аддитивным дополнением.

16.5. Пусть M — модуль и A — его подмодуль. Следующие условия эквивалентны:

а) M артинов;

б) A и M/A — артиновы модули;

в) каждый фактормодуль модуля M конечно копорожден;

г) для каждого непустого множества $\{A_i \mid i \in I\}$ подмодулей модуля M существует конечное подмножество $J \subseteq I$ с условием $\bigcap\limits_{i\in I} A_i = \bigcap\limits_{j\in J} A_j$.

16.6. Пусть M — модуль и A — его подмодуль. Следующие условия эквивалентны:

а) M нетеров;

б) A и M/A — нетеровы модули;

в) каждый подмодуль модуля M конечно порожден;

г) для каждого непустого множества $\{A_i \mid i \in I\}$ подмодулей модуля M существует конечное подмножество $J \subseteq I$ с условием $\sum\limits_{i\in I} A_i = \sum\limits_{j\in J} A_j$.

16.7. Модуль M артинов и нетеров в точности тогда, когда M — модуль конечной длины.

Идемпотент e кольца R называется *локальным*, если eRe — локальное кольцо.

16.8. Пусть R — кольцо и $\sum\limits_{i=1}^{m} e_i = 1 = \sum\limits_{j=1}^{n} f_j$ — два представления 1 в виде суммы ортогонального множества локальных идемпотентов. Тогда $m = n$ и существует обратимый элемент v кольца R и перестановка $s \in S_n$ такая, что $ve_i = f_{s(i)}v$ $(i = 1, \ldots, n)$.

16.9. Пусть M — ненулевой модуль. Тогда:

а) если M — цепной модуль, то M — модуль Безу;

б) если M — конечно порожденный цепной модуль, то M — циклический локальный модуль Безу;

в) M обладает простым подфактором;

г) если M не является цепным модулем, то M обладает подфактором $S \oplus T$, где S и T — простые модули.

16.10. Пусть все подфакторы модуля M изоморфны. Тогда M — дистрибутивный модуль в точности тогда, когда M — цепной модуль.

16.11. Для модуля M_R над локальным кольцом R равносильны следующие условия:

а) M — дистрибутивный модуль;

б) M — модуль Безу;

в) M — цепной модуль.

16.12. Для модуля M равносильны следующие условия:

а) каждый ненулевой фактормодуль модуля M содержит простой подмодуль;

б) каждый ненулевой подфактор модуля M является существенным расширением полупростого модуля.

Модуль M, удовлетворяющий равносильным условиям а), б) упр. 16.12 называется *полуартиновым.*

16.13. Для модуля M равносильны следующие условия:

а) M — артинов модуль;

б) все подфакторы модуля M являются артиновыми;

в) M — конечная прямая сумма артиновых модулей;

г) существует такая цепь $0 = A_0 \subset A_1 \subset \ldots \subset A_k = M$ подмодулей модуля M, что все модули A_i/A_{i-1} являются артиновыми;

д) M — полуартинов конечномерный модуль.

Покажите, что справедливы условия а) – г) с заменой условия артиновости на нетеровость.

Модуль M называется *полунетеровым*, если каждый ненулевой подфактор модуля M обладает максимальным подмодулем.

16.14. 1) Каждый нетеров модуль является полунетеровым.

2) M — вполне циклический модуль в точности тогда, когда M — нетеров модуль Безу.

3) Каждый полунетеров артинов модуль является нетеровым модулем.

4) Условие для модуля M быть цепным нетеровым модулем равносильно как тому, что M — вполне циклический модуль, так и тому, что M — цепной модуль с условием максимальности для циклических подмодулей.

5) M — цепной артинов модуль в точности тогда, когда M — цепной модуль с условием минимальности для циклических подмодулей.

16.15. Конечное прямое произведение нетеровых (артиновых) справа колец является нетеровым (артиновым) справа кольцом.

16.16. Если R содержит в качестве подкольца тело D и R как правое векторное D-пространство конечномерно, то R — артиново справа кольцо.

16.17. Если кольцо R — нетерово (артиново) справа, то нетеров (артинов) любой конечно порожденный правый R-модуль M.

16.18. Пусть f — эндоморфизм модуля M. Покажите, что:

а) если M артинов, то существует $m \in \mathbb{N}$ такое, что $M = \operatorname{Im} f^n + \operatorname{Ker} f^n$ для любого $n \geqslant m$, в частности, если f — мономорфизм, то f является автоморфизмом;

б) если M нетеров, то существует $m \in \mathbb{N}$ такое, что $\operatorname{Im} f^n \cap \operatorname{Ker} f^n = 0$ для любого $n \geqslant m$, в частности, если f — эпиморфизм, то f является автоморфизмом;

в) если M — модуль конечной длины, то существует $m \in \mathbb{N}$ такое, что $M = \operatorname{Im} f^n \oplus \operatorname{Ker} f^n$ для любого $n \geqslant m$, в частности, условие для f быть автоморфизмом равносильно как тому, что f — эпиморфизм, так и тому, что f — мономорфизм.

16.19. Модуль удовлетворяет условию максимальности для прямых слагаемых тогда и только тогда, когда он удовлетворяет условию минимальности для прямых слагаемых.

16.20. Если M_R — ненулевой неразложимый модуль конечной длины, то кольцо $S = \operatorname{End}_R M$ локально и его необратимые элементы являются нильпотентными.

16.21. Пусть $M_R \neq 0$. Покажите, что:

а) если модуль M артинов или нетеров, то у него существуют такие неразложимые подмодули $M_1, \ldots, M_n$, что $M = \bigoplus\limits_{i=1}^{n} M_i$;

б) если M — модуль конечной длины, то $M = \bigoplus\limits_{i=1}^{n} M_i$, где каждое кольцо $\operatorname{End}_R M_i$ $(i = 1, \ldots, n)$ локально.

16.22. Приведите пример модуля M, не являющегося модулем конечной длины такого, что для каждого $f \in \operatorname{End}_R M$ существует $m \in \mathbb{N}$ со свойством $M = \operatorname{Im} f^n \oplus \operatorname{Ker} f^n$ при $n \geqslant m$.

16.23. Ненулевой артинов модуль обладает неразложимым в сумму фактормодулем (модуль M называется *неразложимым в сумму*, если сумма любых двух его собственных подмодулей — снова собственный подмодуль в M).

16.24. Кольцо $M(n, R)$ артиново (нетерово) справа в точности тогда, когда R артиново (нетерово) справа.

16.25. Если R — кольцо главных идеалов без делителей нуля и A — ненулевой правый идеал в R, то модуль $(R/A)_R$ артинов.

16.26. Для нетеровости модуля достаточно, чтобы он удовлетворял условию максимальности для конечно порожденных подмодулей.

16.27. Приведите пример не нетерова модуля, удовлетворяющего условию максимальности для циклических подмодулей.

Подмодуль N модуля M называется *неразложимым относительно пересечения*, если для любых подмодулей $A, B \subseteq M$ из условия $N = A \cap B$ следует, что либо $A = N$, либо $B = N$.

16.28. Каждый подмодуль нетерова модуля M является пересечением конечного числа неразложимых относительно пересечения подмодулей модуля M.

16.29. Пусть R — нетерово справа кольцо. Докажите, что:

а) его первичный радикал является наибольшим нильпотентным правым идеалом и наибольшим левым ниль-идеалом;

б) всякий его ниль-идеал (правый или левый) нильпотентен (см. 13.84).

16.30. 1) Если M — артинов модуль, то для любого его подфактора N модуль $N/J(N)$ является конечной прямой суммой простых модулей.

2) M — артинов полупримитивный модуль в точности тогда, когда M — конечная прямая сумма простых модулей.

16.31. 1) Если кольцо R артиново справа, то $J(R)$ — наибольший нильпотентный правый (соответственно, левый) идеал, в частности, $J(R) = \operatorname{rad} R$ и $R/J(R)$ — классически полупростое кольцо.

2) Если кольцо R артиново справа, то для каждого правого модуля M_R (соответственно, левого модуля ${}_R M$) имеет место равенство $J(M) = MJ(R)$ (соответственно, $J(M) = J(R)M$), причем $J(M)$ является малым подмодулем в M.

16.32. Пусть кольцо $R/J(R)$ классически полупросто и радикал $J(R)$ нильпотентен. Для модуля M_R следующие условия эквивалентны:

а) M_R артинов;

б) M_R нетеров;

в) M_R имеет конечную длину.

16.33. Пусть кольцо R артиново справа. Покажите, что:

а) если модуль M_R артинов (соответственно, нетеров), то он также нетеров (соответственно, артинов);

б) кольцо R нетерово справа;

в) если R нетерово слева, то оно артиново слева.

16.34. Модуль M_R конечно порожден тогда и только тогда, когда конечно порожден модуль $M/J(M)$, причем $J(M)$ — малый подмодуль в M.

16.35. Модуль M нетеров тогда и только тогда, когда для любого подмодуля N в M подмодуль $J(N)$ мал в N и модуль $N/J(N)$ конечно порожден.

16.36. Ненулевой модуль M конечно копорожден тогда и только тогда, когда $\operatorname{Soc} M$ — конечно копорожденный существенный подмодуль в M.

16.37. Модуль M артинов тогда и только тогда, когда для любого фактормодуля M/U его цоколь $\operatorname{Soc}(M/U)$ является конечно копорожденным существенным подмодулем в M/U.

17 Проективные и инъективные модули

Модуль M называется *проективным относительно модуля* N (или N-*проективным*), если для каждого эпиморфизма $h\colon N \to L$ и для любого гомоморфизма $f\colon M \to L$ существует такой гомоморфизм $g\colon M \to N$, что $f = hg$.

Модуль, проективный относительно себя, называется *квазипроективным* (или *самопроективным*) модулем.

Прямые слагаемые свободных модулей называются *проективными* модулями.

Теорема 17.1. *Для модуля M_R равносильны следующие условия:*

а) *M — проективный модуль;*

б) *M проективен относительно любого R-модуля N_R;*

в) *любой эпиморфизм $N_R \to M_R$ расщепляется.*

Модуль M называется *наследственным* (*полунаследственным*, *риккартовым*), если все подмодули (все конечно порожденные подмодули, все циклические подмодули) модуля M проективны. Кольцо называется *наследственным справа* (*слева*), если все его правые (левые) идеалы проективны.

Теорема 17.2 (Капланский). 1) *Пусть M — модуль, причем $M = P \oplus Q = \bigoplus\limits_{i\in I} M_i$, где модули M_i являются счетно порожденными для всех $i \in I$. Тогда P — прямая сумма счетно порожденных модулей.*

2) *Каждое прямое слагаемое прямой суммы конечно порожденных модулей является прямой суммой счетно порожденных модулей.*

3) *Каждый проективный модуль является прямой суммой счетно порожденных модулей.*

Модуль M называется *инъективным относительно модуля* N (или N-*инъективным*), если для любого подмодуля $A \subseteq N$ все гомоморфизмы $A \to M$ продолжаются до гомоморфизмов $N \to M$.

Модуль M называется *инъективным*, если для любого модуля N модуль M является N-*инъективным*. Модуль M называется *квазиинъективным* (или *самоинъективным*), если M — M-инъективный модуль.

Теорема 17.3 (Критерий Бэра). *Для правого модуля M над кольцом R равносильны следующие условия:*

1) *M — инъективный модуль;*

2) *M инъективен относительно свободного циклического модуля R_R;*

3) *для каждого правого идеала I кольца R и каждого гомоморфизма $f\colon I \to M$ существует такой $m \in M$, что $f(x) = mx$ для всех $x \in I$;*

4) *M инъективен относительно некоторого конечно точного модуля H;*

5) *каждый гомоморфизм $A \to M$, где A — существенный правый идеал кольца R, продолжается до гомоморфизма $R_R \to M$.*

Модуль M_R над кольцом R называется *конечно инъективным*, если любой гомоморфизм $A \to M$, где A — произвольный конечно порожденный правый идеал кольца R, продолжается до гомоморфизма $R_R \to M$.

Модуль M_R называется *p-инъективным*, если для любого $a \in R$ каждый гомоморфизм $f\colon aR \to M$ продолжается до некоторого гомоморфизма $R_R \to M$.

Теорема 17.4. 1) *Фактормодуль $\mathbb{Q}/\mathbb{Z}$ является инъективным кообразующим над кольцом $\mathbb{Z}$.*

2) *Естественно определенный модуль $T_R = \operatorname{Hom}(R_{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})_{\mathbb{Z}})$ является правым инъективным кообразующим над кольцом R.*

Подмодуль H модуля M называется *замкнутым* в M, если H не имеет собственных существенных расширений в M. Если $N, H \in L(M)$, H — замкнутый подмодуль в M и N является существенным подмодулем в H, то H называется *замыканием* модуля N в M.

Модуль M называется *непрерывным*, если каждый его подмодуль, изоморфный замкнутому подмодулю (модуля M), является прямым слагаемым модуля M.

Модуль M называется *π-инъективным* или *квазинепрерывным*, если каждый идемпотентный эндоморфизм любого подмодуля модуля M продолжается до эндоморфизма модуля M.

Модуль M называется *малоинъективным*, если каждый эндоморфизм любого подмодуля модуля M продолжается до эндоморфизма модуля M.

Пусть $\overline{M}$ — фактормодуль модуля M, $h\colon M \to \overline{M}$ — канонический эпиморфизм и $\overline{f} \in \operatorname{End}_R \overline{M}$. Если существует такой $f \in \operatorname{End}_R M$, что $\overline{f}h = hf$, т.е. коммутативна диаграмма

$$\begin{array}{ccc} \overline{M} & \xrightarrow{\overline{f}} & \overline{M} \\ h\uparrow & & h\uparrow \\ M & \xrightarrow{f} & M, \end{array}$$

то говорят, что $\overline{f}$ *поднимается* до эндоморфизма $f \in \operatorname{End}_R M$.

Модуль M называется *π-проективным*, если каждый идемпотентный эндоморфизм любого фактормодуля модуля M поднимается до эндоморфизма модуля M.

Модуль M называется *малопроективным*, если для любого эпиморфизма $h\colon M \to N$ и каждого эндоморфизма g модуля N существует такой эндоморфизм f модуля M, что $gh = hf$.

Проективным накрытием модуля M называется любой такой эпиморфизм $f\colon P \to M$, что P — проективный модуль и $\operatorname{Ker} f$ — малый подмодуль в P. Модуль P называется *проективной оболочкой* модуля M. Иногда M и $P/\operatorname{Ker} f$ отождествляют. Проективная оболочка определена не для всякого модуля (см. упр. 17.2 и теорему 18.2).

Любой инъективный модуль, являющийся существенным расширением модуля M, называется его *инъективной оболочкой*.

Задачи

17.1. Пусть M_R — R-модуль. Модуль M^n содержит свободный циклический подмодуль (т.е. M является конечно точным) в точности тогда, когда существуют такие элементы $m_1, \ldots, m_n \in M$, что $r(\{m_1, \ldots, m_n\}) = 0$.

17.2. Несвободный $\mathbb{Z}$-модуль не имеет проективной оболочки.

17.3. *Проективной резольвентой* модуля M называется точная последовательность

$$\ldots \to P_n \to \ldots \to P_1 \to P_0 \to M \to 0,$$

где все P_i — проективные модули.

Каждый модуль обладает проективной резольвентой.

17.4. 1) Пусть N — модуль, $\mathcal{E}$ — класс всех N-проективных модулей. Тогда все прямые слагаемые и все прямые суммы модулей из $\mathcal{E}$ принадлежат $\mathcal{E}$.

2) Пусть M — модуль, $\mathcal{E}$ — класс всех таких модулей N, что M — N-проективный модуль. Тогда все гомоморфные образы, подмодули и конечные прямые суммы модулей из $\mathcal{E}$ принадлежат $\mathcal{E}$.

3) Пусть N — модуль, M — N-проективный модуль, причем существует эпиморфизм $h\colon N \to M$. Тогда h расщепляется, M — квазипроективный модуль, изоморфный прямому слагаемому модуля N. В частности, если N — неразложимый модуль, то h — изоморфизм.

4) Все прямые суммы и прямые слагаемые проективных модулей проективны.

17.5. Циклическая группа простого порядка является квазипроективным простым непроективным модулем над кольцом $\mathbb{Z}$.

17.6. Для кольца R равносильны следующие условия:

а) R — классически полупростое кольцо;

б) каждый правый R-модуль является проективным;

в) каждый простой правый R-модуль проективен относительно модуля R_R.

17.7 (Лемма о дуальном базисе). Для модуля M_R равносильны следующие условия:

а) M — проективный модуль;

б) существуют система образующих $\{m_i\}_{i\in I}$ модуля M и множество $\{f_i\}_{i\in I}$ гомоморфизмов $f_i\colon M_R \to R_R$ такие, что для любого $m \in M$ имеет место равенство $m = \sum\limits_{i\in I} m_i f_i(m)$ ($f_i(m) = 0$ для почти всех индексов i);

в) для любой системы образующих $\{m_i\}_{i\in I}$ модуля M существует множество $\{f_i\}_{i\in I}$ гомоморфизмов $f_i\colon M_R \to R_R$ таких, что для любого $m \in M$ имеет место равенство $m = \sum\limits_{i\in I} m_i f_i(m)$ ($f_i(m) = 0$ для почти всех индексов i).

17.8. Пусть $h_1\colon P_1 \to M_1$ и $h_2\colon P_2 \to M_2$ — модульные эпиморфизмы с ядрами Q_1 и Q_2 соответственно. Тогда если P_1 и P_2 — проективные модули, а $M_1 \cong M_2$, то $P_1 \oplus Q_2 \cong P_2 \oplus Q_1$.

17.9. 1) Пусть $f\colon P \to M$ — проективное накрытие модуля M, $g\colon Q \to M$ — эпиморфизм, где Q — проективный модуль. Тогда существует такой расщепляющийся эпиморфизм $h\colon Q \to P$, что $g = fh$, $Q = \operatorname{Ker} h \oplus \overline{P}$, причем ограничение гомоморфизма h на $\overline{P}$ является изоморфизмом $\overline{P}$ на P.

2) Пусть $f_1\colon P_1 \to M$ и $f_2\colon P_2 \to M$ — два проективных накрытия модуля M. Тогда существует такой изоморфизм $h\colon P_2 \to P_1$, что $f_2 = f_1 h$ и $f_1 = f_2 h^{-1}$. В частности, любые две проективные оболочки модуля M изоморфны.

17.10. 1) Пусть модуль M_R проективен относительно конечно точного модуля N. Тогда M проективен относительно любого конечно порожденного правого R-модуля. Кроме того, если M конечно порожден, то M — проективный модуль.

2) Каждый конечно порожденный конечно точный квазипроективный модуль является проективным.

17.11. Пусть $R = M(2, P)$, где P — поле. Матрицы вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, где $a, b \in P$, образуют правый идеал M кольца R. Покажите, что M_R — проективный, но не свободный модуль.

17.12. 1) Пусть $M_R = \bigoplus\limits_{i \in I} M_i$, причем для каждого $i \in I$ модуль M_i и все его подмодули проективны. Тогда любой подмодуль N модуля M изоморфен прямой сумме $\bigoplus\limits_{i \in I} N_i$, где $N_i \subseteq M_i$ для всех $i \in I$.

2) Если R — коммутативная область главных идеалов, то каждый подмодуль свободного модуля является свободным. В частности, каждый проективный $\mathbb{Z}$-модуль свободен.

17.13. Каждый подмодуль свободного правого модуля над наследственным справа кольцом изоморфен прямой сумме правых идеалов кольца R.

17.14. Кольцо $R \subset M(2, \mathbb{Q})$ всех матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, где $c \in \mathbb{Z}$, а $a, b \in \mathbb{Q}$, наследственно слева, но не справа.

17.15. 1) Если N — модуль, то прямые слагаемые и прямые произведения N-инъективных модулей являются N-инъективными модулями.

2) Прямые слагаемые и прямые произведения инъективных модулей являются инъективными модулями.

17.16. Пусть M — модуль, $\mathcal{E}$ — класс всех таких модулей N, что M — N-инъективный модуль. Тогда все гомоморфные образы, подмодули и прямые суммы модулей из $\mathcal{E}$ принадлежат $\mathcal{E}$.

17.17. Пусть $M = \bigoplus\limits_{i=1}^{n} M_i$. Модуль M квазиинъективен в точности тогда, когда M_i — M_j-инъективный модуль для всех i и j.

17.18. Конечная прямая сумма изоморфных квазиинъективных модулей является квазиинъективным модулем.

17.19. Пусть N — модуль, M — ненулевой N-инъективный модуль, $f\colon M \to N$ — мономорфизм. Тогда $f(M)$ — прямое слагаемое модуля N, M — квазиинъективный модуль и M изоморфен прямому слагаемому модуля N. В частности, если N — неразложимый модуль, то f — изоморфизм.

17.20. Пусть M_R — модуль над кольцом R.

1) Любой инъективный модуль является квазиинъективным и конечно инъективным модулем. Каждый конечно инъективный модуль является p-инъективным.

2) Если R — кольцо главных правых идеалов, то M — p-инъективный модуль тогда и только тогда, когда M — инъективный модуль.

3) M — p-инъективный модуль тогда и только тогда, когда для любых таких $x \in M$ и $a \in R$, что $r(a) \subseteq r(x)$, существует $m \in M$ со свойством $x = ma$.

4) Если M — p-инъективный модуль и a — регулярный справа (т.е $r(a) = 0$) элемент кольца R, то $M = Ma$.

5) Если R — коммутативная область, то M — p-инъективный модуль тогда и только тогда, когда $M = Ma$ для всех ненулевых $a \in R$.

6) Если R — область главных правых идеалов, то M — инъективный модуль тогда и только тогда, когда $M = Ma$ для всех ненулевых $a \in R$.

7) Если $M = \mathbb{Z}_p$ — циклическая группа простого порядка p, то M — квазиинъективный простой $\mathbb{Z}$-модуль, не являющийся p-инъективным.

17.21. Пусть R — коммутативная область. Тогда для R следующие два условия эквивалентны:

а) каждый идеал проективен;

б) каждый делимый R-модуль инъективен (если R — область, то R-модуль M называется *делимым*, если $rM = M$ для каждого ненулевого элемента $r \in R$; в случае произвольного кольца R условие $rM = M$ должно выполняться для каждого r, не являющегося делителем нуля в R).

Коммутативная область со свойствами а), б) называется *дедекиндовой*. В частности, коммутативная область главных идеалов является дедекиндовым кольцом.

17.22. 1) T_R — кообразующий модуль в точности тогда, когда каждый R-модуль M изоморфен подмодулю прямого произведения изоморфных копий модуля T.

2) Если T_R — инъективный модуль, то равносильны следующие условия:

а) T — кообразующий;

б) каждый простой правый R-модуль изоморфен подмодулю модуля T;

в) T содержит прямую сумму представителей всех классов изоморфных простых правых R-модулей.

17.23. 1) M — инъективный модуль тогда и только тогда, когда для любого модуля N и любого мономорфизма $f\colon M \to N$ модуль $f(M)$ является прямым слагаемым модуля N.

2) Если модуль M_R проективен относительно всех инъективных R-модулей, то M — проективный модуль.

17.24. 1) Каждое прямое слагаемое модуля M является замкнутым подмодулем в M.

2) Каждый подмодуль N модуля M обладает замыканием в M.

3) Если $G, N \in L(M)$ и $G \cap N = 0$, то G обладает в M хотя бы одним замкнутым дополнением, содержащим N.

4) Каждый подмодуль G модуля M обладает в M хотя бы одним замкнутым дополнением.

5) Если $N_1, N_2 \in L(M)$ и $N_1 \cap N_2 = 0$, то существуют такие замкнутые подмодули M_1, M_2 модуля M, что $N_1 \subseteq M_1$, $N_2 \subseteq M_2$, $M_1 \cap M_2 = 0$, $M_1 \oplus M_2$ — существенный подмодуль в M и $M_1 \cap K \neq 0$ для любого подмодуля K модуля M, строго содержащего M_2.

6) Если G — замыкание подмодуля $N \in L(M)$, H — дополнение к N в модуле M, то G — дополнение H в M и H — замкнутый подмодуль модуля M.

7) Множество замкнутых подмодулей модуля M совпадает с множеством всех дополнительных подмодулей модуля M.

17.25. Для модуля M равносильны следующие условия:

а) M — π-инъективный модуль;

б) каждый идемпотентный эндоморфизм любого подмодуля модуля M продолжается до идемпотентного эндоморфизма модуля M;

в) для любых подмодулей $N_1, N_2 \in L(M)$ со свойством $N_1 \cap N_2 = 0$ существует такое прямое разложение $M = M_1 \oplus M_2$, что $N_1 \subseteq M_1$, $N_2 \subseteq M_2$;

г) $M = Q_1 \oplus Q_2$ для любых таких замкнутых подмодулей Q_1 и Q_2 модуля M, что $Q_1 \cap Q_2 = 0$ и M — существенное расширение модуля $Q_1 \oplus Q_2$.

17.26. 1) Все малоинъективные модули являются π-инъективными.

2) M — равномерный модуль в точности тогда, когда M — неразложимый π-инъективный модуль.

3) Все прямые слагаемые и вполне инвариантные подмодули квазиинъективных (малоинъективных, π-инъективных) модулей являются квазиинъективными (малоинъективными, π-инъективными).

4) Все квазиинъективные модули малоинъективны.

5) Кольцо целых чисел $\mathbb{Z}$ является малоинъективным $\mathbb{Z}$-модулем, который не является p-инъективным.

6) Каждый подмодуль π-инъективного модуля M является существенным подмодулем некоторого прямого слагаемого модуля M. В частности, каждый замкнутый подмодуль π-инъективного модуля M является его прямым слагаемым.

17.27. 1) Каждый модуль обладает хотя бы одной инъективной оболочкой.

2) Каждый инъективный модуль, содержащий модуль M, содержит хотя бы одну инъективную оболочку модуля M.

3) Если E_1 и E_2 — две инъективные оболочки модуля M, то существует изоморфизм $f\colon E_1 \to E_2$, действующий тождественно на M.

17.28. Пусть $M = \bigoplus\limits_{i=1}^{n} M_i$. Тогда:

а) M — квазиинъективный модуль, если и только если M — π-инъективный модуль и M_i — квазиинъективные модули для всех $i = 1, \ldots, n$;

б) M — квазипроективный модуль, если и только если M_i — M_j-проективный модуль для всех i и j;

в) если все M_i — изоморфные квазипроективные модули, то M — квазипроективный модуль.

17.29. Пусть $M = \mathbb{Z}_2$, $N = \mathbb{Z}_4$. Тогда M и N — квазиинъективные модули над $\mathbb{Z}$. Однако $M \oplus N$ не является ни π-инъективным, ни малоинъективным, ни квазиинъективным $\mathbb{Z}$-модулем.

17.30. 1) Все прямые слагаемые квазипроективных (малопроективных, π-проективных) модулей являются квазипроективными (малопроективными, π-проективными) модулями.

2) M — малопроективный модуль в точности тогда, когда каждый эндоморфизм любого фактормодуля модуля M поднимается до эндоморфизма модуля M. В частности, все малопроективные модули являются π-проективными.

3) Каждый строго неразложимый модуль является π-проективным.

4) M — строго неразложимый модуль в точности тогда, когда все собственные подмодули модуля M являются его малыми подмодулями.

5) Каждый квазипроективный модуль является малопроективным.

17.31. Если $0 \neq e \neq 1$ — некоторый центральный идемпотент кольца R, то eR — проективный, но не свободный правый R-модуль.

17.32. Пусть $M = \bigoplus\limits_{i=1}^{n} M_i$. Тогда M — квазипроективный модуль, если и только если M_i — квазипроективные модули для всех $i = 1, \ldots, n$.

17.33. Пусть $M = \mathbb{Z}_2$, $N = \mathbb{Z}_4$. Тогда M и N являются неразложимыми квазипроективными модулями над кольцом $\mathbb{Z}$. Покажите, что $M \oplus N$ не является ни π-проективным, ни малопроективным, ни квазипроективным $\mathbb{Z}$-модулем.

17.34. Для кольца R равносильны следующие условия:

а) R — наследственное справа кольцо;

б) все подмодули проективных правых R-модулей являются проективными;

в) все подмодули проективных правых R-модулей являются π-проективными;

г) все фактормодули инъективных правых R-модулей являются инъективными модулями;

д) все фактормодули инъективных правых R-модулей являются π-инъективными модулями.

17.35. Для кольца R равносильны следующие условия:

а) R — нетерово справа кольцо;

б) все прямые суммы инъективных правых R-модулей являются инъективными модулями;

в) все счетные прямые суммы инъективных правых R-модулей являются инъективными модулями;

г) все счетные прямые суммы инъективных правых R-модулей являются π-инъективными модулями.

17.36. 1) Все гомоморфные образы прямых сумм инъективных правых модулей над наследственным справа нетеровым справа кольцом являются инъективными модулями.

2) Все гомоморфные образы прямых сумм инъективных правых модулей над областью главных правых идеалов являются инъективными модулями.

3) Все гомоморфные образы прямых сумм инъективных абелевых групп являются инъективными модулями над кольцом $\mathbb{Z}$.

17.37. Для кольца R равносильны следующие условия:

а) R — классически полупростое кольцо;

б) все правые R-модули являются π-инъективными;

в) все правые R-модули являются инъективными.

17.38. Пусть M — неразложимый квазипроективный R-модуль.

1) Если N — малый подмодуль в M и $\mathrm{End}_R M$ — локальное кольцо, то M/N — неразложимый модуль.

2) Если M конечно порожден и $\mathrm{End}_R M$ — локальное кольцо, то $M/J(M)$ — неразложимый модуль.

3) Если $M/J(M)$ — полупростой модуль и $J(M)$ — малый подмодуль в M, то равносильны следующие условия:

а) M — локальный модуль;

б) $\mathrm{End}_R M$ — локальное кольцо.

17.39. Если M_R — конечно инъективный модуль над полунаследственным справа кольцом R, то каждый гомоморфный образ модуля M является конечно инъективным.

17.40. Если M — правый модуль над кольцом R и B — такой правый идеал кольца R, что $B = r_R(X)$ для некоторого подмножества X модуля M, то B называется *правым M-аннулятором.*

Для инъективного модуля M_R равносильны следующие условия:

а) $\bigoplus\limits_{m} M$ — инъективный модуль для любого кардинала m;

б) $\bigoplus\limits_{\aleph_0} M$ — инъективный модуль;

в) R — кольцо с условием максимальности для правых M-аннуляторов.

17.41. Пусть $\{B_i\}_{i \in I}$ — множество всех правых идеалов кольца R, $N_i = R_R/B_i$, $N_R = \bigoplus\limits_{i \in I} N_i$, M — инъективная оболочка модуля N, t — мощность модуля M.

1) Каждый правый идеал кольца R является правым M-аннулятором.

2) Если R — кольцо с условием максимальности (минимальности) для правых M-аннуляторов, то R — нетерово справа (артиново справа) кольцо.

3) R — нетерово справа кольцо в точности тогда, когда $\bigoplus\limits_{\aleph_0} M$ — инъективный модуль.

4) Если P_R — любой модуль, являющийся расширением прямой суммы Q некоторых неизоморфных циклических модулей, то существует мономорфизм $f\colon P \to M$. Следовательно, мощность модуля P не превосходит t.

5) Мощность каждого неразложимого π-инъективного правого R-модуля P не превосходит t.

6) Мощность каждого дистрибутивного правого R-модуля P не превосходит t.

17.42. Для кольца R равносильны следующие условия:

а) R — нетерово справа кольцо;

б) $\bigoplus\limits_{\aleph_0} M$ является инъективным модулем для любого инъективного правого R-модуля M;

в) каждый инъективный правый R-модуль M является прямой суммой неразложимых модулей;

г) существует такое кардинальное число t, что каждый инъективный правый R-модуль является прямой суммой модулей, мощность которых не превосходит t.

17.43. Пусть Q_R — инъективный ненулевой модуль. Следующие условия эквивалентны:

а) Q неразложим;

б) Q является инъективной оболочкой любого своего ненулевого подмодуля;

в) каждый подмодуль в Q равномерен;

г) Q является инъективной оболочкой некоторого своего ненулевого равномерного подмодуля.

17.44. 1) Инъективная оболочка простого модуля неразложима.

2) Неразложимый инъективный модуль содержит не более одного простого подмодуля.

3) Если кольцо R артиново справа, то каждый ненулевой неразложимый инъективный правый R-модуль есть инъективная оболочка некоторого простого модуля.

17.45. Модуль $M \neq 0$ конечно копорожден тогда и только тогда, когда его инъективная оболочка $Q(M)$ представима в виде $Q(M) = Q_1 \oplus \ldots \oplus Q_n$, где каждое Q_i есть инъективная оболочка простого модуля.

17.46. Следующие условия эквивалентны:

а) модуль R_R артинов;

б) каждый инъективный модуль Q_R является прямой суммой инъективных оболочек простых R-модулей.

17.47. 1) Пусть модуль Q_R инъективен, $S = \operatorname{End}_R Q$ и $\alpha \in S$. Тогда малость подмодуля $S\alpha$ в ${}_S S$ равносильна как тому, что $\alpha \in J(S)$, так и тому, что $\operatorname{Ker}\alpha$ — существенный подмодуль в Q_R.

2) Пусть модуль P_R проективен, $S = \operatorname{End}_R P$ и $\alpha \in S$. Тогда малость подмодуля αS в S_S равносильна как тому, что $\alpha \in J(S)$, так и тому, что $\operatorname{Im}\alpha$ — малый подмодуль в P_R.

17.48. Пусть $0 \neq P$ — проективный модуль. Тогда $J(P) \neq P$. В частности, P содержит хотя бы один максимальный подмодуль.

17.49. Для всякого проективного модуля P имеет место равенство $J(P) = PJ(R)$.

17.50. Для модуля M равносильны следующие условия:

а) M — непрерывный модуль;

б) M — π-инъективный модуль и для любого его эндоморфизма f такого, что $\operatorname{Ker} f$ — замкнутый подмодуль в M, $\operatorname{Ker} f$ и $f(M)$ являются прямыми слагаемыми модуля M;

в) M — π-инъективный модуль и для любого его эндоморфизма f такого, что $\operatorname{Ker} f$ — прямое слагаемое модуля M, модуль $f(M)$ является прямым слагаемым модуля M.

17.51. Пусть E — инъективная оболочка модуля M. Равносильны следующие условия:

а) M — π-инъективный модуль;

б) для любого такого подмодуля N модуля M, что $N = \oplus_{i=1}^{k} N_i$, существует такое прямое разложение $M = \oplus_{i=1}^{k+1} M_i$, что M_i — существенное расширение модуля N_i для любых $i = 1, \ldots, k$;

в) для любых таких замкнутых подмодулей $N_1, \ldots, N_k$ модуля M, что сумма модулей N_i является прямой суммой, $\oplus_{i=1}^{k} N_i$ является прямым слагаемым модуля M;

г) для любых таких замкнутых подмодулей N_1, N_2 модуля M, что $N_1 \cap N_2 = 0$, $N_1 \oplus N_2$ — прямое слагаемое модуля M;

д) $f(M) \subseteq M$ для любой проекции f модуля E;

е) $M = \oplus_{i\in I}(M \cap E_i)$ для любого прямого разложения модуля $E = \oplus_{i\in I} E_i$.

17.52. Пусть E — инъективная оболочка модуля M. Равносильны следующие условия:

а) M — квазиинъективный модуль;

б) M непрерывный модуль и $f(M) \subseteq M$ для любого гомоморфизма $f\colon M \to E$;

в) M — вполне инвариантный подмодуль в E.

18 Тензорное произведение, плоские и регулярные модули

Пусть R — кольцо, A_R и ${}_RB$ — правый и левый R-модули соответственно, $A \times B$ — декартово произведение этих модулей. E — свободный $\mathbb{Z}$-модуль (т.е. абелева группа) с базисом $A \times B$; H — подмодуль модуля E (как $\mathbb{Z}$-модуля), порожденный всеми элементами вида

$$(a+a',b)-(a,b)-(a',b)\,,\ (a,b+b')-(a,b)-(a,b')\,,$$
$$(ar,b)-(a,rb)\,,\ \text{где } a,a'\in A,\ b,b'\in B,\ r\in R.$$

Тензорное произведение $A \otimes_R B$ — это $\mathbb{Z}$-модуль E/H. Пишут $A \otimes B$, если кольцо R фиксировано. Образ пары (a, b) при естественном эпиморфизме $E \to A \otimes B$ обозначается через $a \otimes b$. Каждый элемент $x \in A \otimes B$ может быть записан в виде конечной суммы вида $x = \sum a_i \otimes b_i$, определяемой, в общем случае, не однозначно.

Если ${}_SA_R$ и ${}_RB_T$ — бимодули, то группа $A \otimes_R B$ может естественным образом рассматриваться как S-T-бимодуль, если полагать $s(\sum a_i \otimes b_i) = \sum sa_i \otimes b_i$ и $(\sum a_i \otimes b_i)t = \sum a_i \otimes b_i t$ для любых $s \in S$, $t \in T$. В частности, $A \otimes_R R$ является правым R-модулем.

Отображение $f\colon A \times B \to G$ декартова произведения модулей A_R и ${}_RB$ в абелеву группу G называется *R-сбалансированным*, если

$$f(a+a',b)=f(a,b)+f(a',b)\,,\ f(a,b+b')=f(a,b)+f(a,b')\,,$$
$$f(ar,b)=f(a,rb)\ \text{для всех } a,a'\in A, b,b'\in B \text{ и } r\in R.$$

Теорема 18.1. *Пусть A_R и ${}_RB$ — модули над кольцом R, $\tau\ (a, b) = a \otimes b$. Тогда:*

1) *для каждого R-сбалансированного отображения $f\colon A \times B \to G$ существует единственный $\mathbb{Z}$-гомоморфизм $\lambda\colon A \otimes_R B \to G$ такой, что $f = \lambda\tau$, при этом $\lambda(\sum a_i \otimes b_i) = \sum f(a_i, b_i)$;*

2) *если $\gamma\colon A \times B \to C$ есть R-сбалансированное отображение такое, что существует $\mathbb{Z}$-гомоморфизм $\sigma\colon C \to A \otimes_R B$ со свойством $\tau = \sigma\gamma$, причем равенство $\gamma = \eta\gamma$, где $\eta \in \mathrm{Hom}_{\mathbb{Z}}(C, C)$, выполняется лишь для $\eta = 1_C$, то абелевы группы C и $A \otimes_R B$ изоморфны.*

Если даны R-модули A_R, ${}_RB$ и U_R, ${}_RV$ и R-гомоморфизмы $\alpha\colon A \to U$, $\mu\colon B \to V$, то отображение $\varphi\colon A \times B \ni (a, b) \mapsto \alpha(a) \otimes \mu(b) \in U \otimes_R V$ является R-сбалансированным. Отвечающий ему $\mathbb{Z}$-гомоморфизм $A \otimes_R B \to U \otimes_R V$ обозначают через $\alpha \otimes \mu$ и называют тензорным произведением гомоморфизмов α и μ. Тогда $(\alpha \otimes \mu)(\sum a_i \otimes b_i) = \sum \alpha(a_i) \otimes \mu(b_i)$.

Модуль ${}_RM$ называется *плоским*, если для каждого мономорфизма $\alpha\colon A_R \to B_R$ гомоморфизм $\alpha \otimes 1_M$ является мономорфизмом. Каждый проективный модуль является плоским (см. 18.20).

Теорема 18.2. *Для кольца R следующие условия эквивалентны:*

1) *каждый модуль M_R обладает проективной оболочкой;*

2) *каждый плоский правый R-модуль проективен;*

3) *R удовлетворяет условию обрыва убывающих цепей для главных левых идеалов;*

4) *каждый ненулевой левый R-модуль имеет ненулевой цоколь и ${}_RR$ удовлетворяет условию минимальности для прямых слагаемых;*

5) *кольцо $R/J(R)$ классически полупросто и для последовательности элементов $a_i \in J(R)$ существует такое $k \in \mathbb{N}$, что $a_k a_{k-1} \dots a_1 = 0$.*

Кольцо, удовлетворяющее условиям теоремы 18.2, называется *совершенным справа*. Согласно 5) каждое артиново справа или слева кольцо совершенно справа.

Категорией $\mathcal{E}$ называется класс *объектов* $A, B, C, \dots$ и *морфизмов* α, β, $\gamma, \dots$, удовлетворяющих следующим аксиомам:

1. С любой упорядоченной парой A, B объектов из $\mathcal{E}$ связано множество Мар (A, B) морфизмов из $\mathcal{E}$, причем так, что всякий морфизм из $\mathcal{E}$ принадлежит точно одному множеству Мар (A, B). Если $\alpha \in \mathcal{E}$ лежит в Мар (A, B), то пишут $\alpha\colon A \to B$ и называют α *отображением* объекта A в B.

2. С $\alpha \in$ Мар (A, B) и $\beta \in$ Мар (B, C) связан единственный элемент из Мар (A, C), называемый их *произведением* $\beta\alpha$.

3. Если произведения определены, то имеет место ассоциативность $\gamma(\beta\alpha) = (\gamma\beta)\alpha$.

4. Для каждого $A \in \mathcal{E}$ существует *единичный морфизм* $1_A \in$ Мар (A, A) объекта A такой, что $1_A\alpha = \alpha$ и $\beta 1_A = \beta$ всякий раз, когда эти произведения имеют смысл.

Ясно, что правые R-модули и их гомоморфизмы образуют *категорию $\mathcal{M}_R$ всех правых R-модулей*. Можно рассматривать категорию ${}_R\mathcal{M}$ всех левых R-модулей, бимодулей и т.п. Как о гомоморфизмах для алгебраических систем, можно говорить о функторах для категорий. Если $\mathcal{E}$ и $\mathcal{R}$ — категории, то *ковариантный функтор* $F\colon \mathcal{E} \to \mathcal{R}$

ставит в соответствие каждому объекту $A \in \mathcal{E}$ объект $F(A) \in \mathcal{R}$, а каждому морфизму $\alpha\colon A \to B$ в $\mathcal{E}$ — морфизм $F(\alpha) : F(A) \to F(B)$ в $\mathcal{R}$, причем так, что выполнены условия:

1) если имеет смысл произведение $\beta\alpha$, где $\alpha,\ \beta \in \mathcal{E}$, то $F(\beta)F(\alpha)$ определено в $\mathcal{R}$ и $F(\beta\alpha) = F(\beta)F(\alpha)$;

2) $F(1_A) = 1_{F(A)}$ для всех $A \in \mathcal{E}$.

Таким образом, ковариантный функтор сохраняет области определения, области значений, произведения и единицы. *Тождественный функтор* E, определяемый равенствами $E(A) = A$, $E(\alpha) = \alpha$ для всех $A,\ \alpha \in \mathcal{E}$, является ковариантным функтором из категории $\mathcal{E}$ в нее же.

Контравариантный функтор $G\colon \mathcal{E} \to \mathcal{R}$ определяется аналогично, но с обращением стрелок, т.е. G сопоставляет каждому объекту $A \in \mathcal{E}$ объект $G(A) \in \mathcal{R}$ и каждому морфизму $\alpha\colon A \to B$ из $\mathcal{E}$ морфизм $G(\alpha) : G(B) \to G(A)$ из $\mathcal{R}$, причем выполняются равенства $G(\beta\alpha) = G(\alpha)G(\beta)$, $G(1_A) = 1_{G(A)}$.

Просто термин «функтор» обычно обозначает ковариантный функтор.

Если $F\colon \mathcal{E} \to \mathcal{R}$ и $G\colon \mathcal{R} \to \mathcal{B}$ — функторы, то композиция GF — это функтор из $\mathcal{E}$ в $\mathcal{B}$, где $GF(A) = G(F(A))$ и $GF(\alpha) = G(F(\alpha))$ для всех $A,\ \alpha \in \mathcal{E}$.

Рассматривают функторы от нескольких аргументов, ковариантные по некоторым из этих аргументов и контравариантные по остальным. Если, например, $\mathcal{E}, \mathcal{R}, \mathcal{B}$ — категории, то *бифунктор* F из $\mathcal{E} \times \mathcal{R}$ в $\mathcal{B}$, ковариантный на $\mathcal{E}$ и контравариантный на $\mathcal{R}$, сопоставляет каждой паре $(C,\ D)$, где $C \in \mathcal{E}$, $D \in \mathcal{R}$, объект $F(C,\ D) \in \mathcal{B}$, а каждой паре морфизмов $\alpha\colon A \to C$, $\beta\colon B \to D$ $(\alpha \in \mathcal{E}, \beta \in \mathcal{R})$ — морфизм $F(\alpha,\ \beta)\colon F(A,\ D) \to F(C,\ B)$, причем $F(\gamma\alpha,\ \delta\beta) = F(\gamma,\ \beta)F(\alpha,\ \delta)$ и $F(1_C,\ 1_D) = 1_{F(C,\ D)}$, если только $\gamma\alpha$, $\delta\beta$ определены. Эти соотношения делают коммутативной диаграмму

$$\begin{array}{ccc} F(A,\ D) & \xrightarrow{F(\alpha,\ 1_D)} & F(C,\ D) \\ \downarrow{\scriptstyle F(1_A,\ \beta)} & & \downarrow{\scriptstyle F(1_C,\ \beta)} \\ F(A,\ B) & \xrightarrow{F(\alpha,\ 1_B)} & F(C,\ B)\,. \end{array}$$

Задачи

18.1. Покажите, что:

а) $(a + a') \otimes b = a \otimes b + a' \otimes b$; б) $a \otimes (b + b') = a \otimes b + a \otimes b'$;

в) $ar \otimes b = a \otimes rb$; г) $0 \otimes b = a \otimes 0 = 0$;

д) $-(a \otimes b) = (-a) \otimes b = a \otimes (-b)$;

е) $n(a \otimes b) = (na) \otimes b = a \otimes (nb)$, $n \in \mathbb{Z}$.

18.2. Если $A \subseteq B$ и $C \subseteq D$ — подмодули, то проверьте, что отображение $a \otimes c\ (\in A \otimes C) \mapsto a \otimes c\ (\in B \otimes D)$ индуцирует гомоморфизм $f\colon A \otimes C \to B \otimes D$. Приведите пример, когда f — не мономорфизм.

18.3. Если R — коммутативное кольцо, A и B суть R-модули, то имеет место изоморфизм $A \otimes_R B \cong B \otimes_R A$, при котором $a \otimes b$ отображается в $b \otimes a$ для всех $a \in A$, $b \in B$.

18.4. Если I — двусторонний идеал кольца R и $\rho\colon I \to R$ — вложение, то:

а) $\rho \otimes 1_{R/I} = 0$;

б) $I \otimes_R R/I \cong I/I^2$, в частности, $I \otimes_R R/I \neq 0$ для $I \neq I^2$.

18.5. Докажите следующие естественные изоморфизмы:

а) $(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C)$;

б) $(\bigoplus\limits_{i \in I} A_i) \otimes_R (\bigoplus\limits_{j \in J} B_j) \cong \bigoplus\limits_{i \in I,\ j \in J} (A_i \otimes_R B_j)$.

18.6. Пусть даны модули A_R и ${}_R B$. Тогда:

а) если $0 = \sum a_i \otimes b_i \in A \otimes_R B$, то существуют такие конечно порожденные подмодули $C \subseteq A$, $D \subseteq B$, что $a_i \in C$, $b_i \in D$ и $0 = \sum a_i \otimes b_i \in C \otimes_R D$;

б) если $G \subseteq A$, $H \subseteq B$ и $0 = \sum a_i \otimes b_i \in G \otimes_R H$, то $0 = \sum a_i \otimes b_i \in A \otimes_R B$.

18.7. Если каждый конечно порожденный подмодуль модуля M содержится в некотором плоском подмодуле, то сам M является плоским.

18.8. 1) Абелева группа плоска в точности тогда, когда является группой без кручения.

2) Любой плоский модуль является модулем без кручения (последние определены в начале § 15).

3) Если R — коммутативная наследственная область, то R-модуль M является плоским тогда и только тогда, когда M — модуль без кручения.

18.9. Пусть A_R — свободный R-модуль с базисом $\{x_i \mid i \in I\}$. Тогда каждый элемент из $A \otimes_R B$ представим в виде конечной суммы $\sum x_i \otimes b_i$, где элементы $0 \neq b_i \in B$ определены однозначно.

18.10. Пусть R — коммутативное кольцо, A_R — свободный R-модуль с базисом $x_1, \dots, x_m$ и ${}_RB$ — свободный R-модуль с базисом $z_1, \dots, z_n$. Тогда $A \otimes_R B$ есть свободный R-модуль с базисом $\{x_i \otimes z_j \,|\, i = 1, \dots, m; j = 1, \dots, n\}$.

18.11. Пусть $0 \to A \to B \to C \to 0$ — точная последовательность правых R-модулей. Тогда для всякого R-модуля ${}_RM$ индуцированная последовательность абелевых групп $A \otimes M \to B \otimes M \to C \otimes M \to 0$ точна.

18.12. Пусть даны модули A_R, ${}_RB_S$, C_S. Тогда можно определить гомоморфизм аддитивных групп

$$\Phi_{(A,B,C)} \colon \operatorname{Hom}_S(A \otimes_R B, C) \to \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, C)),\ \Phi_{(A,B,C)} \colon f \mapsto \widehat{f},$$

где $\widehat{f}(a)(b) = f(a \otimes b)$, $a \in A$, $b \in B$. Покажите, что $\Phi = \Phi_{(A,B,C)}$ является изоморфизмом. Как действует обратный к нему изоморфизм?

18.13. Напомним, что если $\alpha \colon A \to B$, $\gamma \colon C \to D$ — гомоморфизмы R-модулей, то $\operatorname{Hom}(\alpha, \gamma) : \beta \mapsto \gamma\beta\alpha$ является групповым гомоморфизмом $\operatorname{Hom}(\alpha, \gamma) : \operatorname{Hom}_R(B, C) \to \operatorname{Hom}_R(A, D)$.

Для любых гомоморфизмов $\xi \colon A'_R \to A_R$, $\mu \colon {}_RB'_S \to {}_RB_S$, $\eta \colon C_S \to C'_S$ диаграмма

$$\begin{array}{ccc} \operatorname{Hom}_S(A \otimes_R B, C) & \overset{\Phi_{(A,B,C)}}{\longrightarrow} & \operatorname{Hom}_R(A, \operatorname{Hom}_S(B, C)) \\ {\scriptstyle \operatorname{Hom}(\xi\otimes\mu,\eta)} \downarrow & & \downarrow {\scriptstyle \operatorname{Hom}(\xi,\operatorname{Hom}(\mu,\eta))} \\ \operatorname{Hom}_S(A' \otimes_R B', C') & \overset{\Phi_{(A',B',C')}}{\longrightarrow} & \operatorname{Hom}_R(A', \operatorname{Hom}_S(B', C')) \end{array}$$

коммутативна.

18.14. Пусть $\mathcal{M}_R$, соответственно, ${}_S\mathcal{M}_R$, — категория правых R-модулей, соответственно, бимодулей, $\mathcal{A}$ — категория $\mathbb{Z}$-модулей (т.е. абелевых групп). Покажите, что:

а) тензорное произведение является функтором $\otimes_R \colon \mathcal{M}_R \times_R \mathcal{M} \to \mathcal{A}$, ковариантным по обоим аргументам;

б) тензорное произведение является функтором $\otimes_R \colon {}_S\mathcal{M}_R \times {}_R\mathcal{M}_T \to {}_S\mathcal{M}_T$, ковариантным по обоим аргументам;

в) для каждого $B \in {}_S\mathcal{M}_R$

$$- \otimes_S B \colon \mathcal{M}_S \to \mathcal{M}_R \text{ и } \operatorname{Hom}_R(B, -) : \mathcal{M}_R \to \mathcal{M}_S$$

образуют пару сопряженных функторов (о сопряженных функторах см. [17], [51]).

18.15. 1) Для любого левого идеала I кольца R отображение $\sum a_i \otimes x_i \mapsto \sum a_i x_i$ задает канонический групповой эпиморфизм $h_I \colon A \otimes_R I \to AI$.

Если J — левый идеал кольца R, содержащий I, и $j \colon I \to J$ — естественное вложение, то $h_I = h_J(1_A \otimes j)$.

2) Канонический групповой эпиморфизм $h \colon A \otimes_R R \to A$ является изоморфизмом правого R-модуля $A \otimes R$ и модуля A_R.

3) Модуль A_R является плоским тогда и только тогда, когда для любого левого идеала I кольца R канонический групповой эпиморфизм $A \otimes I \to AI$ является изоморфизмом.

18.16. Если A_R — свободный модуль с базисом $\{e_i\}_{i \in I}$, ${}_RB$ — модуль, то абелева группа $A \otimes_R B$ изоморфна группе $\oplus_{|I|} B$.

18.17. Если ${}_RM_S$ — бимодуль над кольцами R и S, A_R — модуль, причем A_R и M_S являются свободными (проективными, плоскими) модулями, то $(A \otimes_R M)_S$ — свободный (проективный, плоский) модуль.

18.18. Для модуля ${}_RM$ следующие условия эквивалентны:

а) ${}_RM$ — плоский модуль;

б) для каждого конечно порожденного правого идеала $I \subseteq R$ с вложением $\rho \colon I_R \to R_R$ гомоморфизм $\rho \otimes 1_M$ является мономорфизмом;

в) модуль $M^*_R = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ инъективен.

18.19. Все прямые суммы и прямые слагаемые плоских модулей являются плоскими.

18.20. Проективные модули являются плоскими.

18.21. Пусть ${}_RM$ — плоский модуль, U — его подмодуль, I — правый идеал в R и $\rho \colon I \to R$ — вложение. Следующие условия эквивалентны:

а) $\rho \otimes 1_{M/U} \colon I \otimes_R (M/U) \to R \otimes_R (M/U)$ — мономорфизм;

б) $U \cap IM = IU$.

18.22. Пусть ${}_RM$ — плоский модуль, U — его подмодуль. Следующие условия эквивалентны:

а) фактормодуль M/U плоск;

б) $U \cap IM = IU$ для каждого конечно порожденного правого идеала $I \subseteq R$.

18.23. Если модуль ${}_RP$ проективен, $U \subseteq J(P)$ и фактормодуль P/U плоск, то $U = 0$.

18.24. Пусть R и S — кольца, P — проективный правый R-модуль и Q — R-S-бимодуль, являющийся проективным S-модулем. Тогда $P \otimes_R Q$ — проективный S-модуль.

В частности, если R — коммутативное кольцо, то тензорное произведение двух проективных R-модулей — проективный R-модуль.

18.25. Над коммутативным кольцом тензорное произведение двух плоских модулей является плоским модулем.

18.26. Пусть R — коммутативная область, в которой каждый конечно порожденный идеал является главным, т.е. R — кольцо Безу. Тогда левый модуль M является плоским в том и только в том случае, когда M — модуль без кручения.

18.27. Модуль M является регулярным в точности тогда, когда каждый его конечно порожденный подмодуль есть прямое слагаемое в M.

В упражнениях 18.28 – 18.31 S — кольцо эндоморфизмов модуля M_R, $f \in S$ и $m \in \mathbb{N}$. Докажите равносильность указанных в них условий.

18.28. а) Существует такой $g \in S$, что $f = fgf$, т.е. f — регулярный по фон Нейману элемент кольца S;

б) существуют такие идемпотенты $e_1, e_2 \in S$ и элемент $g \in S$, что $fg = e_1$, $gf = e_2$ и $f = e_1 f = f e_2$;

в) существует такой идемпотент $e \in S$, что $fS = eS$;

г) fS — прямое слагаемое модуля S_S;

д) $f(M)$ и $\operatorname{Ker} f$ — прямые слагаемые модуля M.

18.29. а) Существует такой $g \in S$, что $f = fgf$ и $fg = gf$;

б) существует такой $g \in S$, что $f = gf^2 = f^2 g$;

в) $M = \operatorname{Im} f \oplus \operatorname{Ker} f$.

18.30. а) $f = gf^m$ и $f = f^m g$ для некоторого $g \in S$;

б) $M = \operatorname{Im} f^m \oplus \operatorname{Ker} f^m$.

18.31. а) S — регулярное кольцо;

б) для любого $f \in S$ подмодули $\operatorname{Im} f$ и $\operatorname{Ker} f$ являются прямыми слагаемыми модуля M;

в) пересечение любых двух конечно порожденных правых идеалов X и Y кольца S является циклическим прямым слагаемым модуля S_S;

г) для любых таких $f, v \in S$, что $fS + vS = S$, существует такое $w \in S$, что $fS \cap vwS = 0$ и $S = fS \oplus vwS$.

18.32. Для кольца R равносильны следующие условия:

а) R — регулярное кольцо;

б) R_R — регулярный модуль;

в) ${}_R R$ — регулярный модуль;

г) пересечение любых двух конечно порожденных правых идеалов кольца R и правый аннулятор любого элемента кольца R являются циклическими прямыми слагаемыми модуля R_R;

д) пересечение любых двух конечно порожденных левых идеалов кольца R и левый аннулятор любого элемента кольца R являются циклическими прямыми слагаемыми модуля ${}_R R$;

е) для любого $f \in R$ существуют такие идемпотенты $e_1, e_2 \in R$ и элемент $g \in R$, что $fg = e_1$, $gf = e_2$ и $f = e_1 f = f e_2$;

ж) для любых $f, g \in R$ со свойством $fR + gR = R$ существует такой $h \in R$, что $fR \cap ghR = 0$ и $R = fR \oplus ghR$.

18.33. 1) Тела и прямые произведения тел являются регулярными кольцами.

2) Классически полупростое кольцо регулярно.

3) Все факторкольца и прямые произведения регулярных колец являются регулярными кольцами.

4) Кольца эндоморфизмов полупростых модулей являются регулярными.

5) Если кольцо R регулярно, то регулярно кольцо матриц $M(n, R)$ для каждого натурального n.

6) Для квазипроективного R-модуля M равносильны следующие условия:

а) $\operatorname{End}_R M$ — регулярное кольцо;

б) для любого $f \in \operatorname{End}_R M$ подмодуль $\operatorname{Im} f$ является прямым слагаемым модуля M.

18.34. Если Q_R — инъективный модуль, $S = \operatorname{End}_R Q$, то факторкольцо $S/J(S)$ регулярно.

18.35. Если R — регулярное кольцо, то каждый проективный R-модуль регулярен.

18.36. Кольцо R называется *строго регулярным*, если R удовлетворяет следующим равносильным условиям:

а) для любого $a \in R$ существует такой $b \in R$, что $a = a^2 b$;

б) для любого $a \in R$ существует такой $b \in R$, что $a = ba^2$;

в) каждый элемент кольца R является произведением центрального идемпотента и обратимого элемента;

г) R — регулярное редуцированное кольцо;

д) R — регулярное нормальное кольцо.

18.37. Пусть R — регулярное кольцо. Тогда:

а) для любого $a \in R$ найдется $b \in R$ со свойствами $a = aba$ и $b = bab$ (ср. с 2.55);

б) его центр $Z(R)$ является регулярным кольцом;

в) $I^2 = I$ для любого правого или левого идеала I кольца R.

18.38. 1) Если все факторкольца кольца R не имеют ненулевых нильпотентных идеалов (т.е. являются полупервичными), то решетка идеалов кольца R дистрибутивна и $I = I^2$ для любого идеала I кольца R.

2) Если R — регулярное кольцо, то решетка идеалов кольца R дистрибутивна и $I = I^2$ для любого правого или левого идеала I кольца R.

3) Произведение любых двух идемпотентов кольца R является регулярным (по фон Нейману) элементом в точности тогда, когда множество всех регулярных элементов кольца R мультипликативно замкнуто.

18.39. Пусть M_R — модуль, $S = \operatorname{End}_R M$.

1) S — строго регулярное кольцо в точности тогда, когда $M = f(M) \oplus \operatorname{Ker} f$ для любого $f \in S$.

2) R — строго регулярное кольцо в точности тогда, когда $R = aR \oplus r(a)$ для каждого $a \in R$.

3) В M сумма (соответственно, пересечение) любых двух прямых слагаемых снова есть прямое слагаемое модуля M тогда и только тогда, когда $\operatorname{Im}(e_1e_2)$ (соответственно, $\operatorname{Ker}(e_1e_2)$) — прямое слагаемое в M для любых двух идемпотентов $e_1, e_2 \in S$.

4) В M сумма и пересечение любых двух прямых слагаемых снова есть прямое слагаемое, т.е. множество всех прямых слагаемых образует подрешетку в решетке всех подмодулей модуля M тогда и только тогда, когда множество всех регулярных (по фон Нейману) элементов кольца S мультипликативно замкнуто, т.е. образует подполугруппу в мультипликативной полугруппе кольца S.

5) Множество всех идемпотентов кольца S мультипликативно замкнуто тогда и только тогда, когда каждое прямое слагаемое модуля M вполне инвариантно; последнее свойство согласно 15.93 равносильно тому, что S — нормальное кольцо.

18.40. Для кольца R равносильны следующие условия:

а) R — регулярное кольцо;

б) для любого $a \in R$ модуль $(R/aR)_R$ является плоским;

в) все правые и все левые R-модули являются плоскими.

18.41. Пусть M_R — регулярный модуль. Докажите, что:

а) каждый подмодуль U модуля M является регулярным модулем со свойством $J(U) = 0$;

б) если P — вполне инвариантный подмодуль модуля M, то $f(P) \subseteq P$ для всех $f \in \operatorname{Hom}_R(P, M)$;

в) если P и T — вполне инвариантные подмодули модуля M и $P \cong T$, то $P = T$;

г) если H — конечно порожденный, а C — циклический подмодуль модуля M, то $H + C = H \oplus E$ для некоторого циклического подмодуля E;

д) каждый конечно порожденный подмодуль модуля M является конечной прямой суммой циклических прямых слагаемых модуля M;

е) каждый счетно порожденный подмодуль K модуля M является (счетной) прямой суммой циклических прямых слагаемых модуля M;

ж) если M — прямое слагаемое прямой суммы счетно порожденных модулей, то M — прямая сумма циклических регулярных модулей;

з) если M — проективный модуль, то M изоморфен прямой сумме циклических регулярных прямых слагаемых модуля R_R и каждый счетно порожденный подмодуль K модуля M является проективным.

18.42. 1) Если M_R — прямое слагаемое прямой суммы проективных регулярных R-модулей M_i, то M — проективный регулярный модуль, изоморфный прямой сумме циклических регулярных прямых слагаемых модуля R_R;

2) Если M_R — проективный модуль, а R — регулярное кольцо, то M — регулярный модуль, изоморфный прямой сумме циклических регулярных прямых слагаемых модуля R_R, причем каждый счетно порожденный подмодуль модуля M является проективным.

18.43. Для кольца R равносильны следующие условия:

а) R — регулярное кольцо;

б) для любого конечно порожденного проективного R-модуля M_R кольцо $S = \operatorname{End}_R M$ является регулярным;

в) $N \cap MI = NI$ для каждого подмодуля N любого модуля M_R и для любого левого идеала I кольца R.

18.44. Пусть G — конечная группа и R — кольцо. Групповое кольцо RG регулярно тогда и только тогда, когда R регулярно и порядок группы G обратим в R.

18.45. Пусть $\epsilon\colon S \to R$ — гомоморфизм колец, B — правый, A — левый R-модули. Покажите, что отображение образующих элементов $b \otimes_S a \to b \otimes_R a$ индуцирует эпиморфизм абелевых групп $t\colon B \otimes_S A \to B \otimes_R A$ (B и A считаем, как в упражнении 15.10, притягивающими S-модулями).

Глава V. Абелевы группы

19 Основные понятия теории абелевых групп

В абелевых группах принято использовать аддитивную форму записи, применяя + в качестве основной операции, и 0 в качестве нейтрального элемента.

Важное обстоятельство для теории абелевых групп заключается в том, что абелевы групп и модули над кольцом целых чисел $\mathbb{Z}$ можно не различать как алгебраические объекты (см. 15.19). Так, подгруппы абелевой группы A совпадают с подмодулями $\mathbb{Z}$-модуля A. Далее, напомним, что гомоморфизм $\varphi\colon A \to B$ абелевых групп есть отображение со свойством $\varphi(a+b) = \varphi(a) + \varphi(b)$ при всех $a, b \in A$. Поскольку $\varphi(na) = n\varphi(a)$, $n \in \mathbb{Z}$, $a \in A$, то получаем, что групповые гомоморфизмы это в точности гомоморфизмы $\mathbb{Z}$-модулей. Основные понятия, конструкции и факты общего характера теории модулей применимы к абелевым группам. Например, используем все, что касается прямых сумм и произведений модулей (о них написано в § 15). В частности, через $\bigoplus\limits_m A$ обозначаем прямую сумму m групп, изоморфных A, а через $\prod\limits_m A$ или A^m — произведение m таких групп (m — некоторое кардинальное число).

Кольцо целых чисел $\mathbb{Z}$ является примером коммутативной области главных идеалов. Поэтому в теории абелевых групп исключительную роль играют простые числа (т.е. простые элементы кольца $\mathbb{Z}$).

Понятия периодической группы, p-группы, группы без кручения и порядка элемента a (он обозначается $o(a)$) введены в начале § 3. Абелевы p-группы еще называются *примарными*. Периодическая часть $t(A)$ абелевой группы A образует ее подгруппу, называемую *периодической подгруппой*. Для каждого простого числа p множество A_p всех p-элементов группы A также есть подгруппа, называемая *p-компонентой группы A*.

Для конечных абелевых групп справедлива следующая основная теорема о таких группах.

Теорема 19.1. *Всякая конечная абелева группа является прямой суммой примарных циклических подгрупп. Любые два таких разложения имеют по одинаковому числу слагаемых каждого порядка.*

Свободной абелевой группой называется прямая сумма бесконечных циклических групп, т.е. свободный $\mathbb{Z}$-модуль (см. начало § 15). Если эти циклические группы порождаются элементами x_i ($i \in I$), то свободная группа имеет вид $F = \bigoplus\limits_{i\in I} \langle x_i\rangle$, множество $X = \{x_i \mid i \in I\}$ называется *системой свободных образующих* или *свободным базисом* группы F. Мощность $|I|$ множества I называется *рангом* свободной группы F. Ранг свободной группы определяется однозначно. Всякая подгруппа свободной абелевой группы снова является свободной группой. Конечно порожденные абелевы группы без кручения являются свободными группами.

Если $a \in A$, то наибольшее неотрицательное целое число n, для которого уравнение $p^n x = a$ имеет решение $x \in A$, называется *p-высотой* $h_p^A(a)$ элемента a. Если $a \in p^n A$ для каждого натурального n, то a называется *элементом бесконечной p-высоты*, $h_p^A(a) = \infty$.

Последовательность групп A_i и гомоморфизмов α_i

$$A_0 \xrightarrow{\alpha_1} A_1 \xrightarrow{\alpha_2} \dots \xrightarrow{\alpha_k} A_k \quad (k \geqslant 2)$$

называется *точной*, если $\operatorname{Im}\alpha_i = \operatorname{Ker}\alpha_{i+1}$, $i = 1, \dots, k-1$.

Подгруппа G группы A называется *существенной*, если $G \cap B \neq 0$ для любой ненулевой подгруппы B группы A, (т.е. G — существенный $\mathbb{Z}$-подмодуль в A). Отметим, что в литературе вполне инвариантную подгруппу абелевой группы (см. начало § 8 и § 15) иногда называют *вполне характеристической*.

Система $\{a_i \mid i \in I\}$ ненулевых элементов группы A называется *линейно независимой* или просто *независимой*, если из равенства

$$n_1 a_{i_1} + \dots + n_k a_{i_k} = 0 \quad (a_{i_j} \in A_{i_j},\ n_i \in \mathbb{Z})$$

вытекает, что $n_1 a_{i_1} = \dots = n_k a_{i_k} = 0$.

Рангом $r(A)$ группы A называется мощность ее максимальной независимой системы, содержащей только элементы бесконечного порядка или порядка, равного степени некоторого простого числа. Мощность максимальной независимой системы, состоящей только из элементов бесконечного порядка, называется *рангом без кручения* $r_0(A)$ группы A. Для всякой группы A верно равенство $r(A) = r_0(A) + \sum\limits_p r(A_p)$, где p пробегает все простые числа. Ранги $r(A)$ и $r_0(A)$ группы A являются инвариантами этой группы. Инварианты группы (или другой алгебраической структуры) обычно являются натуральными, кардинальными числами или другими легко описываемыми величинами (например, матрицами). Они должны однозначно определяться группой.

Важную роль в теории абелевых групп играют прямые суммы циклических групп. Каждая такая группа A представима в виде $A = F \oplus (\bigoplus\limits_p A_p)$, где F — свободная группа, а A_p есть прямая сумма циклических p-групп. Справедлива теорема

Теорема 19.2. *p-группа A является прямой суммой циклических групп тогда и только тогда, когда A есть объединение возрастающей последовательности подгрупп*

$$A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots, \quad \bigcup_{n=1}^{\infty} A_n = A,$$

где высоты ненулевых элементов, входящих в A_n, меньше фиксированного числа k_n.

Группа C называется *коциклической*, если существует такой элемент $c \in C$, что всякий гомоморфизм $\varphi\colon C \to B$, где $c \notin \operatorname{Ker}\varphi$, является мономорфизмом. Известно, что группа C коциклическая тогда и только тогда, когда $C \cong \mathbb{Z}_{p^k}$, $k = 1, 2, \ldots$ или ∞.

Топология в абелевых группах может быть введена различными способами. Наиболее существенными являются *линейные топологии*. Это такие топологии, что имеется база (фундаментальная система) окрестностей нуля, состоящая из подгрупп, причем смежные классы по этим подгруппам образуют базу открытых множеств.

Большое значение имеют следующие топологии.

1. *$\mathbb{Z}$-адическая топология*, где базу окрестностей нуля образуют подгруппы nA ($n \in \mathbb{Z}$, $n \neq 0$). Она хаусдорфова тогда и только тогда, когда $A^1 = 0$ (через A^1 для группы A обозначается ее подгруппа $A^1 = \bigcap_{n=1}^{\infty} nA$), дискретна тогда и только тогда, когда $nA = 0$ для некоторого n.

2. *p-адическая топология*, где базу окрестностей нуля образуют подгруппы $p^k A$ ($k = 0, 1, 2, \ldots$).

3. *Топология конечных индексов*, где базу окрестностей нуля составляют подгруппы U группы A, имеющие конечный индекс.

Абелева группа A называется *делимой*, если $nA = A$ и p-делимой, если $p^n A = A$ для каждого натурального числа n.

Пусть $\aleph_\sigma$ — кардинальное число. Группа называется *$\aleph_\sigma$-свободной*, если все ее подгруппы мощности $< \aleph_\sigma$ свободны.

Теорема 19.3. *Прямое произведение бесконечного множества бесконечных циклических групп является $\aleph_1$-свободной, но не свободной группой.*

Как правило, в этой главе под словом «группа» понимается «абелева группа».

Задачи

19.1. Всякий эпиморфизм конечной группы на себя является ее автоморфизмом.

19.2. Разложите в прямую сумму группы: $\mathbb{Z}_6$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{60}$, $\mathbb{Z}_{900}$.

19.3. Прямая сумма $\mathbb{Z}_n \oplus \mathbb{Z}_m$ является циклической группой тогда и только тогда, когда $(m, n) = 1$.

19.4. Подгруппа является максимальной тогда и только тогда, когда ее индекс — простое число.

19.5. Найдите с точностью до изоморфизма все абелевы группы порядка 2, 6, 8, 12, 16, 24, 36, 48.

19.6. Изоморфны ли группы: $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$; $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$; $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$ и $\mathbb{Z}_{60} \oplus \mathbb{Z}_{10}$?

19.7. Сколько подгрупп порядков 2 и 6 (порядков 5 и 15) в нециклической группе порядка 12 (порядка 75)?

19.8. Сколько элементов:

а) порядка 2, 4 и 6 в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$;

б) порядков 2, 4 и 5 в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$?

19.9. Докажите неразложимость групп: $\mathbb{Z}_p$, $\mathbb{Z}$, $\mathbb{Z}_{p^\infty}$, $\mathbb{Q}$ и $\widehat{\mathbb{Z}}_p$. Будут ли неразложимыми также и их подгруппы?

19.10. Если в группе подгруппы $A_1, \ldots, A_n$ имеют конечные попарно взаимно простые порядки, то их сумма является прямой.

19.11. 1) $\mathbb{C}$ есть прямая сумма подгрупп вещественных и чисто мнимых чисел.

2) $\mathbb{R}^*$ есть прямое произведение подгруппы положительных чисел и подгруппы чисел ± 1.

3) $\mathbb{C}^*$ есть прямое произведение группы положительных вещественных чисел и группы всех комплексных чисел, по модулю равных 1.

19.12. 1) Замыкание $B^\wedge$ подгруппы B в $\mathbb{Z}$-адической топологии группы A задается формулой $B^\wedge = \bigcap_{n=1}^{\infty} (B + nA)$.

2) Подгруппа B группы A замкнута в $\mathbb{Z}$-адической топологии тогда и только тогда, когда $(A/B)^1 = 0$.

3) Подгруппа B группы A плотна в $\mathbb{Z}$-адической топологии тогда и только тогда, когда A/B — делимая группа.

4) $\mathbb{Z}$-адическая и p-адическая топологии на группе A совпадают, если $qA = A$ для любого простого $q \neq p$.

19.13. 1) Если на группе A задана линейная топология, то всякая открытая ее подгруппа B будет замкнутой.

2) Всякий групповой гомоморфизм непрерывен в $\mathbb{Z}$-адической, в p-адической и в топологии конечных индексов.

19.14. Для группы A эквивалентны следующие условия:

а) p-адическая топология группы A хаусдорфова;

б) A не содержит ненулевых элементов бесконечной p-высоты;

в) $||a|| = e^{(-h_p(a))}$ является нормой на группе A ($a \in A$);

г) $\delta(a,b) = ||a-b||$ служит метрикой на группе A ($a, b \in A$), определяющей ее p-адическую топологию.

19.15. Разложите в прямую сумму циклических групп факторгруппу A/B, где A — свободная группа с базисом x_1, x_2, x_3, а B — ее подгруппа, порожденная элементами y_1, y_2, y_3:

а) $\left\{\begin{array}{lcl} y_1 &=& 7x_1+2x_2+3x_3,\\ y_2 &=& 21x_1+8x_2+9x_3,\\ y_3 &=& 5x_1-4x_2+3x_3; \end{array}\right.$ б) $\left\{\begin{array}{lcl} y_1 &=& 6x_1+5x_2+7x_3,\\ y_2 &=& 8x_1+7x_2+11x_3,\\ y_3 &=& 6x_1+5x_2+11x_3. \end{array}\right.$

19.16. 1) Если A/B — бесконечная циклическая группа, то подгруппа B — прямое слагаемое в A.

2) Если $A/B = \bigoplus\limits_{i\in I}(C_i/B)$, и B выделяется прямым слагаемым в каждой группе C_i, то B — прямое слагаемое в A.

3) Если A/B — свободная группа, то подгруппа B — прямое слагаемое в A.

19.17. 1) Множество $A\,[n] = \{a \in A \,|\, na = 0$ для фиксированного натурального $n\}$ образует вполне инвариантную подгруппу группы A.

2) Множество $\operatorname{Soc} A = \{a \in A \,|\, o(a)$ — число, не делящееся на квадрат$\}$ образует вполне инвариантную подгруппу — это *цоколь* группы A как $\mathbb{Z}$-модуля; $\operatorname{Soc} A = A[p]$ для p-группы A, $\operatorname{Soc} A = 0$ тогда и только тогда, когда A — группа без кручения.

3) Периодическая часть $t(A)$ образует вполне инвариантную подгруппу группы A.

4) Если B — произвольная подгруппа в A, то $t(B) = t(A) \cap B$ и $\operatorname{Soc} B = (\operatorname{Soc} A) \cap B$.

19.18. Прямая сумма p-групп (периодических групп) сама является p-группой (периодической группой). Когда прямое произведение периодических групп является периодической группой?

19.19. Всякая конечно порожденная группа является прямой суммой свободной группы конечного ранга и конечной группы.

19.20. Если $B \subset A$, $|B| < |A|$ и мощность $|A|$ бесконечна, то $|A/B| = |A|$.

19.21. Для всякого гомоморфизма $\alpha\colon A \to B$ существует точная последовательность

$$0 \to \operatorname{Ker}\alpha \to A \xrightarrow{\alpha} B \to B/\operatorname{Im}\alpha \to 0.$$

19.22 (5-лемма, ср. с 15.41). Пусть

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5\\ \downarrow{\scriptstyle\gamma_1} & & \downarrow{\scriptstyle\gamma_2} & & \downarrow{\scriptstyle\gamma_3} & & \downarrow{\scriptstyle\gamma_4} & & \downarrow{\scriptstyle\gamma_5}\\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5 \end{array}$$

— коммутативная диаграмма с точными строками. Тогда

а) если γ_1 — эпиморфизм, а γ_2, γ_4 — мономорфизмы, то γ_3 — мономорфизм;

б) если γ_5 — мономорфизм, а γ_2, γ_4 — эпиморфизмы, то γ_3 — эпиморфизм;

в) если γ_1 — эпиморфизм, γ_5 — мономорфизм, γ_2, γ_4 — изоморфизмы, то γ_3 — изоморфизм.

19.23 (3×3-лемма). Предположим, что диаграмма

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0\\ & & \downarrow & & \downarrow & & \downarrow\\ 0 \to & A_1 & \xrightarrow{\alpha_1} & B_1 & \xrightarrow{\beta_1} & C_1 & \to 0\\ & \downarrow{\scriptstyle\lambda_1} & & \downarrow{\scriptstyle\mu_1} & & \downarrow{\scriptstyle\nu_1} & \\ 0 \to & A_2 & \xrightarrow{\alpha_2} & B_2 & \xrightarrow{\beta_2} & C_2 & \to 0\\ & \downarrow{\scriptstyle\lambda_2} & & \downarrow{\scriptstyle\mu_2} & & \downarrow{\scriptstyle\nu_2} & \\ 0 \to & A_3 & \xrightarrow{\alpha_3} & B_3 & \xrightarrow{\beta_3} & C_3 & \to 0\\ & \downarrow & & \downarrow & & \downarrow & \\ & 0 & & 0 & & 0 & \end{array}$$

коммутативна, а все три ее столбца точны. Тогда если первые две или две последние строки точны, то оставшаяся строка тоже точна.

19.24. Диаграмма:

$$\text{а)}\quad \begin{array}{ccccc} & & G & & \\ & & \downarrow\eta & & \\ 0 & \to A \xrightarrow{\alpha} & B & \xrightarrow{\beta} C, & \end{array} \qquad \text{б)}\quad \begin{array}{ccccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \to 0 \\ & & \downarrow\eta & & & \\ & & G & & & \end{array}$$

с точной строкой может быть пополнена гомоморфизмом φ, где а) $\varphi\colon G \to A$, б) $\varphi\colon C \to G$, так, чтобы получилась коммутативная диаграмма тогда и только тогда, когда а) $\beta\eta = 0$, б) $\eta\alpha = 0$. При этом гомоморфизм φ определяется однозначно.

19.25. 1) Пересечение всех максимальных подгрупп группы A одного и того же простого индекса p совпадает с pA.

2) Подгруппа Фраттини $\Phi(A)$ совпадает с пересечением подгрупп pA, где p пробегает все простые числа.

3) Найдите подгруппу Фраттини групп $\mathbb{Z}_n$, $\mathbb{Z}$, $\mathbb{Z}_{p^\infty}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Q}^{(p)}$, $\widehat{\mathbb{Z}}_p$ (см. 3.51 и 20.19).

19.26. Пусть $\varphi_i\colon B_i \to A$, $\psi_i\colon A \to B_i$ — гомоморфизмы, $i \in I$. Тогда существуют единственные гомоморфизмы $\varphi\colon \bigoplus\limits_{i\in I} B_i \to A$, $\psi\colon A \to \prod\limits_{i\in I} B_i$, превращающие диаграммы

$$\begin{array}{ccc} B_i & \xrightarrow{\rho_i} & \bigoplus\limits_{i\in I} B_i \\ \downarrow{\scriptstyle\varphi_i} & & \downarrow{\scriptstyle\varphi} \\ A & \xrightarrow{1_A} & A, \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{1_A} & A \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi_i} \\ \prod\limits_{i\in I} B_i & \xrightarrow{\pi_i} & B_i \end{array}$$

в коммутативные, где ρ_i — вложения, π_i — проекции.

19.27. Если даны гомоморфизмы $\alpha\colon A \to C$ и $\beta\colon B \to C$, то существуют такая группа G, определенная однозначно с точностью до изоморфизма, и такие гомоморфизмы $\gamma\colon G \to A$, $\delta\colon G \to B$, что 1) диаграмма $(*)$

$$\begin{array}{ccc} G & \xrightarrow{\gamma} & A \\ \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\alpha} \\ B & \xrightarrow{\beta} & C \end{array}$$

коммутативна, и 2) если

$$\begin{array}{ccc} G' & \xrightarrow{\gamma'} & A \\ \downarrow{\scriptstyle\delta'} & & \downarrow{\scriptstyle\alpha} \\ B & \xrightarrow{\beta} & C \end{array}$$

— коммутативная диаграмма, то существует однозначно определенный гомоморфизм $\varphi\colon G' \to G$ со свойствами $\gamma\varphi = \gamma'$ и $\delta\varphi = \delta'$.

Коммутативная диаграмма $(*)$, удовлетворяющая условию 2), называется *коуниверсальным квадратом*.

19.28. Если даны гомоморфизмы $\alpha\colon C \to A$ и $\beta\colon C \to B$, то существуют такая группа G, определенная однозначно с точностью до изоморфизма, и такие гомоморфизмы $\gamma\colon A \to G$, $\delta\colon B \to G$, что 1) диаграмма $(**)$

$$\begin{array}{ccc} C & \xrightarrow{\alpha} & A \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ B & \xrightarrow{\delta} & G \end{array}$$

коммутативна, и 2) если

$$\begin{array}{ccc} C & \xrightarrow{\alpha} & A \\ \downarrow{\scriptstyle\beta} & & \downarrow\gamma' \\ B & \xrightarrow{\delta'} & G' \end{array}$$

— коммутативная диаграмма, то существует однозначно определенный гомоморфизм $\varphi\colon G \to G'$ со свойствами $\varphi\gamma = \gamma'$ и $\varphi\delta = \delta'$.

Коммутативная диаграмма $(**)$, удовлетворяющая условию 2), называется *универсальным квадратом*.

19.29. 1) Если в коуниверсальном квадрате $(*)$ гомоморфизм α является мономорфизмом (эпиморфизмом), то и δ — мономорфизм (эпиморфизм).

2) Если в универсальном квадрате $(**)$ гомоморфизм α является мономорфизмом (эпиморфизмом), то и δ — мономорфизм (эпиморфизм).

19.30. Периодическая группа A является прямой суммой всех своих p-компонент.

19.31. 1) $\mathbb{Q}/\mathbb{Z} \cong \bigoplus\limits_{p} \mathbb{Z}_{p^\infty}$, а $(\mathbb{Z}_p)^m \cong \bigoplus\limits_{2^m} \mathbb{Z}_p$ для каждого бесконечного кардинального числа m.

2) Если $n = p_1^{r_1} \dots p_k^{r_k}$, то $A/nA \cong \bigoplus\limits_{i=1}^{k} A/p_i^{r_i}A$.

19.32. Две свободные группы изоморфны тогда и только тогда, когда они имеют одинаковый ранг.

19.33. Множество $X = \{x_i \mid i \in I\}$ образующих группы F является системой свободных образующих (и, следовательно, F является свободной группой) тогда и только тогда, когда всякое отображение φ множества X в группу A может быть продолжено до ровно одного гомоморфизма $\psi\colon F \to A$ (ср. с 5.43).

Группа G называется *проективной*, если G — проективный $\mathbb{Z}$-модуль (см. § 17).

19.34. Группа проективна тогда и только тогда, когда она — свободная группа.

19.35. Если F — такая группа, что из $B \subseteq A$ и $A/B \cong F$ всегда вытекает, что B — прямое слагаемое группы A, то F — свободная группа.

19.36. 1) Если F — свободная группа, G — ее подгруппа, а H — прямое слагаемое, то $G \cap H$ — прямое слагаемое группы G.

2) Пересечение конечного числа прямых слагаемых свободной группы само является прямым слагаемым.

19.37. Пусть B — подгруппа группы A и C является B-*высокой* подгруппой в A (т.е. C — максимальная подгруппа в A, имеющая нулевое пересечение с B; другими словами, C — д.п. для B в A). Тогда $A = B \oplus C$ в том и только в том случае, когда из равенства $pa = b + c$ ($a \in A$, $b \in B$, $c \in C$) следует $pb' = b$ для некоторого $b' \in B$.

19.38. Независимая система M элементов группы A максимальна, если и только если $\langle M\rangle$ — существенная подгруппа группы A. Всякая максимальная независимая система элементов существенной подгруппы группы A является максимальной независимой системой и в A.

19.39. Пусть B — подгруппа группы A. Тогда:

а) $r(B) \leqslant r(A)$;

б) $r(A) \leqslant r(B) + r(A/B)$, причем возможен случай, когда $r(A) < r(A/B)$;

в) $r_0(A) = r_0(B) + r_0(A/B)$.

19.40. Пусть B_i ($i \in I$) — такие подгруппы группы A, что $A = \sum\limits_{i\in I} B_i$. Тогда $r(A) \leqslant \sum\limits_{i\in I} r(B_i)$, причем если сумма прямая, то имеет место равенство.

19.41. Группа бесконечного ранга m содержит в точности 2^m различных подгрупп.

19.42. 1) Группа A не содержит разложимых подгрупп тогда и только тогда, когда $r(A) \leqslant 1$.

2) $r(A) \leqslant 1$ тогда и только тогда, когда группа A изоморфна подгруппе группы $\mathbb{Q}$ или подгруппе некоторой группы $\mathbb{Z}_{p^\infty}$.

19.43. 1) Если E — существенная подгруппа группы A и $B \subseteq A$, то $E \cap B$ — существенная подгруппа в B.

2) Подгруппа B группы A является существенной тогда и только тогда, когда $\operatorname{Soc} A \subseteq B$ и A/B — периодическая группа.

3) Подгруппа B группы A является существенной тогда и только тогда, когда всякий гомоморфизм $\alpha\colon A \to G$ в произвольную группу G является мономорфизмом, если его ограничение на подгруппу B есть мономорфизм.

19.44 (Ср. с 15.56 и 15.57). Группа A является элементарной тогда и только тогда, когда выполнено одно из следующих условий:

а) каждая подгруппа группы A — прямое слагаемое в A;

б) она является периодической группой, подгруппа Фраттини которой нулевая;

в) она является единственной существенной своей подгруппой.

Группа A называется *ограниченной*, если $nA = 0$ для некоторого $n \in \mathbb{N}$.

19.45. Ограниченная группа является прямой суммой циклических групп.

19.46. Счетная p-группа A является прямой суммой циклических групп тогда и только тогда, когда она не содержит ненулевых элементов бесконечной высоты.

19.47. Пусть A — периодическая подгруппа прямого произведения $\prod\limits_{n=1}^{\infty} \mathbb{Z}_{p^n}$. Тогда A есть p-группа мощности континуума без элементов бесконечной высоты, группа A не является прямой суммой циклических групп. Этот пример показывает, что требование счетности в 19.46 существенно.

Прямые разложения $A = \bigoplus\limits_{i\in I} B_i$ и $A = \bigoplus\limits_{j\in J} C_j$ называются *изоморфными*, если существует биекция $f\colon I \to J$ такая, что $A_i \cong C_{f(i)}$ при всех $i \in I$.

19.48. Любые два разложения группы в прямую сумму циклических групп бесконечного порядка и порядков, равных степеням простых чисел, изоморфны.

19.49. Пусть A, B — прямые суммы циклических групп. Тогда из $A \oplus A \cong B \oplus B$ вытекает $A \cong B$, а из $\bigoplus\limits_{\aleph_0} A \cong \bigoplus\limits_{\aleph_0} B$ не следует $A \cong B$.

19.50. Пусть $G = \bigoplus\limits_{k=1}^{\infty} \mathbb{Z}_{p^k}$. Тогда всякая счетная p-группа является эпиморфным образом группы G, а всякая p-группа мощности $m > \aleph_0$ является эпиморфным образом прямой суммы m групп, изоморфных группе G.

19.51. Подгруппы прямых сумм циклических групп сами являются прямыми суммами циклических групп.

19.52. Счетная группа без кручения является свободной тогда и только тогда, когда каждая ее подгруппа конечного ранга свободна.

19.53. Всякая счетная группа A может быть представлена в виде $A = N \oplus F$, где F — свободная группа, а группа N не имеет свободных факторгрупп. Подгруппа N определяется группой A однозначно.

19.54. Группа делима тогда и только тогда, когда выполнено одно из следующих условий:

а) в ней нет максимальных подгрупп, т.е. когда она совпадает со своей подгруппой Фраттини;

б) она не имеет ненулевых конечных эпиморфных образов.

19.55. 1) Прямая сумма и прямое произведение групп делимы, если и только если каждое слагаемое является делимой группой.

2) Группы $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, а также $\mathbb{Z}_{p^\infty}$, делимы.

3) Факторгруппа делимой группы делима.

4) Если B и A/B — делимые группы, то группа A также делима.

5) Аддитивная группа любого поля характеристики 0 является делимой группой без кручения.

6) Факторгруппа $\widehat{\mathbb{Z}}_p/\mathbb{Z}$ делима.

Группа D называется *инъективной*, если она инъективна как $\mathbb{Z}$-модуль (см. § 17). Инъективность группы D можно интерпретировать как возможность продолжить любой гомоморфизм $\varphi\colon A \to D$ до гомоморфизма группы B, содержащей A, в группу D.

19.56. Делимые группы инъективны (см. 17.20 6)).

19.57. Делимая подгруппа D группы A служит для A прямым слагаемым, т.е. $A = D \oplus C$ для некоторой подгруппы C группы A. Эту подгруппу C можно выбрать так, что она будет содержать заранее заданную подгруппу B группы A, для которой $D \cap B = 0$.

Группа называется *редуцированной*, если она не содержит ненулевых делимых подгрупп.

19.58. Всякая группа A является прямой суммой делимой группы D и редуцированной группы C, $A = D \oplus C$. Подгруппа D группы A здесь определяется однозначно (ее называют *делимой частью группы* A), подгруппа C — с точностью до изоморфизма.

Теорема, содержащаяся в 19.58, имеет большое значение для теории абелевых групп, поскольку сводит проблему описания строения абелевых групп к проблеме описания строения делимых и редуцированных групп.

19.59. Всякая делимая группа D является прямой суммой квазициклических групп и групп, изоморфных группе $\mathbb{Q}$. Таким образом, для делимой группы D имеет место разложение

$$D \cong \bigoplus_{n_0} \mathbb{Q} \oplus \bigoplus_{p} \Big(\bigoplus_{n_p} \mathbb{Z}_{p^\infty}\Big),$$

где $n_0 = r_0(D)$, $n_p = r(D_p)$.

19.60. Группа $\mathbb{R}$ изоморфна группе $\bigoplus\limits_{2^{\aleph_0}} \mathbb{Q}$ и $\mathbb{R}^{\aleph_0} \cong \bigoplus\limits_{\aleph_0} \mathbb{R}$.

19.61. Пусть $K = \prod\limits_{p} \mathbb{Z}_{p^\infty}$, где p пробегает все простые числа. Покажите, что K изоморфна группе вещественных чисел, рассматриваемых по модулю 1, и $K \cong \big(\bigoplus\limits_{p} \mathbb{Z}_{p^\infty}\big) \oplus \big(\bigoplus\limits_{2^{\aleph_0}} \mathbb{Q}\big)$.

19.62. Если m — бесконечное кардинальное число, то $\prod\limits_{m} \mathbb{Z}_{p^\infty} \cong \bigoplus\limits_{2^m} (\mathbb{Z}_{p^\infty} \oplus \mathbb{Q})$.

Группа A, необязательно абелева, называется *хопфовой*, если всякий эпиморфизм группы A на себя является автоморфизмом. Аналогично определяются хопфовы модули, хопфовы кольца и другие подобные объекты. Конечная абелева группа всегда хопфова (упр. 19.1). Любая свободная группа конечного ранга хопфова (А.И. Мальцев). В то

же время доказано существование нехопфовых групп с двумя образующими и одним определяющим соотношением. В следующем упражнении группы предполагаются абелевыми.

19.63. 1) Хопфовость группы A равносильна отсутствию у A изоморфных себе собственных факторгрупп, т.е. таких факторгрупп A/C, что $C \neq 0$ и $A \cong A/C$.

2) Конечно порожденная группа хопфова.

3) Прямое слагаемое хопфовой группы есть хопфова группа. С другой стороны, существует хопфова группа A такая, что группа $A \oplus A$ не хопфова.

4) Хопфова группа не имеет прямых слагаемых, являющихся прямой суммой бесконечного числа копий какой-либо группы.

19.64. Квазиинъективная группа (т.е. квазиинъективный $\mathbb{Z}$-модуль) или инъективна, или является периодической группой, p-компоненты которой — прямые суммы изоморфных между собой циклических групп.

19.65. Всякую группу можно вложить в качестве подгруппы в некоторую делимую группу.

Для заданной группы A делимая группа E, содержащая A, называется *минимальной делимой группой*, если в E нет собственных делимых подгрупп, содержащих A.

19.66. 1) Делимая группа E, содержащая группу A, является минимальной делимой группой тогда и только тогда, когда A — существенная подгруппа группы E.

2) Всякая делимая группа E, подгруппой которой является группа A, имеет минимальную делимую группу, содержащую A, причем любые две минимальные делимые группы, содержащие A, изоморфны над A.

Минимальную делимую группу E, содержащую группу A, называют *делимой* (или *инъективной*) *оболочкой* группы A. Так как $r_0(E) = r_0(A)$ и $r(E_p) = r(A_p)$ для каждого простого p, то строение делимой оболочки группы A полностью определяется рангами группы A.

19.67. (См. упр. 17.21). Для группы D эквивалентны следующие условия:

а) D — делимая группа;

б) D — инъективная группа;

в) D служит прямым слагаемым для всякой содержащей ее группы.

19.68. Пусть A — группа без кручения, E — множество всех пар (a, m), где $a \in A$, m — натуральное число и $(a, m) = (b, n)$, если и только если $mb = na$. Пусть, далее, $(a, m) + (b, n) = (na + mb, mn)$. Покажите, что E — минимальная делимая группа, содержащая образ мономорфизма $A \to E$, $a \mapsto (a, 1)$, $a \in A$.

19.69. Делимая оболочка группы A является делимой оболочкой подгруппы B группы A тогда и только тогда, когда B — существенная подгруппа группы A.

19.70. 1) Делимая группа D, содержащая группу A, минимальна в точности тогда, когда D/A — периодическая группа и A содержит цоколь группы D.

2) Если D — делимая оболочка p-делимой группы A, то факторгруппа D/A имеет нулевую p-компоненту.

19.71. Если группа A служит прямым слагаемым для всякой такой содержащей ее группы G, что G/A — квазициклическая группа, то A — делимая группа.

19.72. Если C — такая подгруппа группы B, что факторгруппа B/C изоморфна какой-то подгруппе группы G, то существует такая содержащая B группа A, что $A/C \cong G$.

Если a — элемент порядка p^k группы A, то через $e(a) = k$ обозначим его *экспоненту*. Положим $A[p^k] = \{a \in A \mid p^k a = 0\}$, причем если A — p-группа, то $A[p^\infty] = A$.

19.73. Пусть $A = B \oplus D$, где B — редуцированная, а D — делимая группы. Подгруппа H вполне инвариантна в A тогда и только тогда, когда H имеет один из следующих видов:

а) $H = B' \oplus (\oplus_p D_p[p^{k_p}])$, где B' — периодическая вполне инвариантная подгруппа группы B и $k_p \geqslant m_p = \sup\{e(b) \mid b \in B'_p\}$;

б) $H = B' \oplus D$, где B' — вполне инвариантная подгруппа группы B.

19.74. Периодические квазинепрерывные группы (т.е. квазинепрерывные $\mathbb{Z}$-модули) являются квазиинъективными, а разложимые квазинепрерывные группы без кручения являются инъективными.

Подгруппа H группы A называется *инвариантной относительно проекций*, если $\pi H \subseteq H$ для каждой проекции π группы A.

19.75. 1) Прямое слагаемое, инвариантное относительно проекций, является вполне инвариантным.

2) Если H — подгруппа группы A, инвариантная относительно проекций, и π — проекция группы A, то отображение $a + H \mapsto \pi a + H$ — проекция группы A/H; в частности, если $A = B \oplus C$, то $A/H = (B + H)/H \oplus (C + H)/H$.

3) Если H, B — такие подгруппы группы A, что $H \subseteq B$ и H инвариантна относительно проекций группы A, а B/H инвариантна относительно проекций группы A/H, то B инвариантна относительно проекций группы A.

4) Инвариантная относительно проекций подгруппа H группы $A = \oplus A_i$ является вполне инвариантной тогда и только тогда, когда каждая $H \cap A_i$ — вполне инвариантная подгруппа группы A_i.

19.76. Пусть $A = B \oplus D$, где B — редуцированная, D — делимая группы, $D = D_0 \oplus t(D)$. Подгруппа H инвариантна относительно проекций группы A тогда и только тогда, когда H имеет один из следующих видов:

а) $H = B' \oplus (\oplus_p D_p[p^{k_p}])$, где B' — инвариантная относительно проекций периодическая подгруппа группы B и $k_p \geqslant m_p = \sup\{e(b) \mid b \in B'_p\}$;

б) $H = B' \oplus D'_0 \oplus t(D)$, где B' — инвариантная относительно проекций подгруппа группы B, $0 \neq D'_0 \subseteq D_0$, причем $D'_0 = D_0$, если B' — непериодическая группа или если группа D_0 разложима.

20 Чистота и чистая инъективность

Подгруппа B группы A называется *чистой* (*сервантной*), если $B \cap nA = nB$ для каждого натурального числа n.

Подгруппа B группы A называется *p-чистой* (p — простое число), если $B \cap p^k A = p^k B$, $k = 1, 2, \ldots$, или другими словами, если p-высоты элементов из B одинаковы в B и в A.

Короткая точная последовательность

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

называется *чисто точной*, если $\operatorname{Im} \alpha$ — чистая подгруппа группы B.

Группа X называется *чисто проективной*, если она проективна относительно класса чисто точных последовательностей, т.е. если каждая диаграмма

$$\begin{array}{ccccccc} & & & & & & X \\ & & & & & & \downarrow \\ 0 & \to & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \to 0 \end{array}$$

с чисто точной строкой может быть пополнена соответствующим гомоморфизмом $\psi\colon X \to B$ так, что получающаяся диаграмма коммутативна.

Группа Y называется *чисто инъективной*, если всякая диаграмма

$$\begin{array}{ccccccc} 0 & \to & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \to 0 \\ & & \downarrow & & & & \\ & & Y & & & & \end{array}$$

с чисто точной строкой может быть вложена в коммутативную диаграмму при соответствующем выборе гомоморфизма $\psi\colon B \to Y$.

Система $\{a_i \mid i \in I\}$ ненулевых элементов группы A называется *p-независимой*, если для любой конечной подсистемы $a_1, \ldots, a_k$ и любого натурального r из

$$n_1 a_1 + \ldots + n_k a_k \in p^r A \quad (n_i a_i \neq 0,\ n_i \in \mathbb{Z})$$

следует, что p^r делит все n_i $(i = 1, \ldots, k)$.

Подгруппа B группы A называется *p-базисной* (p — фиксированное простое число), если выполняются следующие три условия:

1) B является прямой суммой циклических p-групп и бесконечных циклических групп;

2) B есть p-чистая подгруппа группы A;

3) факторгруппа A/B является p-делимой группой.

Базис подгруппы B называется *p-базисом* группы A.

Если A есть p-группа, а $q \neq p$ — простое число, то A имеет лишь одну q-базисную подгруппу, а именно 0. Поэтому в случае p-групп p-базисные подгруппы называются просто *базисными*.

Для данного простого числа p все p-базисные подгруппы группы A изоморфны. Кроме того, базисная подгруппа p-группы A является эндоморфным образом группы A.

Если B — некоторая p-базисная подгруппа группы A, то, собрав в разложении группы B циклические прямые слагаемые одного и того же порядка, можно образовать прямую сумму $B = B_0 \oplus B_1 \oplus \ldots \oplus B_n \oplus \ldots$, где $B_0 \cong$

$\bigoplus_{m_0} \mathbb{Z}$, $B_k \cong \bigoplus_{m_k} \mathbb{Z}_{p^k}$ ($k \in \mathbb{N}$). Согласно вышесказанному, кардинальные числа m_0 и m_k ($k = 1, 2, \dots$) являются инвариантами группы A.

Системой уравнений над группой A называется совокупность уравнений $\sum_{j\in J} n_{ij}x_j = a_i$ ($a_i \in A$, $i \in I$), где $n_{ij} \in \mathbb{Z}$, причем $n_{ij} = 0$ при каждом фиксированном i для почти всех j. Здесь $\{x_j\}_{j\in J}$ — множество неизвестных, а I и J — множества индексов произвольной мощности; $\{x_j = b_j \,|\, b_j \in A,\ j \in J\}$ называется *решением* вышеприведенной системы, если $\sum_{j\in J} n_{ij}b_j = a_i$ для каждого $i \in I$, т.е. если каждое уравнение системы превращается в тождество при замене x_j элементами b_j.

Группа A называется *алгебраически компактной*, если она служит прямым слагаемым всякой группы, содержащей ее в качестве чистой подгруппы. Справедлива

Теорема 20.1. *Следующие условия для группы A эквивалентны*:

а) *A чисто инъективна*;

б) *A алгебраически компактна*;

в) *A — прямое слагаемое прямого произведения коциклических групп*;

г) *A в алгебраическом смысле является прямым слагаемым группы, допускающей компактную топологию*;

д) *если всякая конечная подсистема системы уравнений над A имеет решение в A, то и вся система уравнений разрешима в A.*

Задачи

20.1. 1) Если G является p-чистой подгруппой группы A для каждого простого числа p, то G чиста в A.

2) p-чистая p-подгруппа всегда чиста.

3) Если A есть p-группа, G — ее чистая подгруппа и $G[p] = A[p]$, то $G = A$.

20.2. 1) Если факторгруппа A/B является группой без кручения, то B — чистая подгруппа в A.

2) В группе без кручения пересечение любого семейства чистых подгрупп является чистой подгруппой.

3) Чистота является индуктивным свойством.

4) Если C — чистая подгруппа в чистой подгруппе B группы A, то C — чистая подгруппа в A.

5) Если подгруппа B чиста в A и $C \subset B$, то подгруппа B/C чиста в A/C.

6) Если подгруппа C чиста в A, $C \subset B$ и подгруппа B/C чиста в A/C, то подгруппа B чиста в A.

7) Если $G \cap H$ и $G + H$ — чистые подгруппы группы A, то G и H — также чистые подгруппы в A.

20.3. 1) Подгруппа H группы без кручения G чиста в G тогда и только тогда, когда G/H — группа без кручения.

2) Для всякой группы G факторгруппа $G/t(G)$ является группой без кручения и, значит, подгруппа $t(G)$ чиста в G.

20.4. Для каких групп A каждая подгруппа чиста (есть прямое слагаемое) в A?

20.5. Всякую бесконечную подгруппу можно вложить в чистую подгруппу той же мощности, а всякую конечную подгруппу — в конечную или счетную чистую подгруппу.

20.6. Пусть G — чистая подгруппа группы A. Тогда:

а) подгруппа $G + t(A)$ чиста в A;

б) $G^1 = G \cap A^1$;

в) $(G + A^1)/A^1$ — чистая подгруппа группы A/A^1.

20.7. Пусть H — A^1-высокая подгруппа в A. Тогда H является такой чистой подгруппой в A, что факторгруппа A/H делима и подгруппа $(H + A^1)/H$ существенна в ней.

20.8. Пусть подгруппа B группы A является прямой суммой циклических групп одного и того же порядка p^k. Эквивалентны следующие утверждения:

а) B — чистая подгруппа группы A;

б) для B выполнено равенство $B \cap p^kA = 0$;

в) B — прямое слагаемое группы A.

20.9. 1) Всякий элемент порядка p и конечной высоты можно вложить в конечное циклическое прямое слагаемое группы.

2) Если группа содержит элементы конечного порядка, то она обладает коциклическим прямым слагаемым.

3) Неразложимая периодическая группа является коциклической.

4) Данная группа чиста во всякой содержащей ее группе тогда и только тогда, когда она — делимая группа.

20.10. Всякая ограниченная чистая подгруппа является прямым слагаемым группы.

20.11. Для любого простого числа p и натурального n всякая p^nA-высокая подгруппа группы A служит для A прямым слагаемым.

Подгруппа G группы A называется *слабо чистой*, если $pG = G \cap pA$ при любом простом p.

20.12. 1) Приведите пример слабо чистой, но не чистой подгруппы.

2) В группах без кручения чистота эквивалентна слабой чистоте.

3) Подгруппа G слабо чиста тогда и только тогда, когда G/pG служит прямым слагаемым для группы A/pG.

4) Если подгруппа G слабо чиста в A и либо G, либо A/G — элементарная p-группа, то G — прямое слагаемое в A.

20.13. Группа не имеет нетривиальных чистых подгрупп тогда и только тогда, когда она изоморфна какой-то подгруппе группы $\mathbb{Q}$ или $\mathbb{Z}_{p^\infty}$.

20.14. В группе выполняется условие максимальности (минимальности) для чистых подгрупп тогда и только тогда, когда эта группа имеет конечный ранг.

20.15. Если G — чистая подгруппа группы A, равной $B \oplus C$, причем $G \cap C$ является существенной подгруппой и в C, и в G, то $A = B \oplus G$.

20.16. Подгруппа B группы A чиста тогда и только тогда, когда каждый смежный класс группы A по подгруппе B содержит элемент того же порядка, что и этот смежный класс.

20.17. Если B — чистая подгруппа группы A и A/B — прямая сумма циклических групп, то B — прямое слагаемое группы A.

20.18. Для подгруппы B группы A эквивалентны условия:

а) подгруппа B чиста в A;

б) подгруппа B служит прямым слагаемым для $n^{-1}B = \{a \in A \,|\, na \in B\}$ при любом натуральном числе n;

в) если C — группа, лежащая между B и A, и C/B — конечно порожденная группа, то B служит для C прямым слагаемым.

20.19. 1) $\Phi(A/\Phi(A)) = 0$ для любой группы A.

2) $\Phi(A) = 0$ в точности тогда, когда группа A изоморфна некоторой слабо чистой подгруппе прямого произведения элементарных p-групп.

20.20. Если система уравнений

$$\sum_{j=1}^{m} n_{ij}x_j = b_i \quad (b_i \in B,\ i \in I)$$

над чистой подгруппой B группы A, содержащая конечное число m неизвестных, имеет решение в группе A, то она имеет решение и в группе B.

20.21. 1) Чистота подгруппы B в группе A равносильна справедливости равенства $n^{-1}B = B + n^{-1}0$ для каждого $n \in \mathbb{N}$.

2) Если B — чистая подгруппа группы A, то $(A/B)[n] \cong A[n]/B[n]$ для каждого $n \in \mathbb{N}$.

20.22. Точная последовательность

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

чисто точна тогда и только тогда, когда каждая коциклическая группа (циклическая группа) G инъективна (проективна) относительно нее, т.е. для всякой коциклической группы (циклической группы) G диаграмма а) (диаграмма б))

$$\text{а)}\quad \begin{array}{ccccccc} 0 \to & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \to 0, \\ & \downarrow\varphi & & & & & \\ & G & & & & & \end{array} \qquad\qquad \text{б)}\quad \begin{array}{ccccccc} & & & & & G & \\ & & & & & \downarrow\varphi & \\ 0 \to & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \to 0 \end{array}$$

может быть вложена в коммутативную диаграмму при соответствующем выборе гомоморфизма $\psi\colon B \to G$ ($\psi\colon G \to B$).

20.23. Для любой группы A существует такая прямая сумма циклических групп $X = \bigoplus\limits_{i\in I}\langle x_i\rangle$ и такой эпиморфизм $\eta\colon X \to A$, что $\operatorname{Ker}\eta$ — чистая подгруппа группы X.

20.24. Группа чисто проективна тогда и только тогда, когда она — прямая сумма циклических групп.

20.25. Всякую группу можно вложить в качестве чистой подгруппы в прямое произведение коциклических групп.

20.26. Группа чисто инъективна тогда и только тогда, когда она — прямое слагаемое прямого произведения коциклических групп.

20.27. 1) Любая p-независимая система обязательно независима.

2) p-независимая система содержит только элементы бесконечного порядка и порядков, равных степеням данного простого p.

3) Подгруппа, порожденная p-независимой системой элементов группы A, p-чиста в A.

4) Если независимая система элементов, содержащая только элементы бесконечного порядка и порядков, равных степеням простого числа p, порождает p-чистую подгруппу, то эта система элементов p-независима.

20.28. Система элементов $\{a_i \mid i \in I\}$ служит p-базисом для группы A в точности тогда, когда она является максимальной p-независимой системой в A. Следовательно, всякая группа для любого простого p содержит p-базисные подгруппы.

20.29. 1) p-базисной подгруппой группы $\widehat{\mathbb{Z}}_p$ является подгруппа $\mathbb{Z}$.

2) Если B_i есть p-базисная подгруппа группы A_i при $i \in I$, то $\bigoplus\limits_{i\in I} B_i$ является p-базисной подгруппой группы $\bigoplus\limits_{i\in I} A_i$.

3) Всякая p-базисная подгруппа p-чистой подгруппы группы A служит прямым слагаемым для некоторой p-базисной подгруппы группы A.

20.30. Пусть A — произвольная группа, B — ее p-базисная подгруппа. Тогда:

а) $A = B + p^nA$, $B/p^nB \cong A/p^nA$ и $p^nA/p^nB \cong A/B$ для любого целого $n \geqslant 0$;

б) если B' есть p-базисная подгруппа в B, то B' является p-базисной подгруппой группы A;

в) если $\varphi\colon A \to A_0 = A/A^1$ — канонический эпиморфизм, то $B_0 = \varphi(B)$ является p-базисной подгруппой группы A_0, причем φ индуцирует изоморфизм между B и B_0.

20.31. Если A — редуцированная группа и B_p для каждого простого числа p — ее p-базисная подгруппа, то $|A| \leqslant (\sum\limits_p |B_p|)^{\aleph_0}$ и $|A| \leqslant |A_0|^{\aleph_0}$, где $A_0 = A/A^1$.

20.32. 1) Прямое слагаемое алгебраически компактной группы также является алгебраически компактной группой.

2) Группа алгебраически компактна тогда и только тогда, когда ее редуцированная часть алгебраически компактна.

3) Редуцированная алгебраически компактная группа является прямым слагаемым прямого произведения циклических p-групп.

4) Всякую группу можно вложить в качестве чистой подгруппы в некоторую алгебраически компактную группу.

20.33. Группа A алгебраически компактна тогда и только тогда, когда A служит прямым слагаемым для всякой такой группы G, что A — чистая подгруппа группы G, а факторгруппа G/A изоморфна группе $\mathbb{Q}$ или некоторой группе $\mathbb{Z}_{p^\infty}$.

20.34. Группа A алгебраически компактна тогда и только тогда, когда A служит прямым слагаемым для всякой группы G, в которой A содержится в качестве замкнутой в $\mathbb{Z}$-адической топологии чистой подгруппы.

20.35. Если A — алгебраически компактная группа и B — чистая подгруппа группы A, то A/B — алгебраически компактная группа.

20.36. Группа полна в $\mathbb{Z}$-адической топологии тогда и только тогда, когда она — редуцированная алгебраически компактная группа.

20.37. Пусть полная (в $\mathbb{Z}$-адической топологии) группа A содержится в прямой сумме $\bigoplus\limits_{i\in I} C_i$ таких групп C_i, что $C_i^1 = 0$ для каждого i. Тогда существует такое целое число $n > 0$, что подгруппа nA содержится в прямой сумме конечного числа групп C_i. В частности, если $A = \bigoplus\limits_{i\in I} C_i$ — прямое разложение полной группы A, то все C_i — полные группы и существует такое целое число $n > 0$, что $nC_i = 0$ для почти всех $i \in I$.

20.38. Если C — чистая подгруппа полной группы A, то замыкание (в $\mathbb{Z}$-адической топологии) подгруппы C в A служит для A прямым слагаемым.

20.39. Опишите $\mathbb{Z}$-адические пополнения групп: $\mathbb{Z}$, $\mathbb{Q}_p$, $\mathbb{Q}^{(p)}$, $\bigoplus\limits_{n=1}^{\infty} \mathbb{Z}_{p^n}$, $\bigoplus\limits_p \mathbb{Z}_p$.

20.40. $\mathbb{Z}$-адическое пополнение прямого произведения является прямым произведением $\mathbb{Z}$-адических пополнений компонент.

20.41. Если группа A полна в своей p-адической топологии, то $qA = A$ для каждого простого числа $q \neq p$, а A является *p-адическим модулем*, т.е. модулем над кольцом $\widehat{\mathbb{Z}}_p$.

20.42. Редуцированная группа A алгебраически компактна тогда и только тогда, когда она имеет вид $A = \prod\limits_p A_p$ (произведение берется по всем различным простым числам p), где каждая группа A_p полна в своей p-адической топологии. A_p однозначно определяется группой A, в силу 20.41 она является p-адическим модулем.

Группа A_p из 20.42 называется *p-адической компонентой группы A*. Говорят также, что A_p — *p-адическая алгебраически компактная группа*, подчеркивая то обстоятельство, что A_p — полный в p-адической топологии p-адический модуль. Поэтому группы A_p могут быть охарактеризованы теми же системами инвариантов, что и их базисные подгруппы; а именно каждая A_p изоморфна p-адическому пополнению группы $\bigoplus\limits_{m_0} \mathbb{Z} \oplus \bigoplus\limits_{k=1}^{\infty} \bigoplus\limits_{m_k} \mathbb{Z}_{p^k}$.

Ввиду этого утверждения счетная система кардинальных чисел m_0 и m_k ($k = 1, 2, \dots$) является полной независимой системой инвариантов группы A_p, зная которую, можно восстановить группу A_p, взяв сначала соответствующую прямую сумму и затем p-адическое пополнение: группа A_p изоморфна p-адическому пополнению группы $\bigoplus\limits_{m_0} \mathbb{Z} \oplus \bigoplus\limits_{k=1}^{\infty} \bigoplus\limits_{m_k} \mathbb{Z}_{p^k}$. Если A — произвольная алгебраически компактная группа, то инварианты ее максимальной делимой подгруппы (см. 19.59) вместе с инвариантами ее p-адических компонент образуют полную и независимую систему инвариантов группы A.

20.43. Пусть $m \geqslant \aleph_0$. Тогда группа $\prod\limits_m \widehat{\mathbb{Z}}_p$ изоморфна p-адическому пополнению группы $\bigoplus\limits_{2^m} \widehat{\mathbb{Z}}_p$.

20.44. Пусть m_k ($k = 1, 2, \dots$) — какие-то кардинальные числа. Тогда группа $\prod\limits_{k=1}^{\infty} (\bigoplus\limits_{m_k} \mathbb{Z}_{p^k})$ изоморфна p-адическому пополнению группы $\bigoplus\limits_m \widehat{\mathbb{Z}}_p \oplus \bigoplus\limits_{k=1}^{\infty} \bigoplus\limits_{m_k} \mathbb{Z}_{p^k}$, где $m = \prod\limits_{k=1}^{\infty} m_k$.

20.45. 1) Если редуцированная алгебраически компактная группа является периодической, то она ограничена.

2) Всякая редуцированная алгебраически компактная группа обладает прямым слагаемым, изоморфным группе $\widehat{\mathbb{Z}}_p$ или $\mathbb{Z}_{p^k}$ ($k = 1, 2, \dots$) при некотором p.

20.46. Согласно 20.32 всякую группу A можно вложить в качестве чистой подгруппы в некоторую алгебраически компактную группу G. Выделим в G алгебраически компактную группу F такую, что делимая часть F совпадает с инъективной оболочкой подгруппы A^1 и F/A — делимая группа. Группа F определена однозначно с точностью до изоморфизма над A. Группа F называется *чисто инъективной оболочкой группы A*. Чисто инъективная оболочка группы A изоморфна прямой сумме инъективной оболочки группы A^1 и пополнения в $\mathbb{Z}$-адической топологии группы $A_0 = A/A^1$.

20.47. Пусть C — алгебраически компактная группа, содержащая группу G в качестве чистой подгруппы. Тогда чисто инъективная оболочка A группы G, лежащая в группе C, выделяется в C прямым слагаемым.

20.48. 1) Если A и A' — алгебраически компактные группы, каждая из которых изоморфна чистой подгруппе другой, то $A \cong A'$.

2) Если A — такая алгебраически компактная группа, что $A \oplus \widehat{\mathbb{Z}}_p \cong A' \oplus \widehat{\mathbb{Z}}_p$ или $A \oplus A \cong A' \oplus A'$, то $A \cong A'$.

21 Группы гомоморфизмов

О гомоморфизмах модулей и абелевых групп уже говорилось в параграфах 15 и 19. Еще раз укажем, что если α и β — гомоморфизмы группы A в группу C, то их сумма $\alpha + \beta$, определяемая равенством $(\alpha + \beta)a = \alpha a + \beta a$ ($a \in A$), снова является гомоморфизмом A в C. Все гомоморфизмы группы A в C образуют абелеву группу. Она называется *группой гомоморфизмов* группы A в группу C и обозначается через $\mathrm{Hom}_{\mathbb{Z}}(A, C)$ или просто $\mathrm{Hom}(A, C)$.

Группа $\mathrm{Hom}(A, A) = \mathrm{End}\, A$ называется *группой эндоморфизмов* группы A. Группу $\mathrm{End}\, A$ можно превратить в кольцо (оно рассматривается в § 26, см. также 8.1).

В начале § 18 уже были определены категории и функторы. Сделаем небольшие добавления.

Пусть F и G — ковариантные функторы из категории $\mathcal{E}$ в категорию $\mathcal{R}$. *Естественным преобразованием* $\Phi\colon F \to G$ называется функция, ставящая в соответствие каждому объекту $A \in \mathcal{E}$ морфизм $\varphi_A\colon F(A) \to G(A)$ из $\mathcal{R}$ таким

образом, что для любого морфизма $\alpha\colon A \to B$ категории $\mathcal{E}$ диаграмма (в $\mathcal{R}$)

$$\begin{array}{ccc} F(A) & \xrightarrow{F(\alpha)} & F(B) \\ \downarrow \varphi_A & & \downarrow \varphi_B \\ G(A) & \xrightarrow{G(\alpha)} & G(B) \end{array}$$

коммутативна. В таком случае φ_A называется *естественным* морфизмом между $F(A)$ и $G(A)$. Если φ_A является изоморфизмом для всякого $A \in \mathcal{E}$, то Φ называется *естественной эквивалентностью*.

Ясно, что абелевы группы и их гомоморфизмы образуют *категорию $\mathcal{A}b$ всех абелевых групп*, периодические абелевы группы, группы без кручения и их гомоморфизмы также образуют категории.

Если F — ковариантный функтор из категории $\mathcal{A}b$ в категорию $\mathcal{A}b$ (вместо $\mathcal{A}b$ можно брать ее подкатегории) и $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ — точная последовательность, то функтор F называется *точным слева* или *справа*, если точна последовательность $0 \to F(A) \xrightarrow{F(\alpha)} F(B) \xrightarrow{F(\beta)} F(C)$ или последовательность $F(A) \xrightarrow{F(\alpha)} F(B) \xrightarrow{F(\beta)} F(C) \to 0$ соответственно. Функтор, точный справа и слева, называется *точным*.

Функтор $F\colon \mathcal{A}b \to \mathcal{A}b$ называется *аддитивным*, если $F(\alpha+\beta) = F(\alpha) + F(\beta)$ для всех $\alpha, \beta \in \mathcal{A}b$, для которых $\alpha+\beta$ определено.

Пусть дана функция, ставящая в соответствие каждой группе $A \in \mathcal{A}b$ такую ее подгруппу $F(A)$, что если $\alpha\colon A \to B$ — гомоморфизм группы A в группу B, то $\alpha F(A) \subseteq F(B)$, т.е. ограничение $\alpha|\,F(A)$ отображает $F(A)$ в $F(B)$. Тогда если положить $F(\alpha) = \alpha|F(A)$, то F будет функтором $\mathcal{A}b \to \mathcal{A}b$ (говорят еще, что F — предрадикал). $F(A)$ называют *функторной подгруппой* группы A.

Пусть теперь F^* — соответствие, сопоставляющее каждой группе $A \in \mathcal{A}b$ такую факторгруппу A/A^*, что если $\alpha\colon A \to B$ — гомоморфизм, то $a + A^* \mapsto \alpha a + B^*$ — гомоморфизм группы A/A^* в B/B^*. Соответствие $F^*\colon \mathcal{A}b \to \mathcal{A}b$ обладает функторными свойствами, $F^*(A) = A/A^*$ называют *функторной факторгруппой* группы A.

Если F_1 и F_2 — такие функторы $\mathcal{A}b \to \mathcal{A}b$, что $F_1(A) \subseteq F_2(A) \subseteq A$ для любой группы $A \in \mathcal{A}b$, то пишут $F_1 \leqslant F_2$ и называют F_1 *подфунктором* функтора F_2. Отношение $\leqslant$ между функторами заданного типа определяет частичный порядок в классе $\mathcal{F}$ этих функторов. В $\mathcal{F}$ отношение $\leqslant$ на самом деле задает решеточный порядок. Если $F_1, F_2 \in \mathcal{F}$, то отображения $A \mapsto F_1(A) \cap F_2(A)$ и $A \mapsto F_1(A) + F_2(A)$ порождают подфункторы тождественного функтора, представляющие собой $\inf(F_1, F_2)$ и $\sup(F_1, F_2)$. Эти подфункторы обозначают, соответственно, через $F_1 \wedge F_2$ и $F_1 \vee F_2$.

Задачи

21.1. Функтор GF ковариантен, если F и G одновременно ковариантны или контравариантны; и контравариантен, если один из функторов F, G ковариантен, а второй контравариантен.

21.2. Дайте определение точного контравариантного функтора.

21.3. $F(0) = 0$ для аддитивного функтора $F\colon \mathcal{A}b \to \mathcal{A}b$, где 0 обозначает нулевую группу или нулевой гомоморфизм. Кроме того, $F(n\alpha) = nF(\alpha)$ для любого целого n.

21.4. Отображение $T\colon \mathcal{A}b \to \mathcal{B}$ из категории $\mathcal{A}b$ в категорию $\mathcal{B}$ всех периодических групп является функтором, где $T(A)$ для $A \in \mathcal{A}b$ — периодическая часть $t(A)$ группы A, а $T(\alpha)$ для $\alpha\colon A \to B$ из $\mathcal{A}b$ — ограничение $\alpha\,|\,t(A)\colon\ t(A) \to t(B)$. Подгруппа $T(A)$ является функторной.

21.5. Если взять цоколь $\operatorname{Soc} A$ группы A, то так же, как в 21.4, получится функтор $S\colon \mathcal{A}b \to \mathcal{B}$.

21.6. Получится функтор $M_n\colon \mathcal{A}b \to \mathcal{A}b$, если группе A поставить в соответствие ее подгруппу nA, где n — натуральное число, а гомоморфизму $\alpha\colon A \to B$ — индуцированный гомоморфизм $\alpha\,|\,nA\colon nA \to nB$.

21.7. Пусть $\mathcal{E}$ — категория групп без кручения. Отображение $\alpha^*\colon a + t(A) \mapsto \alpha a + t(B)$ не зависит от выбора элемента a в определяемом им смежном классе по подгруппе $t(A)$. Функтором из $\mathcal{A}b$ в $\mathcal{E}$ является функция, ставящая в соответствие группе $A \in \mathcal{A}b$ факторгруппу $A/t(A)$ и гомоморфизму $\alpha\colon A \to B$ из $\mathcal{A}b$ — индуцированный гомоморфизм α^*.

21.8. Пусть $\mathcal{A}_n$ — категория *n-ограниченных* групп, т.е. таких групп G, что $nG = 0$. Получается функтор, если поставить в соответствие группе A подгруппу $A\,[n]$, а гомоморфизму $\alpha\colon A \to B$ — его ограничение $\alpha\,|\,A\,[n]$.

21.9. Получается функтор $\mathcal{A}b \to \mathcal{A}_n$, если положить $A \mapsto A/nA$ для всех $A \in \mathcal{A}b$ и $\alpha \mapsto \alpha_*$ для $\alpha\colon A \to B$ из $\mathcal{A}b$, где α_* — индуцированный гомоморфизм $a + nA \mapsto \alpha a + nB$.

21.10. 1) $F(A)$ является функторной подгруппой группы A, если и только если $A/F(A)$ есть функторная факторгруппа группы A.

2) $F(\bigoplus\limits_i A_i) = \bigoplus\limits_i F(A_i)$ для подфунктора F тождественного функтора; кроме того, из $C \subseteq A$ следует, что

$$F(C) \subseteq C \cap F(A), \quad (F(A) + C)/C \subseteq F(A/C).$$

21.11. Пусть Δ — класс групп X. С каждой группой $A \in \mathcal{A}b$ свяжем две подгруппы: $V_\Delta(A) = \bigcap\limits_{\varphi} \operatorname{Ker}\varphi$, где $\varphi\colon A \to X \in \Delta$, и $W_\Delta(A) = \sum\limits_{\psi} \operatorname{Im}\psi$, где $\psi\colon X \to A$ $(X \in \Delta)$. Покажите, что V_Δ и W_Δ, где класс Δ фиксирован, являются функторами из категории $\mathcal{A}b$ в категорию $\mathcal{A}b$.
Найдите $V_\Delta(A)$ и $W_\Delta(A)$, если Δ состоит из следующих классов групп:

а) циклических групп порядка p, где p пробегает все простые числа;

б) всех конечных циклических групп;

в) одной фиксированной группы $\mathbb{Z}_m$;

г) одной группы $\mathbb{Q}$.

21.12. Пусть Δ и Ω — два класса групп. Покажите, что:

а) если $\Delta \subseteq \Omega$, то $V_\Omega \leqslant V_\Delta$ и $W_\Delta \leqslant W_\Omega$;

б) $V_{\Delta\cup\Omega} = V_\Delta \wedge V_\Omega$ и $W_{\Delta\cup\Omega} = W_\Delta \vee W_\Omega$.

21.13. Докажите, что $\operatorname{Hom}(A, C) = 0$ в следующих случаях:

а) A — периодическая группа, C — группа без кручения;

б) A является p-группой, а C является q-группой, где p, q — различные простые числа;

в) A — делимая группа, C — редуцированная группа;

г) A не содержит прямых слагаемых, изоморфных группе $\mathbb{Z}$, а $C \cong \mathbb{Z}$.

21.14. 1) Если $C[n] = 0$, то $\operatorname{Hom}(A, C)[n] = 0$ для любой группы A.
2) $\operatorname{Hom}(A, C)$ — группа без кручения, если C — группа без кручения.
3) $\operatorname{Hom}(A, C)$ — делимая группа без кручения, если C — делимая группа без кручения.
4) Если $nA = A$ для некоторого натурального числа n, то $\operatorname{Hom}(A, C)[n] = 0$.
5) Если A — делимая группа, то $\operatorname{Hom}(A, C)$ — группа без кручения.
6) Если A — делимая группа без кручения, то $\operatorname{Hom}(A, C)$ — также делимая группа без кручения.
7) Если A — группа без кручения, C — делимая группа, то $\operatorname{Hom}(A, C)$ — делимая группа.

21.15. Опишите следующие группы:

а) $\operatorname{Hom}(\mathbb{Z}_{p^m}, \mathbb{Z}_{p^n})$; б) $\operatorname{Hom}(A, \mathbb{Z}_m)$;

в) $\operatorname{Hom}(\mathbb{Q}, \mathbb{C})$; г) $\operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$;

д) $\operatorname{Hom}\left(\widehat{\mathbb{Z}}_p, \mathbb{Z}_{p^\infty}\right)$.

21.16. Приведите примеры групп без кручения A, C, для которых $\operatorname{Hom}(A, C) = 0 = \operatorname{Hom}(C, A)$.

21.17. Существуют естественные изоморфизмы:

а) $\operatorname{Hom}\left(\bigoplus\limits_{i\in I} A_i, C\right) \cong \prod\limits_{i\in I} \operatorname{Hom}(A_i, C)$;

б) $\operatorname{Hom}\left(A, \prod\limits_{i\in I} C_i\right) \cong \prod\limits_{i\in I} \operatorname{Hom}(A, C_i)$.

21.18. Если $A = \bigoplus\limits_{m} \mathbb{Z} \oplus \bigoplus\limits_{p} \left(\bigoplus\limits_{k=1}^{\infty} \left(\bigoplus\limits_{m_{p,\,k}} \mathbb{Z}_{p^k}\right)\right)$, то $\operatorname{Hom}(A, C) \cong \prod\limits_{m} C \oplus \prod\limits_{p} \prod\limits_{k=1}^{\infty} \prod\limits_{m_{p,\,k}} C[p^k]$.

21.19. 1) Если A — периодическая группа с p-компонентами A_p, а C_p — это p-компоненты группы C, то $\operatorname{Hom}(A, C) \cong \prod\limits_{p} \operatorname{Hom}(A_p, C_p)$.
2) Для любой группы A имеет место изоморфизм $\operatorname{Hom}(A, \mathbb{Q}) \cong \prod\limits_{n} \mathbb{Q}$, где $n = r_0(A)$.

21.20. Пусть A и C — редуцированные алгебраически компактные группы, A_p и C_p — их p-адические компоненты (см. 20.42). Имеет место изоморфизм $\operatorname{Hom}(A, C) \cong \prod\limits_{p} \operatorname{Hom}(A_p, C_p)$.

21.21. 1) Если A — периодическая группа, то теоретико-множественное объединение $\cup \operatorname{Im}\alpha$, где α пробегает всю группу $\operatorname{Hom}(A, C)$, является подгруппой группы C.

2) Утверждение 1) справедливо не всегда, если A — группа без кручения.

21.22. Индуцированные гомоморфизмы для Hom, введенные в начале § 15, можно объединить следующим образом. Пусть $\alpha\colon A' \to A$ и $\gamma\colon C \to C'$ — фиксированные гомоморфизмы. Покажите, что соответствие $\eta \mapsto \gamma\eta\alpha$ есть гомоморфизм группы $\operatorname{Hom}(A, C)$ в $\operatorname{Hom}(A', C')$, который обозначается через $\operatorname{Hom}(\alpha, \gamma)\colon \operatorname{Hom}(A, C) \to \operatorname{Hom}(A', C')$. $\operatorname{Hom}(1_A, 1_C) = 1_{\operatorname{Hom}(A,C)}$ и $\operatorname{Hom}(\alpha\alpha', \gamma'\gamma) = \operatorname{Hom}(\alpha', \gamma')\operatorname{Hom}(\alpha, \gamma)$. Кроме того, $\operatorname{Hom}(\alpha, \gamma)$ аддитивен по α и γ. Следовательно, Hom есть аддитивный бифунктор из категории $\mathcal{A}b \times \mathcal{A}b$ в категорию $\mathcal{A}b$, контравариантный по первому и ковариантный по второму аргументу.

21.23. Обозначим, как в § 15, $\alpha^* = \operatorname{Hom}(\alpha, 1_C)$ и $\gamma_* = \operatorname{Hom}(1_A, \gamma)$. Пусть (1): $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ — короткая точная последовательность. Тогда для любой группы G точны индуцированные последовательности (см. 15.48):

(2) $0 \to \operatorname{Hom}(C, G) \xrightarrow{\beta^*} \operatorname{Hom}(B, G) \xrightarrow{\alpha^*} \operatorname{Hom}(A, G)$,

(3) $0 \to \operatorname{Hom}(G, A) \xrightarrow{\alpha_*} \operatorname{Hom}(G, B) \xrightarrow{\beta_*} \operatorname{Hom}(G, C)$.

Кроме того, для любой точной последовательности (1) последовательность (2) (соответственно, последовательность (3)) с отображением $\to 0$ в конце точна тогда и только тогда, когда G — делимая (соответственно, — свободная) группа.

21.24. 1) Если последовательность (1) в 21.23 чисто точна, то последовательности (2) и (3) также чисто точны.

2) Если группа G фиксирована, то для любой чисто точной последовательности (1) последовательность (2) (последовательность (3)) остается точной при добавлении в конце отображения $\to 0$ тогда и только тогда, когда группа G алгебраически компактна (является прямой суммой циклических групп); с этими утверждениями связаны теорема в § 20 и упражнения 20.22, 20.24.

21.25. Для кардинального числа m найдите строение групп:

а) $\operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, \bigoplus\limits_m \mathbb{Q}/\mathbb{Z})$ и $\operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, \prod\limits_m \mathbb{Q}/\mathbb{Z})$;

б) $\operatorname{Hom}(\bigoplus\limits_m \mathbb{Q}, \bigoplus\limits_m \mathbb{Q})$ и $\operatorname{Hom}(\bigoplus\limits_m \widehat{\mathbb{Z}}_p, \bigoplus\limits_m \widehat{\mathbb{Z}}_p)$.

21.26. Если группа A — периодическая, то $\operatorname{Hom}(A, G)$ — редуцированная алгебраически компактная группа для любой группы G.

21.27. Пусть A, C — периодические группы, B — базисная подгруппа группы A, а C — редуцированная группа. Не теряя общности, можно считать A и C p-группами. Покажите, что $\operatorname{Hom}(A, C)$ можно рассматривать как подгруппу группы $\operatorname{Hom}(B, C)$. Кроме того, если C не имеет элементов бесконечной высоты, то $\operatorname{Hom}(B, C) = \operatorname{Hom}(A, C) \oplus X$, где X есть p-адическая алгебраически компактная группа без кручения.

Пусть A, C — p-группы. Гомоморфизм $\varphi\colon A \to C$ называется *малым*, если

($*$) для любого $k \geqslant 0$ существует такое n, что при всяком $a \in A$ из $e(a) \leqslant k$ и $h_p(a) \geqslant n$ следует $\varphi a = 0$, т.е. $\varphi(p^n A[p^k]) = 0$, где $p^n A[p^k] = \{x \in p^n A \mid p^k x = 0\}$.

21.28. 1) Малые гомоморфизмы полностью определяются своим действием на базисной подгруппе B группы A.

2) Малые гомоморфизмы группы A в C образуют подгруппу $\operatorname{Small}(A, C)$ группы $\operatorname{Hom}(A, C)$, причем факторгруппа $\operatorname{Hom}(A, C)/\operatorname{Small}(A, C)$ является p-адической алгебраически компактной группой без кручения. Все малые эндоморфизмы группы A составляют идеал $\operatorname{Small} A$ кольца $\operatorname{End} A$.

21.29. Пусть $B = \bigoplus\limits_{i \in I} \langle a_i \rangle$ — базисная подгруппа p-группы A, и пусть для элементов $c_i \in C$ ($i \in I$) выполнено: а) $e(c_i) \leqslant e(a_i)$; б) для любого $k \geqslant 0$ существует такое n, что если $e(c_i) \geqslant n$, то $e(c_i) \leqslant e(a_i) - k$. Тогда существует однозначно определенный малый гомоморфизм φ группы A в группу C, при котором $\varphi(a_i) = c_i$ ($i \in I$).

21.30. Пусть G — чистая подгруппа p-группы A. Всякий малый гомоморфизм группы G в группу C можно продолжить до гомоморфизма группы A в C.

Группа A называется *самомалой*, если образ всякого гомоморфизма $\varphi\colon A \to \oplus_{i \in I} A_i$, где все группы $A_i \cong A$, I — произвольное индексное множество, содержится в сумме конечного числа некоторых слагаемых A_i.

21.31. 1) Конечно порожденная группа является самомалой, а квазициклическая группа $\mathbb{Z}_{p^\infty}$ — нет.

2) Прямое слагаемое самомалой группы будет самомалой группой.

3) Самомалая группа не может разлагаться в прямую сумму бесконечного числа прямых слагаемых.

22 Группы расширений. Тензорные и периодические произведения

Если даны группы A и C, то *проблема расширений* состоит в нахождении таких групп B, что B содержит подгруппу A', изоморфную A, причем $B/A' \cong C$. Это может быть записано с помощью короткой точной последовательности $E\colon 0 \to A \xrightarrow{\mu} B \xrightarrow{\nu} C \to 0$, где μ — вложение, ν — эпиморфизм с ядром μA. В этом случае говорят, что группа B является *расширением группы A при помощи группы C*. Если дана еще одна точная последовательность $E'\colon 0 \to A' \xrightarrow{\mu'} B' \xrightarrow{\nu'} C' \to 0$, то под *морфизмом* E в E' понимается тройка (α, β, γ) групповых гомоморфизмов, для которых диаграмма (1)

$$\begin{array}{lccccc} E\colon 0 \to & A & \xrightarrow{\mu} & B & \xrightarrow{\nu} & C \to 0 \\ & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ E'\colon 0 \to & A' & \xrightarrow{\mu'} & B' & \xrightarrow{\nu'} & C' \to 0 \end{array}$$

коммутативна. Класс всех коротких точных последовательностей и их морфизмов определяет категорию $\mathcal{E}$. Расширения E и E', где $A = A'$, $C = C'$, называются *эквивалентными* ($E \equiv E'$), если существует морфизм $(1_A, \beta, 1_C)$, где $\beta\colon B \to B'$ — изоморфизм.

Если $\gamma\colon C' \to C$ — произвольный гомоморфизм, то существует короткая точная последовательность $E\gamma\colon 0 \to A \xrightarrow{\mu'} B' \xrightarrow{\nu'} C' \to 0$, для которой диаграмма

$$\begin{array}{lccccc} E\gamma\colon 0 \to & A & \xrightarrow{\mu'} & B' & \xrightarrow{\nu'} & C' \to 0 \\ & \downarrow 1_A & & \downarrow \beta & & \downarrow \gamma \\ E\colon\ 0 \to & A & \xrightarrow{\mu} & B & \xrightarrow{\nu} & C \to 0 \end{array}$$

коммутативна (правый квадрат в ней является коуниверсальным). Последовательность $E\gamma$ с этим свойством определяется однозначно с точностью до эквивалентности. Кроме того, $E\,1_C \equiv E$ и $E(\gamma\gamma') \equiv (E\gamma)\gamma'$ для $C'' \xrightarrow{\gamma'} C' \xrightarrow{\gamma} C$.

Для гомоморфизма $\alpha\colon A \to A'$ существует короткая точная последовательность $\alpha E\colon 0 \to A' \xrightarrow{\mu'} B' \xrightarrow{\nu'} C \to 0$, определяемая с точностью до эквивалентности, делающая коммутативной диаграмму

$$\begin{array}{lccccc} E\colon\ 0 \to & A & \xrightarrow{\mu} & B & \xrightarrow{\nu} & C \to 0 \\ & \downarrow \alpha & & \downarrow \beta & & \downarrow 1_C \\ \alpha E\colon 0 \to & A' & \xrightarrow{\mu'} & B' & \xrightarrow{\nu'} & C \to 0. \end{array}$$

Для $A \xrightarrow{\alpha} A' \xrightarrow{\alpha'} A''$ выполняется $1_A E \equiv E$ и $(\alpha\alpha')E \equiv \alpha(\alpha' E)$.

Если даны $\alpha\colon A \to A'$ и $\gamma\colon C' \to C$, то имеет место закон ассоциативности $\alpha(E\gamma) \equiv (\alpha E)\gamma$.

Под *прямой суммой* двух расширений

$$E_i\colon 0 \to A_i \xrightarrow{\mu_i} B_i \xrightarrow{\nu_i} C_i \to 0 \quad (i = 1, 2)$$

понимается расширение

$$E_1 \oplus E_2\colon 0 \to A_1 \oplus A_2 \xrightarrow{\mu_1 \oplus \mu_2} B_1 \oplus B_2 \xrightarrow{\nu_1 \oplus \nu_2} C_1 \oplus C_2 \to 0.$$

Суммой двух расширений E_1, E_2 группы A при помощи группы C служит расширение $E_1 + E_2 = \nabla_A(E_1 \oplus E_2)\Delta_C$, где $\Delta_G\colon g \mapsto (g, g)$ — *диагональное*, а $\nabla_G\colon (g_1, g_2) \mapsto g_1 + g_2$ — *кодиагональное* отображения соответствующей группы G. Эта операция сложения расширений индуцирует операцию сложения классов эквивалентных расширений группы A при помощи группы C. В результате получается абелева группа классов эквивалентных расширений. Она обозначается через $\mathrm{Ext}\,(C, A)$ и называется *группой расширений группы A при помощи группы C*.

Для гомоморфизмов $\alpha\colon A \to A'$ и $\gamma\colon C' \to C$ и расширений E_1, E_2, E группы A при помощи группы C имеют место следующие эквивалентности

$$(2)\ \alpha(E_1 + E_2) \equiv \alpha E_1 + \alpha E_2,\ (E_1 + E_2)\gamma \equiv E_1\gamma + E_2\gamma,$$

$$(3)\ (\alpha_1 + \alpha_2)E \equiv \alpha_1 E + \alpha_2 E,\ E(\gamma_1 + \gamma_2) \equiv E\gamma_1 + E\gamma_2.$$

Эквивалентность (2) выражает тот факт, что $\alpha_*\colon E \mapsto \alpha E$ и $\gamma^*\colon E \mapsto E\gamma$ — это групповые гомоморфизмы

$$\alpha_*\colon \mathrm{Ext}\,(C, A) \to \mathrm{Ext}\,(C, A'),\ \gamma^*\colon \mathrm{Ext}\,(C, A) \to \mathrm{Ext}\,(C', A),$$

а в (3) утверждается, что $(\alpha_1+\alpha_2)_*=(\alpha_1)_*+(\alpha_2)_*$ и $(\gamma_1+\gamma_2)^*=\gamma_1^*+\gamma_2^*$, т.е. соответствие

$$\operatorname{Ext}\colon C\times A\mapsto \operatorname{Ext}(C,A),\ \gamma\times\alpha\mapsto\gamma^*\alpha_*=\alpha_*\gamma^*$$

есть аддитивный бифунктор из категории $\mathcal{A}b\times\mathcal{A}b$ в категорию $\mathcal{A}b$, контравариантный по первому и ковариантный по второму аргументу.

В частности, если $\alpha\colon A\to A$ и $\gamma\colon C\to C$ — эндоморфизмы групп A и C соответственно, то αE и $E\gamma$ — снова расширения группы A при помощи C. Отображения $\alpha_*\colon E\mapsto\alpha E$ и $\gamma^*\colon E\mapsto E\gamma$ являются эндоморфизмами группы $\operatorname{Ext}(C,A)$. Следовательно, $\operatorname{Ext}(C,A)$ является бимодулем над кольцами эндоморфизмов групп A и C, действующими, соответственно, слева и справа.

Вместо $\gamma^*\alpha_*=\alpha_*\gamma^*$ используют также обозначение

$$\operatorname{Ext}(\gamma,\alpha)\colon \operatorname{Ext}(C,A)\to\operatorname{Ext}(C',A'),\ \operatorname{Ext}(\gamma,\alpha)\colon E\mapsto\alpha E\gamma.$$

Если дано расширение $E\colon 0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$, представляющее элемент группы $\operatorname{Ext}(C,A)$, и дан гомоморфизм $\eta\colon A\to G$, то ηE является расширением группы G при помощи группы C, т.е. $\eta E\in\operatorname{Ext}(C,G)$. Получается отображение $E^*\colon \operatorname{Hom}(A,G)\to\operatorname{Ext}(C,G)$, $E^*\colon\eta\mapsto\eta E$.

Аналогично гомоморфизм $\xi\colon G\to C$ позволяет из расширения E получить расширение $E\xi$ группы A при помощи группы G. Это дает гомоморфизм $E_*\colon \operatorname{Hom}(G,C)\to\operatorname{Ext}(G,A)$, где $E_*\colon\xi\mapsto E\xi$. Гомоморфизмы E^* и E_* называются *связывающими гомоморфизмами*. Это оправдывается следующим фактом. Если $0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$ — точная последовательность, то последовательности

$$0\to\operatorname{Hom}(C,G)\to\operatorname{Hom}(B,G)\to\operatorname{Hom}(A,G)\to$$
$$\xrightarrow{E^*}\operatorname{Ext}(C,G)\xrightarrow{\beta^*}\operatorname{Ext}(B,G)\xrightarrow{\alpha^*}\operatorname{Ext}(A,G)\to 0$$
$$\text{и } 0\to\operatorname{Hom}(G,A)\to\operatorname{Hom}(G,B)\to\operatorname{Hom}(G,C)\to$$
$$\xrightarrow{E_*}\operatorname{Ext}(G,A)\xrightarrow{\alpha_*}\operatorname{Ext}(G,B)\xrightarrow{\beta_*}\operatorname{Ext}(G,C)\to 0$$

точны для любой группы G.

Одним из наиболее удивительных фактов теории расширений групп является то, что расширения, соответствующие чисто точным последовательностям, образуют подгруппу группы $\operatorname{Ext}(C,A)$. Ее называют *группой чистых расширений* группы A при помощи группы C и обозначают через $\operatorname{Pext}(C,A)$. Оказывается, что $\operatorname{Pext}(C,A)=\operatorname{Ext}(C,A)^1=\bigcap\limits_n n\operatorname{Ext}(C,A)$. Поскольку Ext является функтором, а ульмовские подгруппы — это функторные подгруппы, то Pext — тоже функтор. Если $\alpha\colon A\to A'$ и $\gamma\colon C'\to C$ — гомоморфизмы, то ограничение гомоморфизма $\operatorname{Ext}(\gamma,\alpha)$ дает отображение $\operatorname{Pext}(\gamma,\alpha)\colon\operatorname{Pext}(C,A)\to\operatorname{Pext}(C',A')$. Таким образом, Pext есть аддитивный бифунктор из категории $\mathcal{A}b\times\mathcal{A}b$ в категорию $\mathcal{A}b$: он контравариантен по первому аргументу и ковариантен по второму. Поведение этого функтора по отношению к коротким точным последовательностям раскрывается в следующем утверждении. Если $E\colon 0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$ — чисто точная последовательность, то для любой группы G точны следующие индуцированные последовательности:

$$0\to\operatorname{Hom}(C,G)\to\operatorname{Hom}(B,G)\to\operatorname{Hom}(A,G)\to$$
$$\xrightarrow{E^*}\operatorname{Pext}(C,G)\xrightarrow{\beta^*}\operatorname{Pext}(B,G)\xrightarrow{\alpha^*}\operatorname{Pext}(A,G)\to 0,$$
$$0\to\operatorname{Hom}(G,A)\to\operatorname{Hom}(G,B)\to\operatorname{Hom}(G,C)\to$$
$$\xrightarrow{E_*}\operatorname{Pext}(G,A)\xrightarrow{\alpha_*}\operatorname{Pext}(G,B)\xrightarrow{\beta_*}\operatorname{Pext}(G,C)\to 0.$$

Группа G называется *копериодической*, если $\operatorname{Ext}(C,G)=0$ для любой группы без кручения C. Это эквивалентно тому, что всякое расширение группы G при помощи группы без кручения расщепляется. Очевидно, что все алгебраически компактные группы являются копериодическими. Обратное места не имеет. Копериодические группы можно также определить как группы G, для которых $\operatorname{Ext}(\mathbb{Q},G)=0$.

Редуцированная копериодическая группа, не имеющая ненулевых прямых слагаемых, являющихся группами без кручения, называется *урегулированной*. Относительно строения копериодических групп, справедливы следующие два основных результата.

Теорема 22.1. *Пусть G — редуцированная копериодическая группа и T — ее периодическая часть. Тогда существует прямое разложение $G=A\oplus C$, где A — алгебраически компактная группа без кручения, а $C\cong\operatorname{Ext}(\mathbb{Q}/\mathbb{Z},T)$ — урегулированная копериодическая группа. Группа C однозначно определяется группой G.*

О подгруппе C из этой теоремы можно говорить как об *урегулированной части* редуцированной копериодической группы G. Всякую копериодическую группу G можно разложить в прямую сумму трех групп: $G=A\oplus C\oplus D$, где

D — делимая часть группы G, C — урегулированная копериодическая группа, A — редуцированная алгебраически компактная группа без кручения. Это разложение определено однозначно с точностью до изоморфизма, так как D и $C \oplus D$ — однозначно определенные подгруппы группы G. Группы A и D можно полностью охарактеризовать с помощью инвариантов, являющихся кардинальными числами. Следовательно, структурная проблема для копериодических групп сводится к случаю урегулированных копериодических групп. В силу следующей теоремы структурная проблема для этих групп эквивалентна такой же проблеме для редуцированных периодических групп.

Теорема 22.2. *Соответствие $T \mapsto \operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T) = G$ дает взаимно однозначное отображение класса редуцированных периодических групп T на класс урегулированных копериодических групп G. Обратное отображение является взятием периодической части группы G.*

Эта теорема сопоставляет группе G те же инварианты, какими обладает группа T, поэтому ее можно считать структурной теоремой для урегулированных копериодических групп в тех случаях, когда группа T известна.

Пусть A — редуцированная группа. Обозначим $A^\bullet = \operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, A)$. Существует естественный мономорфизм $\mu\colon A \to A^\bullet$. Поэтому A можно отождествить с подгруппой группы $A^\bullet$ такой, что $A^\bullet/A$ — делимая группа без кручения. Группа A — копериодическая в том и только в том случае, когда μ является изоморфизмом. Кроме того, $A^{\bullet\bullet} = A^\bullet$ для любой группы A. Если G — такая редуцированная копериодическая группа, что $A \subseteq G$, то $A^\bullet \subseteq G^\bullet = G$. Отсюда следует, что $A^\bullet$ — минимальная редуцированная копериодическая группа, содержащая группу A. Поэтому группу $A^\bullet$ можно рассматривать как *копериодическую оболочку* группы A. Если A — не редуцированная группа и D — ее делимая часть, то $D \oplus A^\bullet$ является копериодической оболочкой группы A. Копериодическая оболочка определяется однозначно с точностью до изоморфизма над A.

Ряд упражнений и важнейших свойств тензорного произведения модулей включены в § 18. Для абелевых групп A, C (как $\mathbb{Z}$-модулей) вместо $A \otimes_{\mathbb{Z}} C$ пишут $A \otimes C$. Группа $A \otimes C$ называется *тензорным произведением* групп A и C. Функция $g\colon A \times C \to G$, где G — произвольная группа, называется *билинейной*, если для любых элементов a, a_1, $a_2 \in A$, c, c_1, $c_2 \in C$ имеют место равенства $g(a_1 + a_2, c) = g(a_1, c) + g(a_2, c)$, $g(a, c_1 + c_2) = g(a, c_1) + g(a, c_2)$. Билинейная функция является $\mathbb{Z}$-сбалансированной в смысле § 18. Главные факты о сбалансированных отображениях собраны в теореме 18.1. Для удобства использования частично повторим ее.

Теорема 22.3. *Если $g\colon A \times C \to G$ — какая-то билинейная функция, то имеется единственный гомоморфизм $\varphi\colon A \otimes C \to G$, для которого коммутативна диаграмма*

$$\begin{array}{ccc} A \times C & \xrightarrow{e} & A \otimes C \\ \downarrow g & & \downarrow \varphi \\ G & \xrightarrow{1_G} & G, \end{array}$$

где $e\colon (a, c) \to a \otimes c$ — так называемое тензорное отображение.

Из теоремы 22.3 выводится, что всегда $A \otimes C \cong C \otimes A$ (см. 18.3).

Пусть $\alpha\colon A \to A'$ и $\gamma\colon C \to C'$ — гомоморфизмы групп. Существует однозначно определенный гомоморфизм $\varphi\colon A \otimes C \to A' \otimes C'$, для которого $\varphi(a \otimes c) = \alpha a \otimes \gamma c$. φ обозначают как $\alpha \otimes \gamma$ и говорят еще, что он индуцируется α и γ. Более кратко иногда пишем $\alpha_* = \alpha \otimes 1_C$, $\gamma_* = 1_A \otimes \gamma$.

Справедливы следующие теоремы.

Теорема 22.4. *Тензорное произведение является аддитивным бифунктором из категории $\mathcal{A}b \times \mathcal{A}b$ в категорию $\mathcal{A}b$, ковариантным по обоим аргументам* (более общая формулировка приведена в 18.14).

Теорема 22.5. (Ср. с упр. 18.11). *Если $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ — точная последовательность и G — произвольная группа, то индуцированная последовательность $A \otimes G \xrightarrow{\alpha_*} B \otimes G \xrightarrow{\beta_*} C \otimes G \to 0$ точна.*

Теорема 22.6. *Если $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ — чисто точная последовательность, то для любой группы G последовательность $0 \to A \otimes G \xrightarrow{\alpha_*} B \otimes G \xrightarrow{\beta_*} C \otimes G \to 0$ чисто точна.*

В случае, когда один из множителей является периодической группой, вопрос о строении тензорного произведения решается до конца, задачи 22.62 – 22.64. О строении тензорных произведений групп без кручения известно по существу мало. Лучшее, что в общем случае можно сделать, — найти некоторые инварианты для группы $A \otimes C$.

Если даны группы A и C, то их *периодическим произведением* $\operatorname{Tor}(A, C)$ называется абелева группа, образующие которой — все тройки (a, m, c), где $a \in A$, $c \in C$, $m \in \mathbb{Z}$ и $ma = mc = 0$, а определяющие соотношения:

$(a_1 + a_2, m, c) = (a_1, m, c) + (a_2, m, c)$, если $ma_1 = ma_2 = mc = 0$,

$(a, m, c_1 + c_2) = (a, m, c_1) + (a, m, c_2)$, если $ma = mc_1 = mc_2 = 0$,

$(a, mn, c) = (na, m, c)$, если $mna = mc = 0$, $(a, mn, c) = (a, m, nc)$, если $ma = mnc = 0$.

Очевидно, что $\operatorname{Tor}(A, C) \cong \operatorname{Tor}(C, A)$. Элементами группы $\operatorname{Tor}(A, C)$ являются конечные суммы вида $\sum (a_i, m_i, c_i)$, где $m_i a_i = m_i c_i = 0$.

Если $\alpha\colon A \to A'$ и $\gamma\colon C \to C'$ — гомоморфизмы, то соответствие $(a, m, c) \mapsto (\alpha a, m, \gamma c)$ между образующими однозначно продолжается до гомоморфизма $\operatorname{Tor}(\alpha, \gamma)\colon \operatorname{Tor}(A, C) \to \operatorname{Tor}(A', C')$.

Теорема 22.7. *Периодическое произведение является аддитивным бифунктором из категории $\mathcal{A}b \times \mathcal{A}b$ в категорию $\mathcal{A}b$, ковариантным по обоим аргументам.*

Пусть $E\colon 0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ — короткая точная последовательность и (c, m, g) — образующий элемент группы $\operatorname{Tor}(C, G)$. Существуют такие элементы $b \in B$, $a \in A$, что $\beta b = c$, $\alpha a = mb$ (так как $mc = 0$). Отображение $E_*\colon (c, m, g) \mapsto a \otimes g$ продолжается до гомоморфизма $E_*\colon \operatorname{Tor}(C, G) \to A \otimes G$.

Теорема 22.8. *Если последовательность E точна, то для любой группы G точна индуцированная последовательность*

$$0 \to \operatorname{Tor}(A, G) \xrightarrow{\alpha_*} \operatorname{Tor}(B, G) \xrightarrow{\beta_*} \operatorname{Tor}(C, G) \to$$
$$\xrightarrow{E_*} A \otimes G \xrightarrow{\alpha\otimes 1} B \otimes G \xrightarrow{\beta\otimes 1} C \otimes G \to 0.$$

Здесь α_*, β_* — сокращенные обозначения отображений $\operatorname{Tor}(\alpha, 1_G)$, $\operatorname{Tor}(\beta, 1_G)$.

Задачи

22.1. 1) Если E — расширение из диаграммы (1), то расширения μE и $E\nu$ расщепляются.

2) Если $(\alpha, \beta, \gamma)\colon E \to E'$ — морфизм в категории $\mathcal{E}$, то $\alpha E \equiv E'\gamma$.

22.2. Группа G обладает тем свойством, что для любого эпиморфизма $\beta\colon B \to C$ индуцированное отображение $\beta^*\colon \operatorname{Ext}(C, G) \to \operatorname{Ext}(B, G)$ является мономорфизмом тогда и только тогда, когда G — делимая группа.

22.3. Группа G является свободной тогда и только тогда, когда для любого мономорфизма $\alpha\colon A \to B$ отображение $\alpha_*\colon \operatorname{Ext}(G, A) \to \operatorname{Ext}(G, B)$ — мономорфизм.

22.4. Если $\beta\colon B \to C$ — эпиморфизм, и $\beta^*\colon \operatorname{Ext}(C, G) \to \operatorname{Ext}(B, G)$ — мономорфизм при любой группе G, то $\operatorname{Ker}\beta$ служит прямым слагаемым для группы B.

22.5. Если $\alpha\colon A \to B$ — мономорфизм, и $\alpha_*\colon \operatorname{Ext}(G, A) \to \operatorname{Ext}(G, B)$ — мономорфизм при любой группе G, то αA — прямое слагаемое группы B.

22.6. Имеют место изоморфизмы: $\operatorname{Ext}(\mathbb{Q}, \mathbb{Z}) \cong \prod_{\aleph_0} \mathbb{Q}$ и $\operatorname{Ext}(\mathbb{Z}_{p^\infty}, \widehat{\mathbb{Z}}_p) \cong \widehat{\mathbb{Z}}_p$.

22.7. Умножение на целое число n в группе A или в группе C индуцирует умножение на n в группе $\operatorname{Ext}(C, A)$. То же имеет место для целых p-адических чисел.

22.8. 1) Для группы C имеет место $\operatorname{Ext}(C, A) = 0$ при любой группе A в том и только в том случае, когда C — свободная группа.

2) Для группы A имеет место $\operatorname{Ext}(C, A) = 0$ при любой группе C в том и только в том случае, когда A — делимая группа.

22.9. Существуют естественные изоморфизмы

$$\operatorname{Ext}(\bigoplus_{i\in I} C_i, A) \cong \prod_{i\in I} \operatorname{Ext}(C_i, A), \operatorname{Ext}(C, \prod_{i\in I} A_i) \cong \prod_{i\in I} \operatorname{Ext}(C, A_i).$$

22.10. Для любой группы A и любого целого числа m имеют место изоморфизмы:

а) $\operatorname{Ext}(\mathbb{Z}_m, A) \cong A/mA$ и б) $\operatorname{Ext}(A, \mathbb{Z}_m) \cong \operatorname{Ext}(A[m], \mathbb{Z}_m)$.

22.11. 1) Если $mA = 0$ или $mC = 0$, то $m\operatorname{Ext}(C, A) = 0$.

2) Если $mA = A$, то $m\operatorname{Ext}(C, A) = \operatorname{Ext}(C, A)$.

22.12. 1) Автоморфизм α группы A индуцирует автоморфизм α_* группы $\operatorname{Ext}(C, A)$.

2) Автоморфизм γ группы C индуцирует автоморфизм $\gamma*$ группы $\operatorname{Ext}(C, A)$.

22.13. 1) Если $C[m] = 0$, то $m\operatorname{Ext}(C, A) = \operatorname{Ext}(C, A)$, в частности, если C — группа без кручения, то $\operatorname{Ext}(C, A)$ — делимая группа.

2) Если A является p-делимой группой, а C есть p-группа, то $\operatorname{Ext}(C, A) = 0$.

22.14. Покажите, что если A — группа без кручения, C — периодическая группа, то $\operatorname{Ext}(C, A) \cong \operatorname{Hom}(C, D/A)$, где D — делимая оболочка группы A. Следовательно, $\operatorname{Ext}(C, A)$ — редуцированная алгебраически компактная группа.

22.15. Если A — группа без кручения, p-базисная подгруппа которой имеет ранг m, то группа $\operatorname{Ext}(\mathbb{Z}_{p^\infty}, A)$ изоморфна p-адическому пополнению группы $\bigoplus_m \widehat{\mathbb{Z}}_p$.

22.16. 1) Если A — группа без кручения, то группа $\operatorname{Ext}(C, A)$ алгебраически компактна для любой группы C.

2) Если группа A алгебраически компактна, то $\operatorname{Ext}(C, A)$ — редуцированная алгебраически компактная группа.

22.17. Если A — периодическая группа, а C — группа без кручения, то $\operatorname{Ext}(C, A)$ или непериодическая группа, или равна 0.

22.18. Равенство $p\operatorname{Ext}(C, A) = \operatorname{Ext}(C, A)$ справедливо тогда и только тогда, когда $C[p] = 0$ или $pA = A$.

22.19. $\operatorname{Ext}(\mathbb{Q}_p, \mathbb{Z}) \cong \mathbb{Z}_{p^\infty} \oplus \prod_{\aleph_0} \mathbb{Q}$.

22.20. 1) $\operatorname{Ext}(\mathbb{Q}_p, \mathbb{Q}_p) = 0$ и $\operatorname{Ext}(\mathbb{Q}, \mathbb{Q}_p) \cong \prod_{\aleph_0} \mathbb{Q}$.

2) $\operatorname{Ext}(\widehat{\mathbb{Z}}_p, \mathbb{Z}) \cong \mathbb{Z}_{p^\infty} \oplus \prod_{2^{\aleph_0}} \mathbb{Q}$ и $\operatorname{Ext}(\widehat{\mathbb{Z}}_p, \mathbb{Q}_p) \cong \operatorname{Ext}(\widehat{\mathbb{Z}}_p, \mathbb{Z})$.

22.21. 1) Группа A обладает свойством, что $\operatorname{Pext}(C, A) = 0$ для любой группы C тогда и только тогда, когда A алгебраически компактна.

2) Для группы C выполнено $\operatorname{Pext}(C, A) = 0$ при любой группе A тогда и только тогда, когда C — прямая сумма циклических групп.

22.22. Если A — такая группа, что $A^1 = 0$, то $\operatorname{Pext}(\mathbb{Q}/\mathbb{Z}, A) \cong \operatorname{Hom}(\mathbb{Q}/\mathbb{Z}, \widehat{A}/A)$, где $\widehat{A}$ есть $\mathbb{Z}$-адическое пополнение группы A.

22.23. Расширение $0 \to A \xrightarrow{\mu} B \xrightarrow{\nu} C \to 0$ лежит в подгруппе Фраттини группы $\operatorname{Ext}(C, A)$ тогда и только тогда, когда $\operatorname{Im}\mu$ — слабо чистая подгруппа группы B.

22.24. Последовательность $0 \to A \xrightarrow{\mu} B \xrightarrow{\nu} C \to 0$ является p-чисто точной тогда и только тогда, когда она представляет элемент из $p^\omega \operatorname{Ext}(C, A)$.

22.25. Имеют место естественные изоморфизмы:

$$\operatorname{Pext}(\bigoplus_{i\in I} C_i, A) \cong \prod_{i\in I} \operatorname{Pext}(C_i, A),\ \operatorname{Pext}(C, \prod_{i\in I} A_i) \cong \prod_{i\in I} \operatorname{Pext}(C, A_i).$$

22.26. Если группа A алгебраически компактна, и T — периодическая часть группы C, то имеет место естественный изоморфизм $\operatorname{Ext}(C, A) \cong \operatorname{Ext}(T, A)$.

22.27. Если A — группа без кручения, и T — периодическая часть группы C, то

$$\operatorname{Ext}(C, A) \cong \operatorname{Ext}(T, A) \oplus \operatorname{Ext}(C/T, A).$$

22.28. Если A — группа без кручения, и C — периодическая группа с базисной подгруппой B, то

$$\operatorname{Ext}(C, A) \cong \operatorname{Ext}(B, A) \oplus \operatorname{Ext}(C/B, A).$$

22.29. Группа G алгебраически компактна тогда и только тогда, когда $\operatorname{Ext}(\mathbb{Q}, G) = 0$ и $\operatorname{Pext}(\mathbb{Q}/\mathbb{Z}, G) = 0$.

22.30. 1) Эпиморфный образ копериодической группы является копериодической группой.

2) Если G — редуцированная копериодическая группа, то ее подгруппа H является копериодической группой тогда и только тогда, когда G/H — редуцированная группа.

3) Если G — редуцированная копериодическая группа, то для любого эндоморфизма φ группы G как $\operatorname{Ker}\varphi$, так и $\operatorname{Im}\varphi$, — копериодические группы.

4) Если H — подгруппа группы G, причем H и G/H — копериодические группы, то группа G копериодическая.

5) Прямое произведение $\prod G_i$ является копериодической группой тогда и только тогда, когда каждая G_i — копериодическая группа.

22.31. 1) Если G — копериодическая группа, то $\operatorname{Hom}(A, G)$ является копериодической группой при любой группе A.

2) Если G — редуцированная копериодическая группа, то существует естественный изоморфизм $\operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, G) \cong G$.

22.32. Редуцированная копериодическая группа G однозначно записывается в виде $G = \prod_p G_p$, где G_p для каждого простого числа p есть копериодическая группа, являющаяся p-адическим модулем (т.е. $\widehat{\mathbb{Z}}_p$-модулем).

22.33. Группа является копериодической тогда и только тогда, когда она — эпиморфный образ алгебраически компактной группы.

22.34. Редуцированная копериодическая группа алгебраически компактна тогда и только тогда, когда ее первая ульмовская подгруппа равна нулю.

22.35. 1) Периодическая группа является копериодической тогда и только тогда, когда она — прямая сумма делимой группы и ограниченной группы.

2) Группа без кручения является копериодической тогда и только тогда, когда она алгебраически компактна.

3) Для любых групп A и C группа $\operatorname{Ext}(C, A)$ является копериодической.

22.36. Если G — редуцированная копериодическая группа и H — ее подгруппа, то существует единственная минимальная копериодическая подгруппа группы G, содержащая H.

22.37. Если D — делимая оболочка копериодической группы G и E $(\subseteq D)$ — делимая оболочка подгруппы G^1, то $E+G$ — алгебраически компактная группа, являющаяся чисто инъективной оболочкой группы G.

22.38. Если T — редуцированная периодическая группа, то периодическая часть группы $\operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T)$ изоморфна группе T, а факторгруппа по ней — делимая группа без кручения.

22.39. Если T — периодическая часть смешанной группы A, то

$$\operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, A) \cong \operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T) \oplus \operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, A/T).$$

22.40. Для любой периодической группы T группа $\operatorname{Ext}(T, A)$ является редуцированной.

22.41. Если T — периодическая группа, то $\operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T)$ — урегулированная копериодическая группа.

22.42. Пусть A, C — урегулированные копериодические группы и S, T — их периодические части. Тогда:

а) существует естественный изоморфизм $\operatorname{Hom}(A, C) \cong \operatorname{Hom}(S, T)$;

б) $\operatorname{Hom}(A, C)$ — алгебраически компактная группа;

в) всякий гомоморфизм $S \to T$ может быть единственным образом продолжен до гомоморфизма $A \to C$.

22.43. Если G — урегулированная копериодическая группа, и T — ее периодическая часть, то соответствие $\alpha \mapsto \alpha|T$ есть изоморфизм между группами автоморфизмов групп G и T.

22.44. Редуцированная копериодическая группа является урегулированной тогда и только тогда, когда для каждого простого числа p ее p-базисная подгруппа периодическая.

22.45. Пусть G — урегулированная копериодическая группа и $T = t(G)$. Тогда $|G| \leqslant |T|^{\aleph_0}$, а если $T = T_1 \oplus T_2$, то существует прямое разложение $G = G_1 \oplus G_2$ со свойством $t(G_1) = T_1$, $t(G_2) = T_2$.

22.46. Всякую группу A можно вложить в копериодическую группу G так, что G/A будет делимой группой без кручения. Если группа A редуцированная, то группу G можно также выбрать редуцированной.

22.47. Если A и B — редуцированные группы, то гомоморфизм $A \to B$ можно единственным образом продолжить до гомоморфизма $A^\bullet \to B^\bullet$.

22.48. Если $A \subseteq G$, где G — редуцированная копериодическая группа и G/A — делимая группа без кручения, то группа G изоморфна над A группе $A^\bullet$.

22.49. 1) Если $m|a$ и $n|c$, то $mn|a \otimes c$.

2) Если $ma = 0$ и $nc = 0$, то $(m, n)(a \otimes c) = 0$.

3) Если $m|a$ и $mc = 0$, то $a \otimes c = 0$.

22.50. 1) Если группа A или группа C является p-делимой (делимой), то $A \otimes C$ есть p-делимая (делимая) группа.

2) Если группа A или группа C является p-группой (периодической группой), то $A \otimes C$ есть p-группа (периодическая группа).

3) Если A есть p-делимая группа, а C есть p-группа, то $A \otimes C = 0$.

4) Если при некотором $m \in \mathbb{Z}$ имеют место включения $a \in mA$ и $c \in C[m]$, то $a \otimes c = 0$ в группе $A \otimes C$.

5) Если $h_p(a) = \infty$, а C есть p-группа, то $a \otimes c = 0$ в группе $A \otimes C$ для любого $c \in C$.

22.51. 1) $h_p(a \otimes c) \geqslant h_p(a) + h_p(c)$.

2) Существуют естественные изоморфизмы $\mathbb{Z} \otimes C \cong C$ и $\mathbb{Z}_m \otimes C \cong C/mC$.

22.52. Если B — подгруппа, порожденная всеми гомоморфными образами группы A в группе C, то существует эпиморфизм $A \otimes \operatorname{Hom}(A, C) \to B$.

22.53. Существует естественный гомоморфизм $A \otimes \prod_{i \in I} C_i \to \prod_{i \in I} (A \otimes C_i)$, который в общем случае не является изоморфизмом.

22.54. Если A — группа без кручения, то $a \mapsto 1 \otimes a$ — естественное вложение группы A в $\mathbb{Q} \otimes A$. В частности, $\mathbb{Q} \otimes A$ можно рассматривать как делимую оболочку группы A.

22.55. Если $\alpha\colon A \to B$ — такой мономорфизм, что $\alpha \otimes 1_G\colon A \otimes G \to B \otimes G$ является мономорфизмом для любой группы G, то $\operatorname{Im}\alpha$ — чистая подгруппа группы B.

22.56. Последовательность $0 \to A \to B \to C \to 0$ является чисто точной тогда и только тогда, когда для любого натурального числа m индуцированная последовательность $0 \to A \otimes \mathbb{Z}_m \to B \otimes \mathbb{Z}_m \to C \otimes \mathbb{Z}_m \to 0$ точна.

22.57. Если A', C' — чистые подгруппы групп A и C соответственно, то при естественном вложении $A' \otimes C'$ в $A \otimes C$ получается чистая подгруппа группы $A \otimes C$.

22.58. Если всегда из точности последовательности $0 \to A \to B \to C \to 0$ следует точность последовательности $0 \to A \otimes G \to B \otimes G \to C \otimes G \to 0$, то G — группа без кручения.

22.59. Если A или C есть p-адическая группа (т.е. $\widehat{\mathbb{Z}}_p$-модуль), то $A \otimes C$ есть p-адическая группа. Если π — целое p-адическое число, то $\pi(a \otimes c) = \pi a \otimes c$ или $\pi(a \otimes c) = a \otimes \pi c$ в зависимости от того, что имеет смысл.

22.60. Пусть A и C — группы без кручения и $\{a_i\}_{i \in I}$, $\{c_j\}_{j \in J}$ — их максимальные независимые системы элементов соответственно. Покажите, что $\{a_i \otimes c_j\}_{i,\,j}$ — максимальная независимая система элементов группы $A \otimes C$. Проверьте равенство $r_0(A \otimes C) = r_0(A)\, r_0(C)$ для произвольных групп A и C.

22.61. Пусть A и C — группы без кручения, и пусть $p^t \,|\, a \otimes c$ для некоторых $a \in A$, $c \in C$. Тогда существуют такие неотрицательные целые числа r, s, что $r + s = t$ и $p^r \,|\, a$, $p^s \,|\, c$.

22.62. Если C есть p-группа, а B есть p-базисная подгруппа группы A, то имеет место естественный изоморфизм $A \otimes C \cong B \otimes C$.

Утверждение 22.62 позволяет определить строение тензорного произведения $A \otimes C$ для любой периодической группы C. Если B_p есть p-базисная подгруппа группы A, а C_p есть p-компонента группы C, то $A \otimes C \cong \bigoplus\limits_p (A \otimes C_p) \cong \bigoplus\limits_p (B_p \otimes C_p)$. Полученный изоморфизм показывает, в частности, что $A \otimes C \cong t(A) \otimes C \oplus (A/t(A)) \otimes C$ для любой периодической группы C.

22.63. Если B — чистая подгруппа группы A и C — периодическая группа, то имеет место изоморфизм: $A \otimes C \cong B \otimes C \oplus (A/B) \otimes C$.

22.64. Тензорное произведение периодических групп является прямой суммой циклических групп.

22.65. Если A и C — группы без кручения с p-базисными подгруппами B и D соответственно, то $A \otimes C$ — группа без кручения, p-базисная подгруппа которой изоморфна $B \otimes D$.

22.66. Для любых групп A, C имеют место изоморфизмы

$$t(A \otimes C) \cong [t(A) \otimes t(C)] \oplus [t(A) \otimes C/t(C)] \oplus [A/t(A) \otimes t(C)],$$
$$(A \otimes C)/t(A \otimes C) \cong A/t(A) \otimes C/t(C).$$

22.67. Если $A/t(A)$ — делимая группа, то $A \otimes C \cong t(A) \otimes C$ для любой периодической группы C.

22.68. 1) $\operatorname{Tor}(A,\, C)$ является периодической группой, это p-группа, если p-группой является A или C.

2) Имеет место естественный изоморфизм $\operatorname{Tor}(A,\, C) \cong \operatorname{Tor}(t(A),\, t(C))$.

3) Если $nA = 0$, то $n \operatorname{Tor}(A,\, C) = 0$ для любой группы C.

4) Если A есть p-группа, а C есть q-группа, p, q — различные простые числа, то $\operatorname{Tor}(A,\, C) = 0$.

5) Существует естественный изоморфизм $\operatorname{Tor}(\bigoplus\limits_i A_i,\, C) \cong \bigoplus\limits_i \operatorname{Tor}(A_i,\, C)$.

6) Если A_p и C_p — p-компоненты групп A и C соответственно, то имеет место изоморфизм $\operatorname{Tor}(A,\, C) \cong \bigoplus\limits_p \operatorname{Tor}(A_p,\, C_p)$.

7) Умножение на целое число n в группе A или в группе C индуцирует умножение на n в группе $\operatorname{Tor}(A,\, C)$.

8) Для любой группы C существуют естественные изоморфизмы

$\operatorname{Tor}(\mathbb{Z}_m,\, C) \cong C\,[m]$, $\operatorname{Tor}(\mathbb{Z}_{p^\infty},\, C) \cong C_p$ и $\operatorname{Tor}(\mathbb{Q}/\mathbb{Z},\, C) \cong t(C)$.

22.69. $\operatorname{Tor}(A,\, C) = 0$ для каждой группы C в точности тогда, когда группа A не имеет кручения.

22.70. Если A', B' — чистые подгруппы групп A и B, то $\operatorname{Tor}(A',\, B')$ — чистая подгруппа группы $\operatorname{Tor}(A,\, B)$.

22.71. 1) Если последовательность $0 \to \operatorname{Tor}(A,\, G) \to \operatorname{Tor}(B,\, G) \to \operatorname{Tor}(C,\, G) \to 0$ точна для любой точной последовательности $0 \to A \to B \to C \to 0$, то G — группа без кручения.

2) Если для точной последовательности $0 \to A \to B \to C \to 0$ последовательность $0 \to \operatorname{Tor}(A,\, G) \to \operatorname{Tor}(B,\, G) \to \operatorname{Tor}(C,\, G) \to 0$ точна при любой группе G (при любой группе $G = \mathbb{Z}_m$), то исходная последовательность чисто точна.

22.72. Докажите законы ассоциативности:

$(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ и $\operatorname{Tor}(\operatorname{Tor}(A,\, B),\, C) \cong \operatorname{Tor}(A,\, \operatorname{Tor}(B,\, C))$.

23 p-группы

Все абелевы группы разбиваются на три класса в зависимости от порядков элементов (см. § 3). Этим классам посвящены настоящий и следующие два параграфа. Еще раз напомним, что если всякий элемент группы A имеет конечный порядок, то A называется *периодической* группой. Если же все ненулевые элементы группы A имеют бесконечный порядок, то A — группа *без кручения*. *Смешанные* группы содержат как ненулевые элементы конечного порядка, так и элементы бесконечного порядка. Теория периодических групп сводится к теории p-групп (19.30).

Произвольная группа называется *сепарабельной*, если любую ее конечную систему элементов можно вложить в прямое слагаемое группы A, являющееся прямой суммой групп ранга 1. Все делимые группы сепарабельны. Редуцированная p-группа сепарабельна тогда и только тогда, когда она не содержит ненулевых элементов бесконечной высоты, такие группы хаусдорфовы в своей p-адической топологии. Все p-группы будут считаться снабженными p-адической топологией.

Пусть A — редуцированная p-группа и $a \in A$ — элемент порядка p^n. Возрастающая последовательность (1)

$$H(a) = (h^*(a),\, h^*(pa),\, \dots,\, h^*(p^n a) = \infty)$$

порядковых чисел и символов ∞ называется *индикатором* элемента a. Здесь h^* обозначает обобщенную высоту, т.е. $h^*(a) = \sigma$, если $a \in p^\sigma A \setminus p^{\sigma+1}A$, и $h^*(0) = \infty$ ($\sigma < \infty$ для любого порядкового числа σ). Подгруппа $p^\sigma A$ для порядкового числа σ определяется так: $p^0 A = A$, $p^{\sigma+1}A = p(p^\sigma A)$ и $p^\sigma A = \bigcap\limits_{\alpha<\sigma} p^\alpha A$, если σ — предельное порядковое число. Часто бывает удобно бесконечно продолжить последовательность (1), добавив к ней символы ∞:

$$H(a) = (h^*(a),\, h^*(pa), \dots,\, h^*(p^n a) = \infty, \infty, \dots).$$

На множестве индикаторов можно ввести частичный порядок: $H(a) \leqslant H(b)$, если $h^*(p^i a) \leqslant h^*(p^i b)$ при $i = 0, 1, 2, \dots$. Если $h^*(p^i a) + 1 < h^*(p^{i+1}a)$, то говорят, что индикатор элемента a имеет *скачок* между $h^*(p^i a)$ и $h^*(p^{i+1}a)$.

Редуцированная p-группа A называется *вполне транзитивной*, если для любых элементов $a, b \in A$ со свойством $H(a) \leqslant H(b)$ существует такой ее эндоморфизм f, что $fa = b$. Сепарабельные p-группы вполне транзитивны.

Если $u = (\sigma_0, \sigma_1, \dots, \sigma_n, \dots)$ — возрастающая последовательность порядковых чисел и символов ∞, то с этой последовательностью свяжем вполне инвариантную подгруппу $A(u) = \{a \in A \,|\, H(a) \geqslant u\}$ группы A. Говорят, что последовательность u удовлетворяет *условию на скачки*, если между σ_n и σ_{n+1} скачок может встретиться только тогда, когда в группе A имеется элемент порядка p и высоты σ_n.

Теорема 23.1. *Пусть A — вполне транзитивная p-группа. Ее подгруппа является вполне инвариантной тогда и только тогда, когда она имеет вид $A(u)$, где последовательность u удовлетворяет условию на скачки. Всякая вполне инвариантная подгруппа представляется в указанном виде единственным образом.*

Вполне инвариантная подгруппа G произвольной p-группы A называется *широкой*, если $G + B = A$ для любой базисной подгруппы B группы A.

Говорят, что подгруппа G p-группы A удовлетворяет *условию Пирса*, если для любого неотрицательного числа k существует такое число $n \geqslant 0$, что $p^n A[p^k] \subseteq G$.

Теорема 23.2. *Для вполне инвариантной подгруппы G редуцированной p-группы A эквивалентны условия:*

1) *G — широкая подгруппа группы A;*

2) *$G = A(u)$, где в последовательности u символ ∞ не встречается, если группа A не является ограниченной;*

3) *для подгруппы G выполнено условие Пирса.*

Периодически полной p-группой называется периодическая часть p-адического пополнения $\widehat{B}$ прямой суммы B циклических p-групп. Эта группа однозначно определяется группой B, поэтому ее обозначают $\overline{B} = t(\widehat{B})$, она имеет вид $\overline{B}$ для любой из своих базисных подгрупп B. Если $B = \bigoplus\limits_{n=1}^{\infty} B_n$, где $B_n = \bigoplus\limits_{m_n} \mathbb{Z}_{p^n}$, то $\overline{B} \subseteq \widehat{B} \subseteq \prod\limits_n B_n$. Если B — базисная подгруппа p-группы A, то существует гомоморфизм группы A на чистую подгруппу группы $\overline{B}$, содержащую B, ядро гомоморфизма совпадает с A^1. Для неограниченной группы B справедливо равенство $|\overline{B}| = |B|^{\aleph_0}$.

Далее в этом параграфе через $\overline{B}$ обозначено периодическое пополнение некоторой прямой суммы B циклических p-групп (p — фиксированное простое число).

Периодически полные группы играют фундаментальную роль в теории p-групп. Они имеют различные характеризации.

Теорема 23.3. *Для редуцированной p-группы A эквивалентны условия:*

1) *A — периодически полная группа;*

2) *A — периодическая часть алгебраически компактной группы;*

3) *группа A чисто инъективна в классе p-групп, т.е. A инъективна относительно всех чисто точных последовательностей p-групп;*

4) *A служит прямым слагаемым для всякой p-группы, в которой она содержится в качестве чистой подгруппы.*

Теорема 23.4. *Редуцированная p-группа A периодически полна тогда и только тогда, когда всякий изоморфизм между ее базисными подгруппами продолжается до автоморфизма самой группы A.*

Теорема 23.5. *Пусть A — сепарабельная p-группа. В группе A всякая последовательность Коши, порядки*

элементов которой ограничены в совокупности, сходится в p-адической топологии тогда и только тогда, когда A — периодически полная группа.

Говорят, что группа A обладает *свойством замены*, если она удовлетворяет следующему условию (2): если $M = A \oplus N = \bigoplus\limits_{i\in I} C_i$, то существуют такие подгруппы E_i групп C_i, что $M = A \oplus \bigoplus\limits_{i\in I} E_i$. Если это свойство выполняется только для конечных систем индексов I, то говорят, что A обладает *свойством конечной замены*.

Периодически полные группы обладают свойством замены.

Подгруппа S цоколя $A[p]$ p-группы A называется *подцоколем* группы A. Говорят, что подцоколь S служит *носителем* подгруппы C группы A, если $C[p] = S$. Подцоколь S называется *дискретным*, если $S \cap p^n A = 0$ при некотором n, т.е. высоты элементов из S ограничены в совокупности.

Редуцированная периодическая группа A называется *квазиполной*, если замыкание G^- в $\mathbb{Z}$-адической топологии группы A всякой ее чистой подгруппы G также чисто в A. p-группа A называется *чисто полной*, если всякий ее подцоколь служит носителем чистой подгруппы группы A.

Периодически полные группы являются квазиполными. Квазиполные группы являются чисто полными.

Теорема 23.6. *Сепарабельная p-группа A квазиполна тогда и только тогда, когда для любого недискретного подцоколя S группы A имеет место равенство: $A[p] + S^- = \overline{B}[p]$, где B — базисная подгруппа группы A (замыкание рассматривается в p-адической топологии группы $\overline{B}$).*

Теорема 23.7. *Редуцированная p-группа A периодически полна тогда и только тогда, когда для любой чистой подгруппы G группы A подгруппа G^- служит для A прямым слагаемым.*

Задачи

23.1. Произвольная группа сепарабельна тогда и только тогда, когда ее редуцированная часть сепарабельна.

23.2. Чистая подгруппа плотна в p-группе A тогда и только тогда, когда ее цоколь плотен в $A[p]$.

23.3. Чистая подгруппа G сепарабельной p-группы A является замкнутой тогда и только тогда, когда подгруппа $G[p^n]$ замкнута в $A[p^n]$ при некотором $n \geqslant 1$.

23.4. Пусть $A = B \oplus C$ есть p-группа и G — такая ее чистая подгруппа, что $G[p] = B[p]$. Тогда $A = G \oplus C$.

23.5. Пусть S — плотной подцоколь p-группы A. Существует подгруппа C группы A, максимальная относительно свойства $C[p] = S$. Подгруппа C чиста и плотна в A.

23.6. Если всякий замкнутый подцоколь — носитель чистой подгруппы, то это верно для любого подцоколя.

23.7. Прямая сумма циклических и квазициклических p-групп является чисто полной.

23.8. 1) Если цоколи двух чистых подгрупп некоторой p-группы совпадают, то эти подгруппы имеют изоморфные базисные подгруппы.

2) В прямой сумме циклических p-групп любые две чистые подгруппы с одинаковыми цоколями изоморфны.

23.9. 1) 0 является широкой подгруппой тогда и только тогда, когда группа A ограниченная.

2) Всякая вполне инвариантная подгруппа ограниченной группы является широкой.

3) $p^n A$ при любом n — широкая подгруппа группы A.

4) Если G — широкая подгруппа группы A, то $p^n G$ при любом n — также широкая подгруппа.

5) A^1 содержится во всякой широкой подгруппе группы A.

23.10. Найдите вполне инвариантные, а также характеристические подгруппы делимой группы.

23.11. В p-группе A единственными чистыми вполне инвариантными подгруппами являются 0, A и делимая часть.

23.12. Вполне инвариантные подгруппы вполне транзитивной p-группы A образуют полную дистрибутивную подрешетку в решетке всех подгрупп группы A.

23.13. Решетка широких подгрупп p-группы является дистрибутивной.

23.14. 1) В неограниченной сепарабельной p-группе вполне инвариантная подгруппа является широкой тогда и только тогда, когда она неограниченная.

2) Если B — базисная подгруппа p-группы A, отличная от A, а G — вполне инвариантная подгруппа в A со свойством $G + B = A$, то G — широкая подгруппа группы A.

23.15. Гомоморфизм $\varphi\colon A \to C$ p-групп является малым тогда и только тогда, когда $\operatorname{Ker}\varphi$ содержит широкую подгруппу группы A (малые гомоморфизмы определены перед 21.28).

23.16. 1) Периодически полные p-группы $\overline{B}$ и $\overline{B'}$ изоморфны тогда и только тогда, когда их базисные подгруппы B и B' изоморфны.

2) $\overline{B} = B$ тогда и только тогда, когда группа B ограниченная.

3) $\overline{B \oplus B'} \cong \overline{B} \oplus \overline{B'}$.

23.17. Редуцированная p-группа A периодически полна тогда и только тогда, когда $\operatorname{Pext}(\mathbb{Z}_{p^\infty}, A) = 0$.

23.18. Если G — такая подгруппа периодически полной p-группы A, что A/G — редуцированная группа, то G сама является периодически полной группой.

23.19. 1) Если G — чистая подгруппа периодически полной p-группы A, то A/G — прямая сумма делимой группы и периодически полной группы.

2) В периодически полной p-группе замыкание чистой подгруппы служит прямым слагаемым (см. теорему 23.7).

23.20. 1) Широкие подгруппы периодически полных p-групп являются периодически полными.

2) Если G — периодически полная подгруппа p-группы A и A/G — ограниченная группа, то A — периодически полная группа.

p-группа A называется *тонкой*, если всякий гомоморфизм периодически полной p-группы в группу A является малым.

23.21. 1) Класс тонких групп замкнут относительно подгрупп, прямых сумм и расширений.

2) Все счетные редуцированные p-группы являются тонкими.

3) Всякий гомоморфизм $\overline{B} \to B$ является малым.

23.22. 1) Группа $A = G \oplus C$ обладает свойством замены тогда и только тогда, когда этим свойством обладают G и C.

2) Если группа A обладает свойством замены для всех таких групп M из условия (2) (см. определение), что группы C_i изоморфны подгруппам группы A, то A обладает свойством замены.

3) Никакая неограниченная p-группа, являющаяся прямой суммой циклических групп, не обладает свойством замены.

4) p-группа, являющаяся бесконечной прямой суммой неограниченных периодически полных групп, не обладает свойством замены.

23.23. Если группа A обладает свойством замены для всех таких множеств индексов I, что $|I| \leqslant |A|$, то A обладает свойством замены.

23.24. Для неразложимой группы свойство конечной замены влечет за собой свойство замены.

23.25. Группа $\mathbb{Q}_p$ обладает свойством замены.

23.26. Для квазиполноты сепарабельной p-группы A необходимо и достаточно, чтобы факторгруппа A/G при любой неограниченной чистой подгруппе $G \subseteq A$ была прямой суммой делимой группы и периодически полной группы.

23.27. Если A — квазиполная, но не периодически полная p-группа, то в любом ее прямом разложении одно из слагаемых является ограниченным.

24 Группы без кручения

Пусть $p_1, p_2, \dots$ — множество всех простых чисел, упорядоченных по возрастанию. Последовательность p-высот $\chi_A(a) = (h_{p_1}(a), h_{p_2}(a), \dots)$ называется *характеристикой* элемента a в группе без кручения A. Характеристики $\chi_1 = (k_1, k_2, \dots)$ и $\chi_2 = (l_1, l_2, \dots)$ считают равными в том и только в том случае, если $k_n = l_n$ для всех n; $\chi_1 \leqslant \chi_2$, если $k_n \leqslant l_n$ для всех n; $\chi_1\chi_2 = (k_1 + l_1, k_2 + l_2, \dots)$ — *произведение* характеристик (полагают, что ∞ плюс нечто есть ∞); *частное* $\chi_1 : \chi_2$ двух характеристик $\chi_1 \geqslant \chi_2$ определяется как наибольшая характеристика χ, для которой $\chi\chi_2 \leqslant \chi_1$. Множество всех характеристик является полной дедекиндовой решеткой относительно операций $\chi_1 \cap \chi_2 = (\min(k_1, l_1), \min(k_2, l_2), \dots)$ и $\chi_1 \cup \chi_2 = (\max(k_1, l_1), \max(k_2, l_2), \dots)$ с наименьшим $(0, \dots, 0, \dots)$ и наибольшим $(\infty, \dots, \infty, \dots)$ элементами. Характеристики χ_1 и χ_2 называются *эквивалентными*, если $k_n \neq l_n$ имеет место лишь для конечного числа номеров n и только тогда, когда k_n и l_n конечны. Класс эквивалентности в множестве характеристик называется *типом*. Тип элемента a обозначается через $t_A(a)$. Если все ненулевые элементы группы без кручения G имеют один и тот же тип t, то группу G называют *однородной*, и пишут $t = t(G)$. Поскольку отношение эквивалентности в множестве характеристик согласовано с решеточными операциями, введенными выше, множество типов также является решеткой.

Пусть G — группа без кручения. Она называется *вполне транзитивной*, если для любых ненулевых $a, b \in G$ с условием $\chi(a) \leqslant \chi(b)$ существует $f \in \operatorname{End} G$ со свойством $fa = b$. Обозначим через $\pi(G)$ множество всех таких простых чисел p, что $pG \neq G$.

Теорема 24.1. *Две группы без кручения ранга* 1 *изоморфны тогда и только тогда, когда они имеют один и тот же тип. Каждый тип является типом некоторой рациональной группы (т.е. подгруппы группы* $\mathbb{Q}$*). Множество всех неизоморфных групп без кручения ранга* 1 *имеет мощность континуума.*

Теорема 24.2. *Пусть A и B — группы без кручения ранга* 1*. Тогда*:

а) $A \otimes B$ — *группа без кручения ранга* 1, *причем* $t(A \otimes B) = t(A)\,t(B)$;

б) *если* $t(A) \not\leqslant t(B)$, *то* $\operatorname{Hom}(A, B) = 0$, *если же* $t(A) \leqslant t(B)$, *то* $\operatorname{Hom}(A, B)$ — *группа без кручения ранга* 1 *и имеет тип* $t(B) : t(A)$.

Группа без кручения называется *вполне разложимой*, если она является прямой суммой групп ранга 1.

Теорема 24.3. *Любые два разложения вполне разложимой группы в прямую сумму групп ранга* 1 *изоморфны* (изоморфизм разложений определен перед 19.48).

Теорема 24.4. *Пусть* A — *вполне разложимая однородная группа типа* t. *Если подгруппа* C *группы* A *является однородной группой типа* t (*в частности, чистой в* A), *то* C — *вполне разложимая группа.*

Теорема 24.5. 1) *Прямые слагаемые вполне разложимых групп без кручения вполне разложимы.*

2) *Всякая чистая подгруппа однородной вполне разложимой группы конечного ранга является в группе прямым слагаемым.*

3) *Счетная сепарабельная группа без кручения вполне разложима.*

Теорема 24.6. *Прямые слагаемые сепарабельных групп без кручения сепарабельны.*

Пусть P — прямое произведение счетного числа бесконечных циклических групп, $P = \prod\limits_{n=1}^{\infty} \langle e_n \rangle$ и $S = \bigoplus\limits_{n=1}^{\infty} \langle e_n \rangle$. Группа без кручения G называется *узкой*, если при любом гомоморфизме $\eta\colon P \to G$ для почти всех n выполнено равенство $\eta\, e_n = 0$.

Для множества индексов I мощности $\aleph_\sigma$ обозначим через P_σ и S_σ прямое произведение и прямую сумму соответственно некоторых групп без кручения A_i, где $i \in I$.

Напомним, что кардинальное число m называется *измеримым,* если множество X мощности m допускает счетно аддитивную меру μ, принимающую лишь два значения 0 и 1 и такую, что $\mu(X) = 1$, $\mu(x) = 0$ для всех $x \in X$. Если кардинальное число неизмеримо, то все кардинальные числа, меньшие, чем оно, также неизмеримы. Таким образом, если измеримые кардиналы вообще существуют, то среди них есть наименьшее и все большие его измеримы.

Теорема 24.7. *Пусть дан гомоморфизм* $\eta\colon P_\sigma \to G$, *где* G — *узкая группа. Тогда:*

1) *равенство* $\eta\, A_i = 0$ *имеет место для почти всех* i;

2) *если* $\aleph_\sigma$ — *неизмеримый кардинал и* $\eta\, S_\sigma = 0$, *то* $\eta = 0$.

Теорема 24.8. *Группа без кручения узка в том и только в том случае, когда она не содержит никакой подгруппы, изоморфной одной из групп* $\mathbb{Q}$, P *или* $\widehat{\mathbb{Z}}_p$, *где* p — *произвольное простое число.*

Теорема 24.9. *Счетная однородная группа без кручения* A *вполне разложима в том и только в том случае, когда каждая подгруппа* $C \subseteq A$, *имеющая конечный ранг и являющаяся прямой суммой чистых подгрупп ранга* 1, *имеет конечный индекс в своей чистой оболочке* $\langle C \rangle_*$.

Если A — группа без кручения, t — некоторый тип, то множество $A(t) = \{a \in A \,|\, t(a) \geqslant t\}$ является подгруппой в A.

Пусть $\aleph_\sigma$ — кардинальное число. Группу называют $\aleph_\sigma$-*свободной*, если все ее подгруппы мощности $< \aleph_\sigma$ свободны.

Группу G называют *группой Уайтхеда* или просто W-*группой*, если $\operatorname{Ext}(G, \mathbb{Z}) = 0$.

Теорема 24.10. *Все* W-*группы узки,* $\aleph_1$-*свободны и сепарабельны.*

Говорят, что группа без кручения G *квазисодержится* в группе без кручения B ($G \preccurlyeq B$), если $nG \subseteq B$ для некоторого натурального n; G *квазиравна* группе B ($G \approx B$), если $G \preccurlyeq B$ и $B \preccurlyeq G$; G *квазиизоморфна* группе B ($G \sim B$), если существуют изоморфные группы G' и B' такие, что $B' \approx B$ и $G' \approx G$. Под (конечным) *квазиразложением* группы G понимается семейство ее подгрупп G_i ($i = 1, \ldots, n$) со свойством $G \approx \bigoplus\limits_{i=1}^{n} G_i$, G_i называются ее *квазислагаемыми.* Группа G называется *сильно неразложимой*, если она не имеет нетривиальных квазиразложений.

Вложим группу без кручения G в ее делимую оболочку V, группу V можно отождествить с тензорным произведением $V = G \otimes \mathbb{Q}$ (см. 22.54), V является векторным пространством над $\mathbb{Q}$. Отождествим G с ее образом при каноническом мономорфизме $G \to G \otimes \mathbb{Q}$, $x \to x \otimes 1$, $x \in G$. Положим $\mathbb{Q}\operatorname{End} G = (\operatorname{End} G) \otimes \mathbb{Q}$, где $\operatorname{End} G$ — кольцо эндоморфизмов группы G. Также отождествим $\operatorname{End} G$ с его образом при вложении $\operatorname{End} G \to (\operatorname{End} G) \otimes \mathbb{Q}$. Пространство V естественным образом превращается в $\mathbb{Q}\operatorname{End} G$-модуль. Кольцо $\mathbb{Q}\operatorname{End} G$ называется *кольцом* (или *алгеброй*) *квазиэндоморфизмов* группы G.

Различные разложения группы без кручения даже конечного ранга в прямую сумму неразложимых групп могут быть неизоморфными. Более того, для любых натуральных чисел $n > k > 1$ можно найти такую группу без кручения G ранга n, что для всякого разбиения числа n на k слагаемых $n = r_1 + \ldots + r_k$, где все $r_i \geqslant 1$, существует прямое разложение $G = G_1 \oplus \ldots \oplus G_k$ на неразложимые группы G_i ранга r_i. Замена изоморфизма на более слабое понятие квазиизоморфизма приводит к теореме единственности в несколько ослабленном смысле.

Теорема 24.11. *Пусть A — группа без кручения конечного ранга и $A \approx A_1 \oplus \ldots \oplus A_m \approx C_1 \oplus \ldots \oplus C_n$, где все группы A_i и C_j сильно неразложимы. Тогда $m = n$ и при подходящей перенумерации $A_i \sim C_i$ для всех i.*

Задачи

24.1. Пусть A — группа без кручения. Покажите, что:

а) $\chi_C(x) \leqslant \chi_A(x)$ для всех элементов x подгруппы $C \subseteq A$;

б) если $\chi(a) = (k_1, k_2, \ldots)$, то $\chi(p_n a) = (k_1, \ldots, k_{n-1}, k_n + 1, k_{n+1}, \ldots)$ (здесь $\infty + 1 = \infty$);

в) всякая последовательность $(k_1, k_2, \ldots)$ неотрицательных целых чисел и символов ∞ является характеристикой, а именно характеристикой элемента 1 в подгруппе группы $\mathbb{Q}$, порожденной всеми элементами вида $p_n^{-l_n}$, где $l_n \leqslant k_n$ при всех n;

г) $\chi(b + c) \geqslant \chi(b) \cap \chi(c)$ для всех b, $c \in A$, а если $A = B \oplus C$ и $b \in B$, $c \in C$, то $\chi(b + c) = \chi(b) \cap \chi(c)$;

д) если B — группа без кручения, то $\chi_A(a) \leqslant \chi_B(\alpha a)$ для всякого гомоморфизма $\alpha\colon A \to B$ и произвольного $a \in A$.

24.2. Пусть A — группа без кручения. Тогда $A(t)$ — ее чистая вполне инвариантная подгруппа, а если $C \subseteq A$ — чистая подгруппа, то подгруппа $C(t)$ также чиста в A.

24.3. Пусть A и B — группы без кручения ранга 1. Группа B изоморфна некоторой подгруппе группы A в том и только в том случае, когда $t(B) \leqslant t(A)$.

24.4. Попарно неизоморфные подгруппы данной группы без кручения ранга 1 образуют либо конечное, либо континуальное семейство.

24.5. Вполне разложимая группа без кручения $A = \bigoplus\limits_{i \in I} A_i$, где $r(A_i) = 1$, имеет коммутативную группу автоморфизмов тогда и только тогда, когда типы групп A_i попарно несравнимы.

24.6. Опишите все группы A без кручения ранга 1, группы автоморфизмов которых изоморфны $\mathbb{Z}_2$.

24.7. Если группа без кручения A имеет конечный ранг, то множество $T(A)$ типов всех ее ненулевых элементов удовлетворяет условию максимальности и условию минимальности.

Приведите примеры групп без кручения A конечного ранга, множество $T(A)$ которых бесконечно.

24.8. Множество неизоморфных групп без кручения конечного ранга имеет мощность континуума.

24.9. 1) Группа сепарабельна в точности тогда, когда ее редуцированная часть сепарабельна.

2) Прямые суммы сепарабельных групп сепарабельны.

3) Всякая вполне инвариантная подгруппа сепарабельной группы является сепарабельной.

4) Если C — вполне инвариантная чистая подгруппа сепарабельной группы без кручения A, то группа A/C сепарабельна.

24.10. Счетная сепарабельная группа без кручения вполне разложима.

24.11. 1) Однородная группа сепарабельна тогда и только тогда, когда каждая ее чистая подгруппа конечного ранга является для группы прямым слагаемым.

2) Чистые подгруппы однородных сепарабельных групп сепарабельны.

24.12. Каждая чистая подгруппа конечного ранга группы без кручения A служит для A прямым слагаемым тогда и только тогда, когда редуцированная часть группы A является однородной сепарабельной группой.

24.13. Тензорное произведение двух сепарабельных групп без кручения также сепарабельно.

24.14. p-чистые подгруппы группы $\widehat{\mathbb{Z}}_p$ неразложимы.

24.15. Группу без кручения называют *связной*, если все ее факторгруппы по ненулевым чистым подгруппам делимы. Покажите, что:

а) чистые подгруппы группы $\widehat{\mathbb{Z}}_p$ связны;

б) группа A связна в том и только в том случае, когда для любого простого числа p группа A либо p-делима, либо изоморфна некоторой p-чистой подгруппе группы $\widehat{\mathbb{Z}}_p$.

24.16. Для групп B и G без кручения проверьте, что:

а) $B \sim G$ в точности тогда, когда существуют подгруппы B' в B, G' в G и числа $m, n \in \mathbb{N}$ такие, что $mB \subseteq B'$, $nG \subseteq G'$ и $B' \cong G'$;

б) если B и G имеют конечные ранги, то наличие квазиизоморфизма $B \sim G$ равносильно тому, что B изоморфна некоторой подгруппе конечного индекса группы G.

Введем *категорию квазигомоморфизмов* **QTF**. Объекты в **QTF** — группы без кручения, множество морфизмов из группы A в группу B есть $\operatorname{Hom}(A, B) \otimes \mathbb{Q}$.

24.17. Проверьте, что **QTF** действительно является категорией (см. также 25.19).

24.18. Пусть B и G — группы без кручения. Тогда если $B \approx G$, то $\mathbb{Q}\operatorname{End} B = \mathbb{Q}\operatorname{End} G$, если же $B \sim G$, то $\mathbb{Q}\operatorname{End} B \cong \mathbb{Q}\operatorname{End} G$.

24.19. Пусть G — группа без кручения, $\mathbb{Q}\operatorname{End} G = \bigoplus_{i=1}^{n} e_i(\mathbb{Q}\operatorname{End} G)$ — разложение кольца $\mathbb{Q}\operatorname{End} G$ в прямую сумму правых идеалов ($e_1, \ldots, e_n$ — полная система ортогональных идемпотентов). Покажите, что $G \approx \bigoplus_{i=1}^{n} e_i G$. Кроме того, $\mathbb{Q}\operatorname{End} e_i(G) \cong e_i(\mathbb{Q}\operatorname{End} G)e_i$ и $e_i G$ — сильно неразложимая группа тогда и только тогда, когда $e_i(\mathbb{Q}\operatorname{End} G)$ — неразложимый $\mathbb{Q}\operatorname{End} G$-модуль. Если e и f — идемпотенты кольца $\mathbb{Q}\operatorname{End} G$, то $eG \sim fG$ в точности тогда, когда $e(\mathbb{Q}\operatorname{End} G)$ и $f(\mathbb{Q}\operatorname{End} G)$ изоморфны как $\mathbb{Q}\operatorname{End} G$-модули.

24.20. Соответствия $H \to H^*$ (H^* — подпространство, порожденное H в V, где $V = G \otimes \mathbb{Q}$), $W \to W \cap G$ являются взаимно обратными между чистыми вполне инвариантными подгруппами группы G и подмодулями $\mathbb{Q}\operatorname{End} G$-модуля V.

24.21. Пусть A — такая группа без кручения, что $|A/pA| \leqslant p$ для каждого простого числа p. Тогда если группа без кручения B квазиизоморфна A, то $B \cong A$.

24.22. Группа без кручения конечного ранга квазиразложима в прямую сумму сильно неразложимых подгрупп.

24.23. Пусть A — группа без кручения конечного ранга. Тогда ее подгруппа, изоморфная A, имеет конечный индекс.

24.24. Кольцо квазиэндоморфизмов группы без кручения A конечного ранга локально в том и только в том случае, когда A — сильно неразложимая группа.

24.25. Редуцированный конечно или счетно порожденный $\widehat{\mathbb{Z}}_p$-модуль без кручения свободен.

24.26. 1) Группа без кручения G узка в том и только в том случае, когда для любого гомоморфизма $\eta\colon \prod_n \langle e_n \rangle \to G$ группа $\operatorname{Im}\eta$ является конечно порожденной.

2) Группа без кручения G узка, если чистая подгруппа H, а также факторгруппа G/H узки.

24.27. Пусть G — узкая группа, A_i ($i \in I$) — группы без кручения и множество I неизмеримо. Тогда существует естественный изоморфизм $\operatorname{Hom}(\prod_{i\in I} A_i, G) \cong \bigoplus_{i\in I} \operatorname{Hom}(A_i, G)$.

24.28. Пусть A_i ($i \in I$) — группы без кручения и множество I неизмеримо. Всякое узкое слагаемое группы $\prod_{i\in I} A_i$ изоморфно некоторому слагаемому прямой суммы конечного числа групп A_i.

24.29. Векторная группа вполне разложима тогда и только тогда, когда почти все ее множители изоморфны группе $\mathbb{Q}$.

Группа G без кручения конечного ранга называется *почти вполне разложимой*, если G содержит вполне разложимую подгруппу конечного индекса. Почти вполне разложимым группам посвящена книга [63].

24.30. 1) Зафиксируем три различных простых числа p_1, p_2, q. В векторном $\mathbb{Q}$-пространстве $\mathbb{Q}a \oplus \mathbb{Q}b$ с базисом a, b возьмем вполне разложимую подгруппу $A = \mathbb{Q}^{(p_1)}a \oplus \mathbb{Q}^{(p_2)}b$. Пусть G — подгруппа в $\mathbb{Q}a \oplus \mathbb{Q}b$, порожденная подгруппой A и элементом $q^{-1}(a+b)$, $G = \langle A, q^{-1}(a+b)\rangle$. Тогда G — неразложимая почти вполне разложимая группа и $G/A \cong \mathbb{Z}_q$.

2) Для любого $n > 2$ постройте неразложимую почти вполне разложимую группу ранга n.

24.31. 1) Свободные группы являются W-группами.

2) Подгруппы W-групп являются W-группами.

3) Прямые суммы W-групп являются W-группами.

4) W-группы являются группами без кручения.

5) W-группа конечного ранга свободна.

24.32. 1) Всякая однородная сепарабельная группа без кручения вполне транзитивна.

2) Если A — однородная вполне транзитивная группа, то всякая ее вполне инвариантная подгруппа имеет вид $A(\chi) = \{a \in A \mid \chi(a) \geqslant \chi\}$, где χ — некоторая характеристика.

3) Если всякая вполне инвариантная подгруппа группы A имеет вид $A(\chi)$, где χ — некоторая характеристика, то A вполне транзитивна.

4) Алгебраически компактные группы без кручения вполне транзитивны.

Пусть R_p — класс групп без кручения без ненулевых элементов бесконечной p-высоты. Если $a \in A \in R_p$ и $\xi \in \widehat{\mathbb{Z}}_p$, то через $\xi\, a$ обозначим элемент группы A, являющийся пределом в p-адической топологии последовательности $s_n(\xi)\, a$, где $s_n(\xi) = r_0 + r_1 p + \ldots + r_n p^n$ — n-я частичная сумма числа $\xi = r_0 + r_1 p + \ldots + r_n p^n + \ldots$. Таким образом, на группе A введена внешняя частичная операция умножения на целые p-адические числа. Множество $H_p^A(a) = \{\xi \in \widehat{\mathbb{Z}}_p \mid \xi\, a$ определено$\}$ называется *p-характеристикой* элемента a в группе $A \in R_p$. Группа $A \in R_p$ называется *p-циклической*, а элемент $a \in A$ — ее p-образующим, если для любого $b \in A$ существует $\xi \in \widehat{\mathbb{Z}}_p$ со свойством $b = \xi\, a$.

24.33. Для каждой группы $A \in R_p$ справедливо:

а) если $a \in A$ и $\xi,\ \eta \in H_p^A(a)$, то $\xi \pm \eta \in H_p^A(a)$ и $\xi\, a \pm \eta\, a = (\xi \pm \eta)a$;

б) если $a,\ b \in A$ и $\xi \in H_p^A(a) \cap H_p^B(b)$, то $\xi \in H_p^A(a \pm b)$ и $\xi\, a \pm \xi\, b = \xi(a \pm b)$;

в) если $0 \neq a \in A$, $\xi,\ \eta \in H_p^A(a)$ и $\xi\, a = \eta\, a$, то $\xi = \eta$;

г) если $a \in A$, то $H_p^A(a)$ является p-чистой подгруппой группы $\widehat{\mathbb{Z}}_p$, содержащей группу целых чисел.

24.34. Если A — p-чистая подгруппа группы $\widehat{\mathbb{Z}}_p$, содержащая группу целых чисел, то группа A является p-циклической, целое число 1 будет ее p-образующим и $H_p^A(1) = A$.

24.35. Для группы $A \in R_p$ эквивалентны следующие условия:

а) A — p-циклическая группа;

б) $|A/pA| = p$;

в) A — ненулевая p-чистая подгруппа группы $\widehat{\mathbb{Z}}_p$.

Две p-характеристики H_1, H_2 называются *эквивалентными*, если существуют числа $n,\ m \in \mathbb{N}$ со свойствами $nH_1 \subseteq H_2$, $mH_2 \subseteq H_1$. Класс эквивалентности называется *p-типом*. На множестве p-типов можно ввести отношение порядка $\leqslant$: $\tau_1 \leqslant \tau_2$ означает, что для p-характеристик $H_1 \in \tau_1$, $H_2 \in \tau_2$ найдется натуральное n со свойством $nH_1 \subseteq H_2$.

Группа $A \in R_p$ называется: *p-вполне транзитивной*, если для любых $a,\ b \in A$ таких, что $h_p^A(a) \leqslant h_p^A(b)$ и $H_p^A(a) \subseteq H_p^A(b)$ найдется $\varphi \in \operatorname{End} A$ со свойством $\varphi\, a = b$; *p-однородной*, если p-типы любых двух ее ненулевых элементов совпадают.

24.36. 1) Всякая p-однородная группа является однородной.

2) Две связные группы из класса R_p изоморфны тогда и только тогда, когда они содержат по ненулевому элементу одинакового p-типа.

3) Если A — p-вполне транзитивная группа такая, что все ее ненулевые эндоморфизмы являются мономорфизмами, $0 \neq a \in A$, то $(\operatorname{End} A)^+ \cong A\,(H_p^A(a))$.

4) Вполне транзитивная группа из класса R_p является p-вполне транзитивной.

5) Если однородная группа A p-вполне транзитивна для всякого $p \in \pi(A)$, то A является вполне транзитивной.

25 Смешанные группы

Теория смешанных групп некоторое время отставала в своем развитии от теории периодических групп и групп без кручения. Сейчас положение изменилось. Особенно активно изучаются прямые суммы групп ранга без кручения 1. Смешанные группы всегда разложимы. Смешанная группа A называется *расщепляющейся*, если ее периодическая часть служит для A прямым слагаемым.

Теорема 25.1. *Периодическая группа T обладает тем свойством, что всякая смешанная группа с периодической частью T расщепляется в том и только в том случае, когда T является прямой суммой делимой и ограниченной групп.*

Теорема 25.2. *Смешанная группа A расщепляется в том и только в том случае, когда существует такая цепочка $A_1 \subseteq A_2 \subseteq \ldots$ ее подгрупп, что $\bigcup\limits_n A_n = A$, причем для каждого n группа $t(A_n)$ ограничена и справедливо равенство $t(A/A_n) = (t(A) + A_n)/A_n$.*

Группа G называется *группой Бэра*, если $\operatorname{Ext}(G,\ T) = 0$ для любой периодической группы T.

Теорема 25.3. *Группы Бэра свободны.*

Отметим, что существуют несвободные группы G, для которых $\operatorname{Ext}(G,\ T) = 0$, где T — произвольная p-группа, а простое число p может быть каким угодно.

Группа A называется *квазирасщепляющейся*, если она содержит такую расщепляющуюся подгруппу B, что $nA \subseteq B$ для некоторого натурального n.

Теорема 25.4. *Квазирасщепляющиеся смешанные группы A со счетной факторгруппой $A/t(A)$ расщепляются.*

Пусть $p_1, p_2, \dots$ — последовательность всех простых чисел в порядке возрастания. Как и ранее, $h_p^*(a)$ обозначает обобщенную p-высоту элемента $a \in A$, т.е. $h_p^*(a) = \sigma$, если $a \in p^\sigma A \setminus p^{\sigma+1}A$ для порядкового числа σ; и $h_p^*(a) = \infty$, если $a \in p^\alpha A = p^{\alpha+1}A$ ($\sigma < \infty$ для каждого порядкового числа σ). С каждым элементом $a \in A$ можно связать *высотную матрицу* $\mathbb{H}(a)$, а именно следующую бесконечную матрицу:

$$\mathbb{H}(a) = \begin{bmatrix} h_{p_1}^*(a) & \dots & h_{p_1}^*(p_1^k a) & \dots \\ \dots & \dots & \dots & \dots \\ h_{p_n}^*(a) & \dots & h_{p_n}^*(p_n^k a) & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix} = [\sigma_{nk}],$$

элементы которой — порядковые числа или символ ∞. Из определения сразу следует, что матрица $\mathbb{H}(p_n a)$ получается из $\mathbb{H}(a)$ заменой n-й строки $\sigma_{n0}, \dots, \sigma_{nk}, \dots$ строкой $\sigma_{n\,1}, \dots, \sigma_{n,\,k+1}, \dots$.

Пусть a, b — элементы бесконечного порядка в группе A и $ra = sb$ для некоторых целых чисел r, $s \neq 0$. Из отмеченного выше свойства следует, что n-е строки матриц $\mathbb{H}(a) = [\sigma_{nk}]$ и $\mathbb{H}(b) = [\rho_{nk}]$ могут отличаться друг от друга только в том случае, когда $p_n \,|\, rs$, причем для этого p_n должны найтись целые числа l, $m \geqslant 0$ со свойством (1): $\sigma_{n,\,k+l} = \rho_{n,\,k+m}$ при всех k.

Учитывая сказанное, две $\omega \times \omega$-матрицы $[\sigma_{nk}]$ и $[\rho_{nk}]$ назовем *эквивалентными, если* n-е строки матриц совпадают для почти всех n, а для каждого из оставшихся n найдутся такие целые числа l, $m \geqslant 0$ (зависящие от n), что выполняется условие (1).

Если ранг без кручения группы A равен 1, то любые два ее элемента a, b бесконечного порядка имеют эквивалентные высотные матрицы. Следовательно, группе A можно поставить в соответствие однозначно определенный класс эквивалентности матриц, который обозначают через $\mathbb{H}(A)$.

Имеются хорошие структурные результаты для нерасщепляющихся смешанных групп из ряда важных классов. Одним из таких исходных является класс счетных смешанных групп ранга без кручения 1. А именно *две счетные смешанные группы ранга без кручения* 1 *изоморфны тогда и только тогда, когда их периодические части изоморфны и высотные матрицы этих групп эквивалентны.*

Пусть A — произвольная абелева группа. Она называется *вполне транзитивной*, если для любых a, $b \in A$ таких, что $\mathbb{H}(a) \leqslant \mathbb{H}(b)$ и $o(b) \,|\, o(a)$ следует существование $\varphi \in \operatorname{End} A$ со свойством $\varphi a = b$. Отметим, что если A — редуцированная группа, то условие $o(b) \,|\, o(a)$ в определении вполне транзитивной группы можно опустить (25.15), кроме того, группа вполне транзитивна в том и только в том случае, когда ее редуцированная часть вполне транзитивна (25.17 (2)). Данное определение расширяет понятие вполне транзитивности для периодических групп (§ 23) и групп без кручения (§ 24) на случай смешанных групп (см. 25.16).

Задачи

25.1. 1) Прямые слагаемые расщепляющихся групп расщепляются.

2) Подгруппа конечного индекса группы A расщепляется в том и только в том случае, когда A расщепляется.

3) Если A — расщепляющаяся группа, то всякая ее подгруппа, содержащая $t(A)$, также расщепляется.

4) Смешанная группа с периодической частью T не обязана расщепляться, даже если все ее подгруппы, содержащие T и имеющие ранг без кручения 1, расщепляются.

5) Если A — такая смешанная группа, что при некотором $n \in \mathbb{N}$ группа nA расщепляется, то и A расщепляется.

25.2. Пусть A — смешанная группа с ограниченной периодической частью T, и пусть $C = T \oplus H$ — чистая подгруппа группы A. Тогда $A = T \oplus G$ для некоторой подгруппы G, содержащей H.

25.3. Если T — редуцированная неограниченная периодическая группа, то $\operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T)$ является копериодической нерасщепляющейся смешанной группой с периодической частью, изоморфной T (см. 22.38 и 22.41).

25.4. Пусть $p_1, p_2, \dots$ — различные простые числа. Положим $T_1 = \bigoplus\limits_{i=1}^{\infty} \langle a_i \rangle$, где $o(a_i) = p_i$. Рассмотрим элемент $b_0 = (a_1, a_2, \dots) \in \prod\limits_i \langle a_i \rangle$. Покажите, что:

а) T_1 — периодическая часть группы $\prod\limits_i \langle a_i \rangle$;

б) группа $\prod\limits_i \langle a_i \rangle$ содержит такие однозначно определенные элементы b_i ($i = 1, 2, \dots$), что i-я координата элемента b_i есть 0 и выполняется равенство $p_i b_i = (a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots) = b_0 - a_i$;

в) группа $A_1 = \langle T_1, b_1, b_2, \dots \rangle$ не расщепляется.

Расщепляется ли $\prod\limits_i \langle a_i \rangle$?

25.5. Для простого числа p положим $T_2 = \bigoplus\limits_{i=1}^{\infty} \langle a_i \rangle$, где $o(a_i) = p^{2i}$. Рассмотрим элементы

$$b_i = (0, \dots, 0, a_i, pa_{i+1}, p^2 a_{i+2}, \dots) \in \prod_i \langle a_i \rangle.$$

Покажите, что элементы b_i имеют бесконечные порядки и удовлетворяют равенствам $pb_{i+1} = b_i - a_i$, а группа $A_2 = \langle T_2, b_1, b_2, \dots \rangle$ не расщепляется.

25.6. Следующие группы не расщепляются:

а) $\langle a_1, \dots, a_n, \dots ; pa_1 = \dots = p^n a_n = \dots \rangle$;

б) $\langle a_1, \dots, a_n, \dots ; p^2(a_1 - pa_2) = \dots = p^{2n}(a_n - pa_{n+1}) = \dots = 0 \rangle$.

25.7. Любые два прямых разложения расщепляющейся смешанной группы $A = T \oplus G$ обладают изоморфными продолжениями в том и только в том случае, когда этому условию удовлетворяют обе группы T и G.

25.8. Существуют ли эпиморфизмы $A_1 \to T_1$ (25.4) и $A_2 \to T_2$ (25.5)?

25.9. Приведите пример такой смешанной группы A, что ее периодическая часть не является эндоморфным образом группы A.

25.10. Пусть A — такая смешанная группа, что ее периодическая часть T содержит лишь конечное число p-компонент T_i. Покажите, что T является эндоморфным образом группы A в том и только в том случае, когда каждая T_i обладает этим свойством. Приведите контрпример в случае, когда A содержит бесконечное число p-компонент.

25.11. Для произвольной периодической группы T существует такая смешанная группа A с периодической частью T, что всякий периодический эпиморфный образ группы A является прямой суммой делимой и ограниченной групп.

25.12. Пусть существует автоморфизм смешанной группы A, действующий как умножение на -1 на ее периодической части T и индуцирующий тождественное отображение группы A/T. Покажите, что если $A[2] = 0$, то группа A расщепляется.

25.13. Пусть $T = \bigoplus\limits_{n=1}^{\infty} \mathbb{Z}_{p^n}$, а G есть p-адическое пополнение группы $\bigoplus\limits_{\aleph_0} \widehat{\mathbb{Z}}_p$. Тогда $G/pG \cong T/pT$. Поэтому существует эпиморфизм $\eta\colon G \to T/pT$, $\operatorname{Ker}\eta = pG$. Пусть, далее, группа A определяется диаграммой

$$\begin{array}{ccccccc} 0 \to & pT & \to T \to & T/pT & \to 0 \\ & \| & \uparrow & \uparrow\eta & \\ 0 \to & pT & \to A \to & G & \to 0 \end{array}$$

с точными строками и коммутативными квадратами. Покажите, что группу A можно определить следующим образом: $A = \{(g, h) \mid g \in G, h \in T, \text{ где } \eta g = h + pT\}$ (см. 19.27). Тогда $pA \subseteq pG \oplus pT \subseteq A$, значит, A — квазирасщепляющаяся группа. Покажите, что группа A не расщепляется.

25.14. Пусть A — такая подгруппа группы G, что G/A — группа без кручения. Тогда $p^\sigma A = A \cap p^\sigma G$ для всех порядковых чисел σ и простых чисел p.

25.15. Если A — редуцированная группа, то условие $o(b) \mid o(a)$ в определении вполне транзитивной группы можно опустить.

25.16. Пусть A — редуцированная группа без кручения. Покажите, что $\chi_A(a) \leqslant \chi_A(b)$ тогда и только тогда, когда $\mathbb{H}(a) \leqslant \mathbb{H}(b)$ для любых $a, b \in A$. Докажите соответствующее утверждение для p-групп.

25.17. 1) Прямые слагаемые вполне транзитивных групп вполне транзитивны.

2) Группа A вполне транзитивна в том и только в том случае, когда ее редуцированная часть вполне транзитивна.

25.18. Пусть $A = \prod\limits_{i \in I} A_i$ ($A = \bigoplus\limits_{i \in I} A_i$) и $\pi(A_i) \cap \pi(A_j) = \varnothing$ при $i \neq j$, где $\pi(G)$ — множество всех простых чисел p со свойством $pG \neq G$. Группа A вполне транзитивна в том и только в том случае, когда каждая группа A_i вполне транзитивна.

Определим *категорию Уокера* **Walk**. Объектами категории **Walk** служат группы, а множество морфизмов из группы A в группу C равно $\operatorname{Hom}(A, C)/\operatorname{Hom}(A, t(C))$.

25.19. Убедитесь, что **Walk** есть категория.

Абелеву группу A назовем *qc-группой*, если замыкание в $\mathbb{Z}$-адической и в p-адической топологии для каждого простого числа p любой ее чистой подгруппы является чистой подгруппой в A. Периодические qc-группы — это в

точности квазиполные группы. Всякая группа без кручения является qc-группой. Если G — подгруппа группы A, то обозначим через G_p^- — замыкание подгруппы G в p-адической топологии группы A.

25.20. 1) Редуцированная группа A является qc-группой тогда и только тогда, когда для любой чистой подгруппы G в A утверждение «G замкнута в $\mathbb{Z}$-адической топологии» (соответственно, в «p-адической топологии») эквивалентно утверждению «A/G — редуцированная группа» («p-редуцированная группа»).

2) Если A — qc-группа, то A^1 — ее делимая часть.

3) Любая группа без кручения является qc-группой, алгебраически компактные группы являются qc-группами, периодическая группа является qc-группой тогда и только тогда, когда она квазиполна.

4) Группа A является qc-группой тогда и только тогда, когда для каждого простого числа p и произвольной p-чистой подгруппы G в A следует, что подгруппа G_p^- чиста в A.

5) В группе A утверждение «для любой p-чистой подгруппы G в A следует, что подгруппа G_p^- чиста в A» справедливо тогда и только тогда, когда соответствующее утверждение выполняется в $A/p^\omega A$, причем $p^\omega A = \bigcap\limits_n p^n A$ — чистая подгруппа в A.

6) Редуцированная смешанная группа A является qc-группой тогда и только тогда, когда $t(A)$ — квазиполная группа, $A^1 = 0$ и для каждого простого числа p условие «H — p-чистая подгруппа без кручения (включая $H = 0$)» влечет, что H_p^- — p-чистая подгруппа в A.

25.21. Группы, в которых замыкание (в $\mathbb{Z}$-адической и в p-адической топологии для каждого простого числа p) любой чистой подгруппы является прямым слагаемым, называются *cs-группами*. Строение таких групп довольно хорошо изучено. Покажите, что:

а) алгебраически компактные группы являются cs-группами;

б) qc-группа является cs-группой, если всякая ее замкнутая в $\mathbb{Z}$-адической топологии чистая подгруппа служит прямым слагаемым в группе.

26 Кольца эндоморфизмов

С каждой абелевой группой A можно связать кольцо $\operatorname{End} A$ всех ее эндоморфизмов. Оно определяется во введении в § 8 (см. еще 8.1), о связях с эндоморфизмами модулей написано в начале §§ 15, 21. С одной стороны, теорию колец эндоморфизмов абелевых групп можно рассматривать как часть теории абелевых групп, а с другой — как ветвь теории колец эндоморфизмов модулей. Кольца эндоморфизмов абелевых групп являются прекрасным введением в общую теорию колец эндоморфизмов модулей. Проблематика теории колец эндоморфизмов формулируется следующим образом: найти различные соотношения между свойствами данной абелевой группы A и свойствами ее кольца эндоморфизмов $\operatorname{End} A$. Отметим совпадение группы автоморфизмов $\operatorname{Aut} A$ группы A с группой обратимых элементов кольца $\operatorname{End} A$ (упр. 8.1). Подробное изложение теории колец эндоморфизмов абелевых групп представлено в книгах [23], [24].

Кольца эндоморфизмов допускают различные топологии, определяющиеся большей частью через соответствующие группы. Для конечного подмножества X группы A под *X-окрестностью* элемента $\alpha \in \operatorname{End} A$ понимают подмножество $U_X(\alpha) = \{\eta \in \operatorname{End} A \,|\, \eta x = \alpha x \text{ для всех } x \in X\}$. Ясно, что $U_X(\alpha) = \bigcap\limits_{x\in X} U_x(\alpha)$ и $U_X(\alpha) = \alpha + U_X(0)$. Поэтому *конечная топология* может быть определена с помощью подбазы окрестностей нуля: $U_x = \{\eta \in \operatorname{End} A \,|\, \eta x = 0\}$ для всех $x \in A$. Кольцо $\operatorname{End} A$ является полным в этой топологии.

Пусть $A = \oplus_{i=1}^n A_i$ и ε_i — соответствующие проекции, рассматриваемые как идемпотенты кольца $\operatorname{End} A$. Для $\alpha \in \operatorname{End} A$ и $a \in A$ имеем $\alpha\, a = \sum_{i=1}^n \alpha\varepsilon_i a = \sum_{i,j=1}^n (\varepsilon_j \alpha \varepsilon_i)\, a$. Поэтому с каждым $\alpha \in \operatorname{End} A$ ассоциируется $n\times n$-матрица: $\varphi\colon \alpha \mapsto [\alpha_{ji}]$, где $\alpha_{ji} = \varepsilon_j \alpha \varepsilon_i$. Если $\beta \in \operatorname{End} A$ и $[\beta_{ji}]$, где $\beta_{ji} = \varepsilon_j \beta \varepsilon_i$, — соответствующая матрица, то $\alpha - \beta$ и $\alpha\beta$ ассоциированы в точности с разностью $[\alpha_{ji} - \beta_{ji}]$ и произведением $[\sum_{k=1}^n \alpha_{jk}\beta_{ki}]$ матриц $[\alpha_{ji}]$ и $[\beta_{ji}]$ соответственно. Значит, φ — кольцевой гомоморфизм. Обратно, если $[\alpha_{ji}]$ — матрица с элементами $\alpha_{ji} \in \varepsilon_j(\operatorname{End} A)\varepsilon_i$, то она соответствует некоторому $\alpha \in \operatorname{End} A$, а именно $\alpha\, a = \sum_{i,j=1}^n \alpha_{ji} a$. Если отождествить $\operatorname{Hom}(A_i, A_j)$ с подгруппой $\varepsilon_j(\operatorname{End} A)\varepsilon_i$ из $\operatorname{End} A$, то получится

Теорема 26.1. *Если $A = \oplus_{i=1}^n A_i$ — прямое разложение группы A, то кольцо $\operatorname{End} A$ изоморфно кольцу всех $n \times n$-матриц $[\alpha_{ji}]$, $\alpha_{ji} \in \operatorname{Hom}(A_i, A_j)$.*

Отличительной чертой периодических групп является то, что они имеют «много» эндоморфизмов. Естественно поэтому ожидать наличие более тесных связей между периодической группой и ее кольцом эндоморфизмов. Это действительно так, кольца эндоморфизмов периодических групп определяют эти группы. Справедлив даже более общий факт.

Теорема 26.2. *Если A и C — периодические группы, кольца эндоморфизмов которых изоморфны, то всякий изоморфизм ψ между $\operatorname{End} A$ и $\operatorname{End} C$ индуцируется некоторым групповым изоморфизмом $\varphi\colon C \to A$, т.е. $\psi : \eta \mapsto \varphi^{-1}\eta\varphi$, $\eta \in \operatorname{End} A$.*

Для периодических сепарабельных групп можно полностью ответить на вопрос, когда данное кольцо реализуется в качестве кольца эндоморфизмов некоторой абелевой группы. Сначала выделим ряд свойств таких колец. Общий случай сразу сводится к примарным группам.

Пусть A — сепарабельная p-группа. Обозначим через E_0 левый идеал кольца $\operatorname{End} A$, порожденный его примитивными идемпотентами. Так как примитивные идемпотенты соответствуют неразложимым прямым слагаемым, эти идемпотенты в рассматриваемом случае имеют конечный порядок.

1) *Правый аннулятор кольца* E_0 *в* $\operatorname{End} A$ *равен нулю.*

2) *Если* η, ν — *примитивные идемпотенты кольца* $\operatorname{End} A$, *то* $\eta(\operatorname{End} A)\nu$ — *циклическая группа порядка* p^k *для некоторого* k.

3) *Если* η, ν — *примитивные идемпотенты кольца* $\operatorname{End} A$ *и* $o(\eta) \leqslant o(\nu)$, *то левый аннулятор кольца* $(\operatorname{End} A)\nu$ *содержится в левом аннуляторе кольца* $(\operatorname{End} A)\eta$ *и* $(\operatorname{End} A)\eta(\operatorname{End} A)\nu = (\operatorname{End} A)\nu[o(\eta)]$.

4) *Если* $E_0 = K \oplus L$, *где* K, L — *правые идеалы и* $K \neq 0$, *то* $\tau L = 0$ *для некоторого примитивного идемпотента* $\tau \in E_0$.

5) $\operatorname{End} A$ *служит пополнением для* E_0 *в топологии, в которой в качестве подбазы окрестностей нуля в* E_0 *взяты левые аннуляторы примитивных идемпотентов из* E_0.

Теорема 26.3. *Ассоциативное кольцо с единицей изоморфно кольцу эндоморфизмов некоторой сепарабельной* p*-группы тогда и только тогда, когда оно обладает свойствами* 1) – 5).

В случае групп без кручения на кольца их эндоморфизмов налагается меньше ограничений. Так, справедлива

Теорема 26.4 (Корнер). 1) *Всякое счетное кольцо с единицей, аддитивная группа которого является редуцированной группой без кручения, изоморфно кольцу эндоморфизмов некоторой счетной редуцированной группы без кручения.*

2) *Всякое кольцо с единицей, аддитивная группа которого является редуцированной группой без кручения конечного ранга* n, *изоморфно кольцу эндоморфизмов редуцированной группы без кручения ранга не больше* $2n$.

В дополнение к теоремам 26.3, 26.4 отметим, что в настоящее время задача выяснения, когда абстрактное кольцо является кольцом эндоморфизмов, полностью решена для различных весьма обширных классов колец.

Можно накладывать те или иные кольцевые условия на кольца эндоморфизмов и пытаться узнать, как они отражаются на свойствах соответствующих групп.

Теорема 26.5. *Кольцо эндоморфизмов группы* A *является артиновым слева* (*или справа*) *тогда и только тогда, когда* $A = B \oplus D$, *где* B — *конечная группа, а* D — *делимая группа без кручения конечного ранга.*

Теорема 26.6. *Пусть* A — *периодическая группа. Кольцо* $\operatorname{End} A$ *нетерово слева* (*или справа*) *тогда и только тогда, когда* A — *прямая сумма конечного числа коциклических групп.*

Напомним, что элемент α кольца R называется *регулярным*, если $\alpha\beta\alpha = \alpha$ для некоторого $\beta \in R$.

Теорема 26.7. 1) *Если* A — *периодическая группа, то кольцо* $\operatorname{End} A$ *регулярно в точности тогда, когда* A — *элементарная группа.*

2) *Если* A — *нередуцированная группа, то для регулярности кольца* $\operatorname{End} A$ *необходимо и достаточно, чтобы* A *была прямой суммой делимой группы без кручения и элементарной группы.*

3) *Если* A — *смешанная редуцированная группа и* $\operatorname{End} A$ — *регулярное кольцо, то* $t(A)$ — *элементарная группа,* $A/t(A)$ — *делимая группа и* $\bigoplus\limits_p A_p \subset A \subseteq \prod\limits_p A_p$ (при естественном отождествлении).

4) *Пусть* A — *такая смешанная группа, что* $t(A)$ — *элементарная группа,* $A/t(A)$ — *делимая группа конечного ранга и справедливы включения из* 3). *Тогда* $\operatorname{End} A/\operatorname{Hom}(A, t(A))$ — *конечномерная* $\mathbb{Q}$*-алгебра. Регулярность кольца* $\operatorname{End} A$ *эквивалентна тому, что* $\operatorname{End} A/\operatorname{Hom}(A, t(A))$ — *полупростая алгебра и* $A = C \oplus B$, *где* C — *смешанная самомалая группа,* B — *элементарная группа и ненулевые* p*-компоненты групп* C *и* B *относятся к различным* p (самомалые группы есть в 21.31).

Другие направления теории колец эндоморфизмов — это рассмотрение группы как модуля над своим кольцом эндоморфизмов (26.27 – 26.30) и описание радикалов (26.37 – 26.39).

Задачи

26.1. Пусть A — группа и $R = \operatorname{End} A$. Проверьте справедливость равенств $C = \operatorname{End}_R A$ и $\operatorname{End} A = \operatorname{End}_C A$, где C — центр кольца $\operatorname{End} A$.

26.2. Докажите, что:

$\operatorname{End}(\mathbb{Q}\oplus\mathbb{Z})\cong\begin{pmatrix}\mathbb{Q}&\mathbb{Q}\\0&\mathbb{Z}\end{pmatrix}$ и $\operatorname{End}(\mathbb{Z}_m\oplus\mathbb{Z})\cong\begin{pmatrix}\mathbb{Z}_m&\mathbb{Z}_m\\0&\mathbb{Z}\end{pmatrix}$ (см. 13.82 и 17.14).

26.3. Кольца $F_p\times F_p$, $\mathbb{Q}\times\mathbb{Q}$ и $\widehat{\mathbb{Z}}_p\times\widehat{\mathbb{Z}}_p$ не изоморфны кольцу эндоморфизмов никакой абелевой группы. То же справедливо и для колец матриц $\begin{pmatrix}\mathbb{Z}&\mathbb{Q}\\0&\mathbb{Q}\end{pmatrix}$ и $\begin{pmatrix}F_p&0\\F_p&\mathbb{Z}\end{pmatrix}$, где F_p — поле из p элементов.

26.4. Пусть C — центр кольца $\operatorname{End}A$, $\alpha\in C$. Тогда:

а) подгруппы $\operatorname{Im}\alpha$ и $\operatorname{Ker}\alpha$ вполне инвариантны;

б) если $A=\oplus A_i$, то $\alpha A_i\subseteq A_i$.

В частности, прямые слагаемые группы с коммутативным кольцом эндоморфизмов вполне инвариантны.

26.5. Покажите, что кольцо эндоморфизмов свободной группы конечного ранга n изоморфно кольцу целочисленных матриц порядка n. Рассмотрите кольца эндоморфизмов делимой группы без кручения, делимой p-группы и др.

26.6. 1) Групповой изоморфизм $\varphi\colon A\to C$ индуцирует кольцевой изоморфизм $\varphi^*\colon\operatorname{End}A\to\operatorname{End}C$, где $\varphi^*\colon\alpha\mapsto\varphi\alpha\varphi^{-1}$, $\alpha\in\operatorname{End}A$.

2) Если $A=B\oplus C$ и $\varepsilon\colon A\to B$ — соответствующая проекция, то можно произвести отождествление $\operatorname{End}B=\varepsilon(\operatorname{End}A)\varepsilon$.

3) Если группы $A=B\oplus C$ и A' имеют изоморфные кольца эндоморфизмов и $\psi\colon\operatorname{End}A\to\operatorname{End}A'$ — изоморфизм, то $A'=B'\oplus C'$, причем ψ индуцирует изоморфизмы $\operatorname{End}B\to\operatorname{End}B'$ и $\operatorname{End}C\to\operatorname{End}C'$.

4) Существует взаимно однозначное соответствие между конечными прямыми разложениями $A=A_1\oplus\ldots\oplus A_n$ группы A и разложениями кольца $\operatorname{End}A$ в конечные прямые суммы левых идеалов $\operatorname{End}A=L_1\oplus\ldots\oplus L_n$: если $A_i=\varepsilon_iA$, где $\varepsilon_1,\ldots,\varepsilon_n$ — попарно ортогональные идемпотенты, то $L_i=(\operatorname{End}A)\varepsilon_i$.

5) Группу $\operatorname{Hom}(A,C)$, где $C\subseteq A$, можно рассматривать как правый идеал кольца $\operatorname{End}A$, если при этом подгруппа C вполне инвариантна в A, то получается идеал кольца $\operatorname{End}A$.

26.7. 1) Пусть $A=B\oplus C=B'\oplus C'$ и $\varepsilon\colon A\to B$, $\varepsilon'\colon A\to B'$ — соответствующие проекции. Покажите, что $B\cong B'$ в том и только в том случае, когда существуют такие элементы α, $\beta\in\operatorname{End}A$, что $\alpha\beta=\varepsilon$ и $\beta\alpha=\varepsilon'$.

2) Для проекций f,e группы A эквивалентны следующие условия:

а) существует такой $u\in\operatorname{Aut}A$, что $f=u^{-1}eu$;

б) $eA\cong fA$ и $(1-e)A\cong(1-f)A$.

26.8. Всякий автоморфизм кольца эндоморфизмов периодической группы является внутренним.

26.9. Приведите примеры неизоморфных групп без кручения ранга 1 с изоморфными кольцами эндоморфизмов.

26.10. Две группы с изоморфными кольцами эндоморфизмов одновременно являются либо смешанными, либо нет.

26.11. Вычислите центры колец эндоморфизмов групп $\mathbb{Q}\oplus\mathbb{Z}$, $\mathbb{Z}_m\oplus\mathbb{Z}$ и $\mathbb{Z}_{p^n}\oplus\mathbb{Z}_{p^k}$.

26.12. *Орбита* $O_x=\{\eta x\,|\,\eta\in\operatorname{End}A\}$ элемента $x\in A$ является вполне инвариантной подгруппой, изоморфной факторгруппе $\operatorname{End}A/U_x$, где $U_x=\{\eta\,|\,\eta x=0\}$.

26.13. Пусть $\widehat{A}$ является $\mathbb{Z}$-адическим пополнением группы A со свойством $A^1=0$. Тогда для любого $\eta\in\operatorname{End}A$ существует ровно один $\widehat{\eta}\in\operatorname{End}(\widehat{A})$ такой, что $\widehat{\eta}\,|\,A=\eta$.

26.14. Пусть $A=\oplus A_i$. Тогда $\operatorname{End}A$ содержит подкольцо, изоморфное $\prod\operatorname{End}A_i$, а если все A_i — вполне инвариантные подгруппы группы A, то $\operatorname{End}A\cong\prod\operatorname{End}A_i$.

26.15. Кольцо эндоморфизмов абелевой группы является полным топологическим кольцом в конечной топологии.

26.16. Конечную топологию кольца $\operatorname{End}A$ редуцированной периодической группы A можно определить, взяв в качестве подбазы окрестностей нуля совокупность левых аннуляторов элементов $\eta\varepsilon$, где $\eta\in\operatorname{End}A$ и ε — примитивный идемпотент.

Если группа сепарабельна, то достаточно взять лишь левые аннуляторы примитивных идемпотентов.

26.17. Если A — сепарабельная p-группа, то в конечной топологии E_0 плотно в $\operatorname{End}A$ и $\operatorname{End}A$ — пополнение кольца E_0.

26.18. Кольцо $\operatorname{End}A$ группы A компактно в конечной топологии тогда и только тогда, когда A — периодическая группа, p-компоненты которой — конечные прямые суммы циклических групп.

26.19. Для периодической группы A ее $\mathbb{Z}$-адическая топология тоньше топологии конечных индексов.

26.20. 1) Конечная топология кольца эндоморфизмов группы без кручения конечного ранга дискретна.

2) Если A — бесконечная группа и $|\operatorname{End}A|>|A|$, то $\operatorname{End}A$ не дискретно в конечной топологии.

3) Если A — сепарабельная p-группа с базисной подгруппой B, то в конечной топологии $\operatorname{End}A$ — замкнутое подкольцо в $\operatorname{End}\overline{B}$.

26.21. Кольцо эндоморфизмов периодической группы A коммутативно тогда и только тогда, когда A — подгруппа группы $\mathbb{Q}/\mathbb{Z}$.

Кольцо R называется *инвариантным справа* (*слева*), если для любых a, $b \in R$ найдется $c \in R$ со свойством $ab = bc$ ($ab = ca$).

26.22. Если кольцо $\operatorname{End} A$ инвариантно справа (слева), то все образы (ядра) эндоморфизмов группы A вполне инвариантны.

26.23. Для периодической группы A любая инвариантность (левая или правая) кольца $\operatorname{End} A$ эквивалентна его коммутативности; коммутативность $\operatorname{End} A$ эквивалентна также тому, что все эндоморфные образы группы A вполне инвариантны в A.

26.24. Пусть A — сепарабельная группа без кручения. Следующие свойства эквивалентны:

а) кольцо $\operatorname{End} A$ коммутативно;

б) $\operatorname{End} A$ — инвариантное справа (слева) кольцо;

в) все образы (ядра) эндоморфизмов группы A вполне инвариантны;

г) $A = \oplus A_i$, где A_i — группы ранга 1 с попарно несравнимыми типами.

26.25. Если кольцо $\operatorname{End} A$ коммутативно, то p-компоненты A_p группы A являются коциклическими и $A/t(A)$ делится на те простые числа p, для которых $A_p \neq 0$.

26.26. 1) Если кольцо $\operatorname{End} A$ локально и $pA \neq A$, то $qA = A$ для всякого простого числа $q \neq p$.

2) Группа A с локальным кольцом $\operatorname{End} A$ является либо коциклической, либо неразложимой группой без кручения.

Действие всякого эндоморфизма $\alpha \in \operatorname{End} A$ на группе A: $\alpha \cdot a = \alpha(a)$, $a \in A$, задает на ней структуру левого модуля над кольцом $\operatorname{End} A$. Под *эндосвойством* группы понимается ее свойство как модуля над кольцом эндоморфизмов этой группы.

26.27. 1) Группа A эндоартинова тогда и только тогда, когда $A = B \oplus D$, где B — ограниченная группа и D — делимая группа с конечным числом ненулевых p-компонент.

2) Группа A эндонетерова тогда и только тогда, когда $A = B \oplus C$, где B — ограниченная группа и C — эндонетерова группа без кручения.

26.28. Артинов (нетеров) модуль является эндоартиновой (эндонетеровой) группой.

26.29. Пусть A — эндоартинова (эндонетерова) группа, G — вполне инвариантная подгруппа в A. Тогда группы G и A/G также эндоартиновы (эндонетеровы).

26.30. Пусть A — группа без кручения конечного ранга. Тогда $\mathbb{Q}\operatorname{End} A$-модуль $A \otimes \mathbb{Q}$ артинов и нетеров.

26.31. Рассмотрев кольца $\widehat{\mathbb{Z}}_p \oplus \widehat{\mathbb{Z}}_p$, $\mathbb{Q} \oplus \mathbb{Q}$ и $F_p \oplus F_p$, покажите, что в теореме 26.4 каждое из трех условий на аддитивную группу кольца: 1) счетность, 2) редуцированность, 3) свойство быть группой без кручения, существенно.

26.32. Рассмотрев кольцо $\mathbb{Z} \oplus \mathbb{Z}$ и кольцо целых гауссовых чисел $\mathbb{Z}[i]$, покажите, что существуют группы без кручения конечного ранга с изоморфными группами эндоморфизмов, кольца эндоморфизмов которых не изоморфны.

Пусть R — кольцо. Отображение, ставящее в соответствие элементу $r \in R$ эндоморфизм $x \mapsto rx$, $x \in R$, аддитивной группы R^+, является кольцевым гомоморфизмом $R \to \operatorname{End} R^+$. Это так называемое *левое регулярное представление* кольца R. Кольцо R называется *E-кольцом*, если его левое регулярное представление есть изоморфизм.

26.33. 1) Следующие утверждения эквивалентны:

а) R есть E-кольцо;

б) если $\alpha \in \operatorname{End} R^+$ и $\alpha(1) = 0$, то $\alpha = 0$;

в) кольцо $\operatorname{End} R^+$ коммутативно.

2) E-кольцами являются следующие кольца: $\mathbb{Z}_n$, подкольца поля $\mathbb{Q}$, кольца $\widehat{\mathbb{Z}}_p$ и их чистые подкольца.

26.34. Кольцо эндоморфизмов группы A является телом тогда и только тогда, когда группа A изоморфна $\mathbb{Q}$ или $\mathbb{Z}_p$ при некотором p (т.е. группа A является аддитивной группой некоторого простого поля).

Тело служит кольцом эндоморфизмов абелевой группы в точности тогда, когда оно — простое поле.

26.35. Кольцо эндоморфизмов $\operatorname{End} A$ является простым кольцом (т.е. не имеющим нетривиальных идеалов) тогда и только тогда, когда A — конечная прямая сумма групп, изоморфных группе $\mathbb{Q}$, или конечная прямая сумма циклических групп фиксированного простого порядка p.

Простое кольцо служит кольцом эндоморфизмов абелевой группы тогда и только тогда, когда оно — полное кольцо матриц конечного порядка над простым полем.

26.36. Кольца эндоморфизмов следующих групп являются чистыми:

а) делимые группы;

б) периодически полные (следовательно, ограниченные, конечные) p-группы (чистые кольца определены перед 11.11).

Элемент x кольца R с единицей называется *квазирегулярным,* если $1 + x$ — обратимый элемент; в этом случае элемент $x' = (1 + x)^{-1} - 1$ называется *квазиобратным* к элементу x.

26.37. Пусть A — p-группа, $\theta \in \operatorname{End} A$. Покажите, что $\sum_{n=1}^{\infty}(-1)^n p^n \theta^n$ — элемент, квазиобратный к $p\theta$. Выведите отсюда, что радикал Джекобсона кольца $\operatorname{End} A$ равен нулю тогда и только тогда, когда A — элементарная группа.

Введем *идеал Пирса* $H(A)$ редуцированной p-группы A, полагая $H(A) = \{\alpha \in \operatorname{End} A \mid$ если $x \in A[p]$ и $h(x) < \infty$, то $h(x) < h(\alpha x)\}$ (здесь $h(\dots)$ обозначает высоту соответствующего элемента).

26.38. 1) Для любой редуцированной p-группы A справедливо включение $J(\operatorname{End} A) \subseteq H(A)$.

2) Если A — конечная p-группа, более общо, периодически полная p-группа, то $J(\operatorname{End} A) = H(A)$.

Для редуцированной группы без кручения A положим $H(A) = \{\alpha \in \operatorname{End} A \mid$ если $x \in A$ и $h_p(x) < \infty$, то $h_p(x) < h_p(\alpha x)$ для каждого p с $pA \neq A\}$.

26.39. Пусть A — редуцированная группа без кручения конечного ранга. Тогда ниль-идеалы кольца $\operatorname{End} A$ нильпотентны и $H(A) \subseteq J(\operatorname{End} A)$.

26.40. 1) Кольцо эндоморфизмов чистой подгруппы конечного ранга группы $\widehat{\mathbb{Z}}_p$ локально.

2) Пусть A и C — чистые подкольца конечного ранга в кольце $\widehat{\mathbb{Z}}_p$ (групповая терминология, примененная к этим кольцам, относится к их аддитивным группам), $\pi\colon \widehat{\mathbb{Z}}_p \to \mathbb{Z}_p$ — канонический эпиморфизм,

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \Big| \, a \in A, b \in \widehat{\mathbb{Z}}_p, c \in C, \pi(a) = \pi(c) \right\}.$$

Тогда кольцо R локально.

27 Аддитивные группы колец

Кольцо R (не обязательно ассоциативное и с 1), аддитивная группа R^+ которого совпадает или изоморфна группе A, называется *кольцом на группе* A. Свойства аддитивной группы кольца в этом параграфе переносятся на само кольцо, например, *делимое* или *редуцированное* кольцо, *p-кольцо* и т.п. Кольцо, в котором все произведения равны 0, называется *нуль-кольцом.* Изучение аддитивных групп колец — еще одна линия, связывающая абелевы группы с кольцами. По традиции и характеру результатов это направление относят к теории абелевых групп.

Функция $\mu\colon A \times A \to A$ называется *умножением на группе* A, если для всех элементов a, b, $c \in A$ выполняются равенства

$$\mu(a, b + c) = \mu(a, b) + \mu(a, c), \quad \mu(b + c, a) = \mu(b, a) + \mu(c, a).$$

Всякое кольцо R на группе A задает некоторое умножение: $\mu(a, b) = ab$. Это соответствие между кольцевыми структурами и умножениями на группе A биективно. Кольцо R можно представлять как пару (A, μ).

Если μ и ν — умножения на группе A, то их *сумма* $\mu + \nu$ определяется по правилу: $(\mu + \nu)(a, b) = \mu(a, b) + \nu(a, b)$ для всех a, $b \in A$. Относительно введенной операции умножения образуют абелеву группу — *группу умножений на* A, $\operatorname{Mult} A$. Ассоциативные умножения образуют группу лишь в немногих случаях.

Теорема 27.1. *Имеют место изоморфизмы:*

$$\operatorname{Mult} A \cong \operatorname{Hom}(A \otimes A, A), \ \operatorname{Mult} A \cong \operatorname{Hom}(A, (\operatorname{End} A)^+).$$

На делимой периодической группе не существует иного умножения, кроме тривиального. Поэтому представляет интерес

Теорема 27.2. *Всякое кольцо без кручения может быть вложено как подкольцо в минимальное делимое кольцо без кручения, единственное с точностью до изоморфизма.*

Кольцевые структуры на группах продолжаются до кольцевых структур на чисто инъективных и копериодических оболочках этих групп.

Теорема 27.3. *Пусть G — чисто инъективная (копериодическая) оболочка группы A. Всякое частичное умножение $\nu\colon A \times A \to G$ может быть продолжено до умножения $\mu\colon G \times G \to G$, единственное, если группа G редуцированная.*

Теория периодических колец сводится к теории p-колец, а для последних справедлива следующая интересная теорема.

Теорема 27.4. *Умножение μ на p-группе A полностью определяется своими значениями $\mu(a_i, a_j)$, где элементы a_i и a_j пробегают p-базис группы A.*

Более того, для любого выбора значений $\mu(a_i, a_j) \in A$, где элементы a_i и a_j берутся из некоторого p-базиса группы A, при единственном условии, чтобы всегда выполнялось неравенство $o(\mu(a_i, a_j)) \leqslant \min(o(a_i), o(a_j))$, существует умножение на группе A, являющееся продолжением сопоставления $(a_i, a_j) \to \mu(a_i, a_j)$.

Абелеву группу называют *нильгруппой*, если она допускает лишь тривиальное умножение. Если же группа допускает лишь конечное число неизоморфных колец, то ее называют *квазинильгруппой*.

Теорема 27.5. *Периодическая группа является нильгруппой тогда и только тогда, когда она делима. Смешанных нильгрупп не существует.*

Периодическая группа является квазинильгруппой тогда и только тогда, когда $A = B \oplus D$, где B — конечная группа, D — делимая группа.

Теорема 27.6. *Кольцо без кручения ранга 1 либо является нуль-кольцом, либо изоморфно некоторому подкольцу поля рациональных чисел, имеющему вид $m\mathbb{Z}(q_j^{-1},\ j \in J)$, где $(m, q_j) = 1$. Группа без кручения ранга 1 не является нильгруппой, если и только если ее тип идемпотентен.*

Задачи

27.1. В каждом кольце R имеются следующие идеалы: nR и $R[n]$ для всякого n, периодическая часть $t(R)$ и ее p-компоненты, цоколь и делимая часть. Более общо, для всякого левого (правого) идеала L кольца R подобные подмножества также являются левыми (правыми) идеалами кольца R.

27.2. 1) Если R — периодическое кольцо, то R^1 — аннулятор кольца R, а разложение $R = \bigoplus\limits_p R_p$ является теоретико-кольцевым.

2) Если R — кольцо без кручения, то $\chi(ac) \geqslant \chi(a)\chi(c)$ для всех $a, c \in R$, поэтому для всякого идеала L и для всякого типа t подгруппы $L(\chi)$, $L(t)$ — идеалы кольца R (по поводу обозначений см. § 24).

3) В кольце R без кручения с единицей 1 всегда $\chi(1) \leqslant \chi(a)$ для всех $a \in R$.

4) Вполне инвариантные подгруппы группы R^+ всегда являются идеалами в кольце R независимо от того, каким образом в R определено умножение.

27.3. Обозначим через $I(A) = \langle \varphi A \,|\, \varphi \in \operatorname{Hom}(A, (\operatorname{End} A)^+)\rangle$ — подгруппу, порожденную всеми гомоморфными образами группы A в группе $(\operatorname{End} A)^+$. Покажите, что:

а) $I(A)$ — идеал кольца $\operatorname{End} A$;

б) подгруппа C группы A служит идеалом в каждом кольце на группе A, если и только если C является $I(A)$-допустимой подгруппой, т.е. $I(A)C \subseteq C$;

в) если A — редуцированная периодическая группа, то $I(A)$ — периодическая часть группы $(\operatorname{End} A)^+$.

27.4. В группе A только вполне инвариантные подгруппы являются идеалами в каждом кольце на A в том и только в том случае, когда для всякого $a \in A$ группа $(\operatorname{End} A)^+$ порождается единицей и подгруппами $I(A)$ и $\{\eta \in \operatorname{End} A \,|\, \eta a = 0\}$.

27.5. 1) Если A — циклическая группа, то $\operatorname{Mult} A \cong A$.

2) Если $mA = 0$, то $m \operatorname{Mult} A = 0$.

3) Если $pA = A$, то $\operatorname{Mult} A$ не содержит элементов порядка p.

4) Если группа A не содержит элементов порядка p, то их не содержит и группа $\operatorname{Mult} A$.

27.6. Умножения μ и ν определяют изоморфные кольца на группе A тогда и только тогда, когда существует автоморфизм α группы A, сохраняющий произведения, т.е. $\mu(a, b) = \alpha^{-1}\nu(\alpha a, \alpha b)$ при всех $a, b \in A$.

27.7. 1) Умножения, являющиеся коммутативными, образуют подгруппу $\operatorname{Mult}_c A$ группы $\operatorname{Mult} A$.

2) Если $C = \langle a \otimes b - b \otimes a \,|$ для всех $a, b \in A\rangle$, то $\operatorname{Mult}_c A \cong \operatorname{Hom}((A \otimes A)/C, A)$.

27.8. Приведите пример, показывающий, что ассоциативные умножения не образуют подгруппу в группе $\operatorname{Mult} A$.

27.9. 1) Умножения μ и ν на группе $\mathbb{Z}$ определяют изоморфные кольца тогда и только тогда, когда $\mu = \pm\nu$.

2) Существует бесконечно много неизоморфных колец на группе $\mathbb{Z}$, и каждое из них изоморфно $n\mathbb{Z}$ $(n > 0)$, либо нуль-кольцу на $\mathbb{Z}$.

27.10. 1) Умножения μ и ν на группе $\mathbb{Z}_m$ определяют изоморфные кольца тогда и только тогда, когда $\mu = k\nu$ при некотором k, для которого $(k, m) = 1$.

2) Каждое кольцо на группе $\mathbb{Z}_{p^n}$ изоморфно одному из колец $p^k\mathbb{Z}/p^{n+k}\mathbb{Z}$ $(k = 0, 1, \ldots, n)$.

27.11. Всякое кольцо на группе $\widehat{\mathbb{Z}}_p$ изоморфно одному из колец $p^k\widehat{\mathbb{Z}}_p$ ($k = 0, 1, \dots$) или нуль-кольцу на $\widehat{\mathbb{Z}}_p$.

27.12. Пусть C — чистая и плотная в $\mathbb{Z}$-адической топологии подгруппа редуцированной группы A. Тогда частичное умножение $\nu\colon C \times C \to A$ может быть продолжено до умножения $\mu\colon A \times A \to A$ не более чем одним способом.

27.13. Пусть R — кольцо без кручения и D — делимое кольцо, такое же, как в теореме 27.2. Установите взаимно однозначное соответствие между чистыми левыми идеалами в R и чистыми левыми идеалами в D. Проверьте, что при этом соответствии простые идеалы переходят в простые.

27.14. Если A — периодическая группа и $A^1 = 0$, то существует естественный изоморфизм $\operatorname{Mult}\widehat{A} \cong \operatorname{Mult} A$.

27.15. Если A — редуцированная периодическая группа и $A^\bullet$ — ее копериодическая оболочка, то существует естественный изоморфизм $\operatorname{Mult} A^\bullet \cong \operatorname{Mult} A$.

27.16. Пусть A — периодическая группа, $F = \bigcap\limits_p pA$ — ее подгруппа Фраттини. Тогда:

а) аннулятор всякого кольца на группе A содержит A^1;

б) всякий элемент из F порождает нильпотентный идеал в каждом кольце на A.

27.17. Пусть A — периодическая группа. Тогда:

а) подгруппа Фраттини F группы A содержится в радикале Джекобсона всякого ассоциативного кольца на группе A;

б) существует ассоциативное и коммутативное кольцо на группе A, радикал которого совпадает с F.

27.18. Постройте такое p-кольцо, которое не является нильпотентным, но каждый его элемент порождает нильпотентный идеал.

27.19. Всякий простой идеал и всякий максимальный идеал p-кольца R содержит pR.

27.20. Пусть R — некоторое p-кольцо. Тогда если каждый элемент из некоторой базисной подгруппы группы R^+ является нильпотентным, то и каждый элемент из R нильпотентен.

27.21. Радикал Джекобсона произвольного кольца на смешанной группе всегда содержит подгруппу Фраттини ее периодической части.

27.22. Для произвольного максимального левого идеала M кольца без кручения R либо $(R/M)^+$ — делимая группа без кручения, либо $pR \subseteq M$ при некотором простом числе p.

27.23. Пусть F — свободная группа и G — подгруппа группы F. Покажите, что существует такое кольцо R на группе F, что аддитивная группа кольца R^2 совпадает с G.

27.24. Свободная группа конечного ранга допускает счетное число попарно неизоморфных ассоциативных колец.

27.25. Пусть R, S, T — рациональные группы, содержащие целые числа, и $(R, S, T) = \{q \in \mathbb{Q} \mid qRS \subseteq T\}$. Покажите, что:

а) (R, S, T) — подгруппа группы $\mathbb{Q}$;

б) если $A = \bigoplus\limits_{i\in I} R_i$, где R_i — такие рациональные группы, что $(R_i, R_j, R_k) = 0$ при любом выборе индексов $i, j, k \in I$, то A — нильгруппа.

27.26. Существуют нильгруппы без кручения произвольного ранга.

27.27. 1) Если A, C — нильгруппы, то группа $A \oplus C$ не обязана быть нильгруппой.

2) Всякая ненулевая делимая группа без кручения служит аддитивной группой некоторого поля.

3) Группа A служит аддитивной группой некоторого булева кольца тогда и только тогда, когда A является элементарной 2-группой.

Глава VI. Поля

28 Простейшие свойства полей

Поле называется *простым*, если оно не содержит собственных подполей. Каждое поле P содержит единственное простое подполе, изоморфное полю рациональных чисел $\mathbb{Q}$ (в этом случае говорят, что поле P имеет *нулевую характеристику*) или полю F_p для некоторого простого числа p (поле P имеет *характеристику* p). Характеристика поля P обозначается через $\operatorname{char} P$.

Если некоторое поле K содержится в поле P, то поле P называется *расширением* поля K, а поле K — *подполем* поля P. Минимальное поле, содержащее поле K и элемент $\theta \in P$, называется *простым расширением поля* K, полученным путем присоединения к полю K элемента θ, и обозначается через $K(\theta)$. Элемент $\alpha \in P$ называется *алгебраическим* над K, если α является корнем некоторого многочлена $f(x) \in K[x]$, в противном случае α называется *трансцендентным* над K. Расширение P поля K называется *алгебраическим*, если всякий элемент из P алгебраичен над K.

В случае расширения $K \subset P$ размерность $\dim_K P$ векторного пространства P над K называется *степенью расширения* P *над* K и обозначается через $[P : K]$. Для трансцендентного элемента $\theta \in P$ семейство элементов $1, \theta, \theta^2, \ldots$ линейно независимо над K и $[K(\theta) : K] = \infty$. Если θ — алгебраический элемент над K, то $[K(\theta) : K] = n \in \mathbb{N}$ и каждый элемент $\alpha \in K(\theta)$ допускает однозначное представление в виде $\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, где $a_0, \ldots, a_{n-1} \in K$; в данном случае поле $K(\theta)$ совпадает с кольцом $K[\theta]$, где под $K[\theta]$ понимается кольцо, получающееся из кольца многочленов $K[x]$ формальной заменой переменной x на θ. Унитарный многочлен $f_\alpha(x) \in K[x]$ наименьшей степени со свойством $f(\alpha) = 0$ называется *минимальным многочленом* алгебраического элемента $\alpha \in P$; обозначают его $f_\alpha(x)$ или $f_\alpha(x, K)$, чтобы подчеркнуть роль поля K.

Пусть E, F — расширения поля K. Если E и F содержатся в некотором поле L, то через EF обозначают наименьшее подполе в L, содержащее E и F, оно называется *композитом* E и F в L.

Поле P называется *алгебраически замкнутым*, если каждый многочлен из кольца $P[x]$ разложим на линейные множители. Теорема Штейница утверждает, что для всякого поля существует алгебраически замкнутое расширение. Алгебраически замкнутое и алгебраическое расширение поля P определено однозначно с точностью до изоморфизма. Всякое такое расширение поля P называется его *алгебраическим замыканием*.

Расширение $P \subset F$ называется *конечным*, если оно получается из P присоединением конечного числа элементов $\alpha_1, \ldots, \alpha_m$, т.е. $F = P(\alpha_1, \ldots, \alpha_m)$. Конечное расширение является алгебраическим тогда и только тогда, когда оно имеет конечную степень.

Теорема 28.1. *Если $L \subset P \subset F$ и поле F конечно над L, а F конечно над P. Обратно, если P конечно над L, а F конечно над P, то F конечно над L и $[F : L] = [F : P]\,[P : L]$.*

Теорема 28.2. *Пусть K — поле, $E = K(\alpha)$, где α алгебраичен над K. Тогда если $\sigma\colon K \to L$ — вложение K в алгебраически замкнутое поле L, то число возможных продолжений σ до вложения E в L равно числу различных корней многочлена $f_\alpha(x) \in K[x]$.*

Теорема 28.3. *Пусть K — поле, P — его алгебраическое расширение и $\sigma\colon K \to F$ — вложение K в алгебраически замкнутое поле F. Тогда существует продолжение σ до вложения P в F. Если P алгебраически замкнуто и F алгебраично над σK, то любое такое продолжение σ будет изоморфизмом поля P на F.*

Задачи

28.1. Пусть n — фиксированное целое число. Образует ли поле относительно обычных матричных операций множество матриц вида

$$\left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} \mid a, b \in K \right\}, \text{ где:}$$

а) $K = \mathbb{Q}$; б) $K = \mathbb{R}$; в) $K = \mathbb{Z}$; г) $K = \mathbb{Z}_p$, а $p = 2, 3, 5, 7$?

28.2. Опишите поля, имеющие единственное собственное подполе.

28.3. Расширение $P \subset F$ поля P простой степени не имеет собственных ($\neq P, F$) подполей.

28.4. Простое тело (не имеющее собственных подтел) является полем.

28.5. Если A — коммутативная область, то $A[x]$ также коммутативная область. Если K — поле частных кольца A, то поле частных $K(x)$ кольца $A[x]$ называется его *полем рациональных дробей*. В случае нескольких переменных поле частных $K(x_1, \ldots, x_n)$ кольца $A[x_1, \ldots, x_n]$ называется *полем рациональных дробей* или *полем рациональных функций* от неизвестных $x_1, \ldots, x_n$.

28.6. 1) Элемент θ трансцендентен над полем P в точности тогда, когда существует изоморфизм расширения $P(\theta)$ на поле рациональных дробей, сохраняющий неподвижными элементы из P.

2) Поле рациональных дробей над конечным полем является бесконечным полем конечной характеристики.

28.7. Пусть $F = \mathbb{C}(x)$ — поле рациональных дробей. Тогда:

а) если $y = x^n + \dfrac{1}{x^n}$ и $K = \mathbb{C}(y)$, то $[F : K] = 2n$;

б) если $P = \mathbb{C}\left(x^2\right)$ и $E = \mathbb{C}\left(x^2 + x\right)$, то $[F : P] = [F : E] = 2$, но $[F : P \cap E] = \infty$.

28.8. Поле рациональных дробей $P(x)$ — бесконечное расширение поля P, но конечное расширение поля $P\left(x^n\right)$, $n \in \mathbb{N}$.

28.9. Множество всех элементов K-алгебры A с 1, алгебраических над K, является подалгеброй в A, а если A — поле, то подполем.

28.10. Покажите, что элемент α алгебраичен над полем P тогда и только тогда, когда степень расширения $[P(\alpha) : P]$ конечна. В случае алгебраичности α поле $P(\alpha)$ совпадает с алгеброй $P[\alpha]$ (под $P[\alpha]$ понимается алгебра, получающаяся из алгебры многочленов $P[x]$ формальной заменой x на α), а степень $[P(\alpha) : P]$ равна степени минимального многочлена $f_\alpha(x)$ элемента α над P. Покажите также, что алгебраичность α над P эквивалентна тому, что гомоморфизм $P[x] \to P(\alpha)$, тождественный на P и переводящий x в α, имеет ненулевое ядро, равное идеалу $(f_\alpha(x))$. Кроме того, $P[x]/(f_\alpha(x)) \cong P(\alpha)$ и многочлен $f_\alpha(x)$ неприводим.

28.11. Если каждый многочлен из $P[x]$ имеет в поле P хотя бы один корень, то P алгебраически замкнуто.

28.12. Пусть K — поле и F — поле дробей алгебры формальных степенных рядов $K[[x]]$. Покажите, что каждый элемент из F представим в виде $x^{-s}h$, где $s \geqslant 0$ и $h \in K[[x]]$, т.е. F состоит из степенных рядов, допускающих наряду с положительными степенями элемента x также и конечное число отрицательных степеней этого элемента (ряды Лорана, см. перед 11.25).

28.13. Для любого автоморфизма φ поля P множество элементов, неподвижных относительно φ, является подполем.

28.14. Пусть $P \subset F$ — расширение поля P. Покажите, что:

а) множество всех автоморфизмов поля F, оставляющих неподвижными элементы поля P, образует группу $\mathrm{Aut}\ F/P$;

б) если H — подгруппа в $\mathrm{Aut}\ F/P$, то $F^H = \{a \in F \mid \varphi(a) = a,\ \varphi \in H\}$ образует подполе в F, содержащее P.

28.15. Проверьте, что размерность расширения $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ над $\mathbb{Q}$ равна четырем, т.е. каждый элемент $\alpha \in F$ однозначно записывается в виде линейной комбинации $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ с рациональными a, b, c, d. Покажите, что $F = \mathbb{Q}\left(\theta, \theta^2, \theta^3\right)$, где $\theta = \sqrt{2} + \sqrt{3}$, т.е. в качестве базиса над $\mathbb{Q}$ можно выбрать элементы $1, \theta, \theta^2, \theta^3$. Элемент θ имеет минимальный многочлен $f_\theta(x) = x^4 - 10x^2 + 1$ с корнями $\theta_1 = \theta = \sqrt{2} + \sqrt{3}$, $\theta_2 = \sqrt{2} - \sqrt{3}$, $\theta_3 = -\sqrt{2} + \sqrt{3}$, $\theta_4 = -\sqrt{2} - \sqrt{3}$ (в частности, θ_i — целые алгебраические числа).

28.16. Какова степень $\mathbb{Q}\left(\sqrt{-2}\right)$ и $\mathbb{Q}\left(i, \sqrt{2}\right)$ над полем $\mathbb{Q}$?

28.17. 1) Для всякого алгебраического числа α совокупность всех аннулирующих многочленов для α является идеалом в кольце $\mathbb{Q}[x]$.

2) Множество всех алгебраических чисел образует поле, являющееся бесконечным расширением поля $\mathbb{Q}$.

28.18. 1) Рациональное число является целым алгебраическим тогда и только тогда, когда оно является целым числом.

2) Для того, чтобы алгебраическое число было целым алгебраическим, необходимо, чтобы его минимальный многочлен имел целые коэффициенты.

3) Множество всех целых алгебраических чисел образует кольцо — кольцо целых алгебраических чисел.

4) Всякое алгебраическое число представимо в виде β/q, где β — целое алгебраическое, q — целое число. В частности, поле алгебраических чисел является полем частных кольца целых алгебраических чисел.

28.19. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ и $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$. Покажите, что для $\alpha \neq 0$ верна импликация $f(\alpha) = 0 \Rightarrow F(1/\alpha) = 0$. Воспользовавшись этим, покажите, что целое алгебраическое число будет обратимым в кольце целых алгебраических чисел тогда и только тогда, когда его минимальный многочлен имеет свободный член, равный ± 1.

28.20. Пусть d — целое число, свободное от квадратов. Элемент $\alpha \in \mathbb{Q}(\sqrt{d})$ является целым алгебраическим числом, если $\alpha = \dfrac{a + b\sqrt{d}}{2}$, где a и b — целые числа такие, что

$$a \equiv b \pmod 2 \text{ при } d \equiv 1 \pmod 4 \text{ и } a \equiv b \equiv 0 \pmod 2 \text{ при } d \equiv 2, 3 \pmod 4.$$

28.21. Целые алгебраические числа полей:

а) $\mathbb{Q}\left(\sqrt{-2}\right)$ — это все числа вида $a + b\sqrt{-2}$, где $a, b \in \mathbb{Z}$;

б) $\mathbb{Q}\left(\sqrt{-3}\right)$ — это все числа вида $a + b\sqrt{-3}$, где $a, b \in \mathbb{Z}$, и все числа вида $\dfrac{a}{2} + \dfrac{b}{2}\sqrt{-3}$, где a, b — нечетные целые числа. Все их можно также представить в виде $m + n\dfrac{-1 + \sqrt{-3}}{2}$, где $m, n \in \mathbb{Z}$.

28.22. Целое алгебраическое число $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ обратимо в кольце целых алгебраических чисел поля $\mathbb{Q}(\sqrt{d})$ в точности тогда, когда норма $n(\alpha) = r^2 - ds^2 = \pm 1$.

28.23. Пусть d — отрицательное целое число, свободное от квадратов. Покажите, что целое алгебраическое число $\alpha \in \mathbb{Q}(\sqrt{d})$ обратимо в кольце целых алгебраических чисел, если $\alpha = \dfrac{a + b\sqrt{d}}{2}$, где $a, b \in \mathbb{Z}$ и $\dfrac{a^2 - b^2 d}{4} = 1$. Выведите отсюда, что единственные мнимые квадратичные поля, содержащие обратимые целые алгебраические элементы, отличные от ± 1, — это поле $\mathbb{Q}(i)$ (*поле гауссовых чисел*) и поле $\mathbb{Q}(\sqrt{-3})$.

28.24. 1) Всякое алгебраически замкнутое поле бесконечно.

2) Если P — бесконечное поле, то его алгебраическое замыкание $\overline{P}$ имеет ту же мощность, что и P.

3) Если P — конечное поле, то поле $\overline{P}$ — счетное.

28.25. 1) Всякая конечная подгруппа мультипликативной группы поля — циклическая.

2) Если P^* — циклическая группа, то поле P конечно.

3) В поле из n элементов выполняется тождество $x^n = x$.

4) Если $x^n = x$ для всех элементов поля K, то K конечно и его характеристика делит n.

28.26. Найдите какие-нибудь конкретные конечные нетривиальные подгруппы в $\mathbb{R}^*$ и в $\mathbb{C}^*$ и непосредственно покажите, что они циклические.

28.27. Опишите поля, аддитивная группа которых — циклическая.

28.28. В поле $\mathbb{Z}_p$ решите уравнение $x^p = a$.

28.29. Пусть K — поле характеристики p. Тогда:

а) для всех элементов $a, b \in K$ и для каждого натурального m справедлива формула $(a+b)^{p^m} = a^{p^m} + b^{p^m}$;

б) множество $K^p = \{x^p \,|\, x \in K\}$ является подполем в K;

в) если K конечно, то отображение $a \to a^p$ является автоморфизмом поля K.

28.30. 1) Конечное поле характеристики p содержит p^m элементов для некоторого натурального m.

2) Аддитивная группа поля F_q из $q = p^m$ элементов является прямой суммой m циклических групп порядка p, а его мультипликативная группа — циклической порядка $q - 1$.

3) Для всякого натурального делителя $d \,|\, m$ поле F_{p^m} содержит в точности одно подполе, изоморфное полю F_{p^d}, и этим исчерпываются все подполя поля F_{p^m}.

4) Если K — поле характеристики p, то совокупность корней многочлена $x^q - x$, $q = p^m$, принадлежащих полю K, образует подполе поля K.

28.31. Пусть a — элемент конечного поля F_q, $m = o(a)$ — его порядок. Тогда:

а) $m \,|\, q - 1$;

б) если n — натуральный делитель числа $q - 1$, то число элементов поля F_q порядка n равно $\varphi(n)$.

28.32. Поля $\mathbb{Q}$ и $\mathbb{R}$ не имеют автоморфизмов, отличных от тождественного.

28.33. Найдите все автоморфизмы поля $\mathbb{C}$, при которых каждое вещественное число переходит в себя.

28.34. Имеет ли поле $\mathbb{Q}(\sqrt{2})$ автоморфизмы, отличные от тождественного?

28.35. При каких $n, m \in \mathbb{Z} \backslash \{0\}$ поля $\mathbb{Q}(\sqrt{m})$ и $\mathbb{Q}(\sqrt{n})$ изоморфны?

28.36. Решите в поле $\mathbb{Q}(\sqrt{2})$ уравнения:

а) $x^2 + \left(4 + 2\sqrt{2}\right) x + 3 + 2\sqrt{2} = 0$; б) $x^2 - 2x - 5 = 0$; в) $x^2 - 3x + \sqrt{2} = 0$;

г) $x^2 + 2x - 2 - 2\sqrt{2} = 0$; д) $x^2 + \left(-1 + \sqrt{2}\right) x - 6 + 2\sqrt{2} = 0$;

е) $x^2 - 2\left(3 - \sqrt{2}\right) x - 6 + 6\sqrt{2} = 0$.

28.37. Решите систему уравнений:

$$\text{а)} \begin{cases} x + 2z = 1 \\ y + 2z = 2 \\ 2x + z = 1; \end{cases} \qquad \text{б)} \begin{cases} 3x + y + 2z = 1 \\ x + 2y + 3z = 1 \\ 4x + 3y + 2z = 1 \end{cases}$$

в поле вычетов по модулю 3, по модулю 5 и по модулю 7.

28.38. Найдите такой многочлен $f(x)$ степени не выше 3 с коэффициентами из $\mathbb{Z}_5$, что

$$f(0) = 3, \quad f(1) = 3, \quad f(2) = 0, \quad f(4) = 4.$$

28.39. Найдите все многочлены $f(x)$ с коэффициентами из $\mathbb{Z}_5$ такие, что

$$f(0) = f(1) = f(4) = 1, \quad f(2) = f(3) = 3.$$

28.40. Какие из уравнений:

$$\text{а) } x^2 = 3, \ \text{б) } x^5 = 6, \ \text{в) } x^8 = 7, \ \text{г) } x^3 = a$$

имеют решения в поле $\mathbb{Z}_{11}$?

28.41. В поле $\mathbb{Z}_{11}$ решите уравнения:

а) $x^2+3x+8=0$; б) $x^2+5x+4=0$; в) $x^2+2x+3=0$;

г) $x^2+7x+4=0$; д) $x^2+9x+15=0$; е) $2x^2-8x+7=0$.

28.42. В поле $\mathbb{Z}_{37}$ решите уравнения:

а) $x=17+19$; б) $x=17\cdot 19$;

в) $x=17:19$; г) $x^2-2=0$ и $x^2-3=0$.

28.43. Найдите все порождающие элементы в мультипликативной группе поля:

а) $\mathbb{Z}_7$; б) $\mathbb{Z}_{11}$; в) $\mathbb{Z}_{17}$.

28.44. Пусть a, b — элементы поля F порядка $|F|=2^n$, где n нечетно. Тогда если $a^2+ab+b^2=0$, то $a=b=0$.

28.45. В поле $\mathbb{Z}_p$ выполняются равенства:

а) $\sum\limits_{k=1}^{p-1} k^{-1}=0$ $(p>2)$; б) $\sum\limits_{k=1}^{(p-1)/2} k^{-2}=0$ $(p>3)$.

28.46. 1) Докажите, что в поле 7-адических чисел содержатся квадратные корни из 2. Положив
$$\sqrt{2}=3+a_1\cdot 7+a_2\cdot 7^2+a_3\cdot 7^3+\dots \text{ или } \sqrt{2}=4+b_1\cdot 7+b_2\cdot 7^2+b_3\cdot 7^3+\dots,$$
докажите по индукции, что $a_1,a_2,\dots$ $(b_1,b_2,\dots)$ последовательно однозначно определяются. Вычислите первые 10 цифр.

2) Покажите, что, напротив, многочлены x^2-3 и x^2-5 корней в поле 7-адических чисел не имеют.

28.47. Найдите наибольший общий делитель многочленов:

а) $f(x)=x^3+x^2+2x+2$, $g(x)=x^2+x+1$;

б) $f(x)=x^4+1$, $g(x)=x^3+x+1$

над полем $\mathbb{Z}_3$ и $\mathbb{Z}_5$.

28.48. Докажите, что если многочлены $f(x)$ и $g(x)$ с целыми коэффициентами взаимно просты над полем $\mathbb{Z}_p$, причем хотя бы один из старших коэффициентов не делится на p, то эти многочлены взаимно просты над полем $\mathbb{Q}$. Покажите, что для любого простого p обратное утверждение не верно.

28.49. Многочлены $f(x)$ и $g(x)$ с целыми коэффициентами тогда и только тогда взаимно просты над полем $\mathbb{Q}$, когда они взаимно просты над полем $\mathbb{Z}_p$ для почти всех простых p.

28.50. Следующие многочлены разложите на неприводимые множители:

а) $x^5+x^3+x^2+1$ над полем $\mathbb{Z}_2$;

б) x^3+2x^2+4x+1 над полем $\mathbb{Z}_5$;

в) $x^4+3x^3+2x^2+x+4$ над полем $\mathbb{Z}_5$.

28.51. Разложите на неприводимые множители над полем $\mathbb{Z}_2$ все многочлены второй (третьей) степени.

28.52. Найдите все многочлены второй (третьей) степени со старшим коэффициентом 1, неприводимые над полем $\mathbb{Z}_3$.

28.53. Докажите, что если многочлен с целыми коэффициентами приводим над полем $\mathbb{Q}$, то он приводим над полем $\mathbb{Z}_p$ по любому простому p, не делящему старший коэффициент. Приведите пример многочлена, приводимого над полем $\mathbb{Q}$, но не приводимого над полем $\mathbb{Z}_p$, где p делит старший коэффициент.

28.54. Существуют многочлены с целыми коэффициентами, неприводимые над полем $\mathbb{Q}$, но приводимые над полем $\mathbb{Z}_p$ для любого простого p.

Таким будет, например, многочлен $f(x)=x^4-10x^2+1$. Он является многочленом наименьшей степени с целыми коэффициентами, имеющим корень $\sqrt{2}+\sqrt{3}$.

28.55. Пусть P — конечное расширение поля K, $f_\alpha(x)=x^m+a_1x^{m-1}+\dots+a_m$ — минимальный многочлен элемента $\alpha\in P$. Тогда норма элемента α равна $N(\alpha)=(-1)^m a_m$, а след $S(\alpha)=-a_1$ (определение нормы и следа см. в § 12).

28.56. Пусть $K\subset P$ — алгебраическое расширение. Тогда расширение $K(x)\subset P(x)$ также алгебраическое и $[P(x):K(x)]=[P:K]$.

Пусть $K\subset P$ — расширение полей. Элементы $a_1,\dots,a_s\in P$ называются *алгебраически независимыми над* K, если $f(a_1,\dots,a_s)\neq 0$ для всякого ненулевого многочлена $f(x_1,\dots,x_s)\in K[x_1,\dots,x_s]$.

28.57. Элементы $a_1,\dots,a_s\in P$ алгебраически независимы над K тогда и только тогда, когда расширение $K(a_1,\dots,a_s)$ K-изоморфно полю рациональных функций $K(x_1,\dots,x_s)$.

28.58. Пусть $K\subset P$ — расширение полей и $a_1,\dots,a_m;\ b_1,\dots,b_n\in P$ — две максимальные алгебраически независимые над K системы элементов. Тогда $m=n$ (*степень трансцендентности* P над K).

28.59. 1) В конечномерной коммутативной K-алгебре A с 1 имеется лишь конечное число максимальных идеалов, и их пересечение совпадает с множеством $N(A)$ всех нильпотентных элементов алгебры A (*нильрадикал* алгебры A).

2) $A^{red} = A/N(A)$ — *редуцированная* алгебра (не содержит ненулевых нильпотентных элементов).

3) Алгебра $A/N(A)$ изоморфна прямому произведению полей $K_1, \ldots, K_s$, являющихся расширениями поля K.

4) $s \leqslant [A : K]$.

5) Набор расширений K_i определен для алгебры A однозначно с точностью до изоморфизма (расширения $K_1, \ldots, K_s$ вместе с каноническими гомоморфизмами $A \to K_i$ называются *компонентами алгебры* A).

28.60. Пусть A — конечномерная K-алгебра с 1, L — расширение поля K и $A_L = L \otimes_K A$. Тогда:

а) если $e_1, \ldots, e_n$ — базис A над K, то $1 \otimes e_1, \ldots, 1 \otimes e_n$ — базис A_L над L;

б) при естественном вложении A в A_L образ A является K-подалгеброй в A_L.

28.61. Пусть A — K-алгебра с 1 и L — расширение поля K, $L \subseteq A$ и A — L-алгебра. Тогда:

а) если $f_1, \ldots, f_n$ — различные K-гомоморфизмы $A \to L$, то $f_1, \ldots, f_n$ линейно независимы как элементы векторного пространства над L всех K-линейных отображений $A \to L$;

б) число различных K-гомоморфизмов $A \to L$ не превосходит $[A : L]$.

Найдите все автоморфизмы полей $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\mathbb{Q}(\sqrt[3]{2})$.

28.62. Пусть A — конечномерная K-алгебра с 1, L — расширение поля K. Тогда:

а) если B — подалгебра в A, то B_L — подалгебра в A_L;

б) если I — идеал алгебры A и I_L — соответствующий идеал в A_L, то $(A/I)_L \cong A_L/I_L$;

в) если $A = \prod_{i=1}^{s} A_i$, то $A_L = \prod_{i=1}^{s} (A_i)_L$;

г) если $K_1, \ldots, K_s$ — множество компонент алгебры A, то множество компонент алгебры A_L совпадает с объединением множеств компонент алгебр $(K_1)_L, \ldots, (K_s)_L$;

д) если F — расширение поля L, то $(A_L)_F \cong A_F$.

28.63. Пусть A — конечномерная K-алгебра с 1, L — расширение поля K, B — некоторая L-алгебра. Тогда:

а) каждый K-гомоморфизм $A \to B$ однозначно продолжается до L-гомоморфизма $A_L \to B_L$;

б) множество K-гомоморфизмов $A \to L$ находится в биективном соответствии с множеством компонент алгебры A_L, изоморфных L;

в) число различных K-гомоморфизмов $A \to L$ не превосходит $[A : K]$.

29 Поля разложения

Если K — поле, $\{f_i(x) \mid i \in I\}$ — некоторое семейство многочленов из $K[x]$, $\deg f_i(x) \geqslant 1$, то под *полем разложения* этого семейства понимают расширение P поля K, в котором всякий $f_i(x)$ разложим на линейные множители, причем P порождается всеми корнями многочленов $f_i(x)$. Поля разложения всегда существуют и изоморфны между собой. Кроме того, если все корни α_i $(i = 1, \ldots, n)$ многочлена $f(x) \in K[x]$ различны и F, $\tilde{F}$ — два его поля разложения, то существует в точности $[F : K]$ различных изоморфизмов полей F и $\tilde{F}$ над K. В частности, группа автоморфизмов $\operatorname{Aut} F/K$ поля F над K (см. 28.14) имеет порядок $\leqslant [F : K]$. Если все корни многочлена $f(x)$ различны, то $|\operatorname{Aut} F/K| = [F : K]$.

Теорема 29.1. *Пусть P — алгебраическое расширение поля K, содержащееся в его алгебраическом замыкании $\overline{K}$. Тогда следующие условия эквивалентны:*

1) *всякое вложение поля P в $\overline{K}$ над K является автоморфизмом поля P;*

2) *P — поле разложения некоторого семейства многочленов из $K[x]$;*

3) *всякий неприводимый в $K[x]$ многочлен, имеющий корень в P, разложим в $P[x]$ на линейные множители.*

Расширение P поля K, удовлетворяющее условиям теоремы 29.1, называется *нормальным*.

Если θ — корень неразложимого в кольце $K[x]$ многочлена, обладающего лишь простыми корнями, то θ называется *сепарабельным элементом* над полем K. Многочлен называется *сепарабельным*, если его неприводимые множители имеют различные корни. Алгебраическое расширение P поля K, все элементы которого сепарабельны над K, называется *сепарабельным*; это эквивалентно тому, что расширение $K(a)$ сепарабельно для каждого $a \in P$. Иногда в литературе под сепарабельными понимают только конечные сепарабельные расширения.

В случае характеристики нуль каждый неразложимый многочлен (а потому и каждое алгебраическое расширение) является сепарабельным. В случае поля K характеристики p для каждого неразложимого многочлена $f(x)$ над

полем K существует целое число $\mu \geqslant 0$ такое, что всякий корень α многочлена $f(x)$ имеет кратность p^μ, а элемент α^{p^μ} сепарабелен над K.

Поле K называется *совершенным*, если любой неразложимый над K многочлен сепарабелен.

Поле K характеристики p является совершенным тогда и только тогда, когда оно вместе с каждым своим элементом содержит и корень p-й степени из него, т.е. $K^p = K$.

Все алгебраически замкнутые поля совершенны. Каждое алгебраическое расширение совершенного поля сепарабельно над этим полем.

Справедлива теорема

Теорема 29.2. *Пусть $K(\alpha_1, \ldots, \alpha_n)$ — конечное алгебраическое расширение поля K и $\alpha_1, \ldots, \alpha_n$ — сепарабельные элементы. Тогда $K(\alpha_1, \ldots, \alpha_n)$ является простым расширением $K(\alpha_1, \ldots, \alpha_n) = K(\theta)$.*

Элемент θ из этой теоремы называется *примитивным* элементом. В этом случае, если $[K(\theta):K] = m$, то элементы $1, \theta, \ldots, \theta^{m-1}$ образуют базис пространства $K(\theta)$.

Пусть $P \subset F$ — некоторое расширение поля P, $H \subseteq \operatorname{Aut} F/P$. Через F^H обозначают подмножество $F^H = \{a \in F \mid \varphi(a) = a, \varphi \in H\}$. Справедлива теорема

Теорема 29.3. *Следующие условия на расширение $P \subset F$ эквивалентны:*

1) *F — поле разложения некоторого сепарабельного многочлена над P;*

2) *$P = F^G$ для некоторой конечной группы $G \subseteq \operatorname{Aut} F/P$;*

3) *F — конечномерное нормальное и сепарабельное расширение поля P.*

Все алгебры в данном параграфе предполагаются с 1.

Задачи

29.1. Пусть $P \subset F$ — алгебраическое расширение поля P. Элемент $\alpha \in F$ является сепарабельным над P в точности тогда, когда его минимальный многочлен $f_\alpha(x)$ и его производная взаимно просты в $P[x]$.

29.2. Для любого несовершенного поля существуют несепарабельные расширения.

29.3. 1) Каждое квадратичное поле над P нормально над P.

2) Каждое расширение степени 2 нормально.

29.4. Каждое конечное нормальное расширение является полем разложения некоторого многочлена.

29.5. Пусть $K \subseteq P \subseteq F$ — башня конечных расширений поля K. Докажите, что:

а) если расширение $K \subset F$ нормально, то расширение $P \subset F$ также нормально;

б) если расширения $K \subset P$ и $P \subset F$ нормальны, то расширение $K \subset F$ не обязательно нормально;

в) если расширения $K \subset F$ и $P \subset F$ нормальны, то расширение $K \subset P$ не обязательно нормально.

29.6. Если P — нормальное, а F — произвольное расширения поля K и P, F содержатся в некотором большем поле L, то PF нормально над F. Если к тому же и F нормально над K, то поля PF и $P \cap F$ также нормальны над K.

29.7. Если $P \subset F$ — нормальное расширение, то F содержит поле разложения минимального многочлена каждого элемента $a \in F$.

29.8. Постройте поле разложения многочлена $x^3 - 2$ над $\mathbb{Q}$ и покажите, что если α — один из корней этого многочлена, то $\mathbb{Q}(\alpha)$ не является нормальным.

29.9. Покажите, что $\mathbb{Q}(\sqrt[3]{5})$ (под $\sqrt[3]{5}$ понимается вещественный корень) не может быть полем разложения многочлена $x^3 - 5$. Найдите поле разложения этого многочлена, покажите, что оно является простым расширением поля $\mathbb{Q}$.

29.10. Найдите поля разложения многочлена $x^2 + 1$ над $\mathbb{Q}$ и $\mathbb{R}$.

29.11. Пусть G — конечная группа автоморфизмов поля K и $P = K^G$. Покажите, что $[K : P] \leqslant |G|$.

29.12. Если F — расширение поля P, то имеются два отображения:

1) $H \mapsto K = F^H$ — из множества подгрупп $H \subseteq \operatorname{Aut} F/P$ во множество подполей $P \subseteq K \subseteq F$;

2) $K \mapsto H = \operatorname{Aut} F/K$ — из множества промежуточных подполей $P \subseteq K \subseteq F$ во множество подгрупп $H \subseteq \operatorname{Aut} F/P$.

Докажите свойства этих отображений:

а) если $G_2 \subseteq G_1 \subseteq G = \operatorname{Aut} F/P$, то $F^{G_1} \subseteq F^{G_2}$;

б) если $P \subseteq P_2 \subseteq P_1 \subseteq F$, то $\operatorname{Aut} F/P_1 \subseteq \operatorname{Aut} F/P_2$;

в) $P \subseteq F^{\operatorname{Aut} F/P}$;

г) $H \subseteq \operatorname{Aut} F/F^H$ для любой подгруппы $H \subseteq G$.

29.13. Поле $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ является полем разложения многочлена $x^4 - 10x^2 + 1$, а $\sqrt{2} + \sqrt{3}$ — примитивный элемент этого поля (ср. с 28.15).

29.14. Какие из следующих расширений являются нормальными:

а) $\mathbb{Q}(\sqrt[3]{3})$; б) $\mathbb{Q}(\sqrt{-3})$; в) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

29.15. Если p — простое число и $\varepsilon = \sqrt[p]{1} \neq 1$, то $\mathbb{Q}(\varepsilon)$ является полем разложения многочлена $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$.

29.16. Покажите, что если присоединить к F_2 корень θ неприводимого многочлена $x^2 + x + 1$, то получится поле $F_2(\theta) = \{0, 1, \theta, 1 + \theta\}$ из четырех элементов, изоморфное полю $F_2[x]/(x^2 + x + 1)$.

Используя соотношение $x^2 + x + 1 = (x - \theta)(x - \theta^2)$, покажите, что $F_2(\theta)$ — поле разложения многочлена $x^2 + x + 1$.

29.17. Найдите степень поля разложения над $\mathbb{Q}$ для многочленов:

а) $ax + b$ $(a, b \in \mathbb{Q},\ a \neq 0)$;

б) $x^2 - 2$; в) $x^3 - 1$; г) $x^3 - 2$; д) $x^4 - 2$;

е) $x^p - 1$ (p — простое число); ж) $x^n - 1$ $(n \in \mathbb{N})$;

з) $x^p - a$ ($a \in \mathbb{Q}$ и не является p-й степенью в $\mathbb{Q}$, p — простое число).

29.18. Конечное расширение $K \subset P$ является простым тогда и только тогда, когда множество промежуточных полей между K и P конечно.

29.19. Пусть K — поле характеристики p. Покажите, что:

а) $K(x, y)$ имеет степень p^2 над $K(x^p, y^p)$;

б) между $K(x, y)$ и $K(x^p, y^p)$ существует бесконечно много расширений. Это дает пример конечного расширения, не являющегося простым.

29.20. В случае нулевой характеристики неприводимый многочлен $f(x) \in P[x]$ имеет только простые корни. В случае характеристики p многочлен степени > 1 имеет кратные корни тогда и только тогда, когда его можно представить как многочлен от x^p, причем существует целое число $\mu \geqslant 0$ такое, что всякий корень многочлена $f(x)$ имеет кратность p^μ, а если α — корень $f(x)$, то элемент α^{p^μ} сепарабелен над K.

29.21. Пусть $K \subset F$ — алгебраическое расширение поля K. Элемент $\alpha \in F$ не является сепарабельным тогда и только тогда, когда K имеет простую характеристику p и минимальный многочлен $f_\alpha(x) = g(x^p)$ для некоторого многочлена $g(x) \in K[x]$.

29.22. Пусть $K \subset F$ — алгебраическое расширение поля K, порожденное семейством $\{a_i | a_i \in F\}$. Если каждый элемент a_i сепарабелен над K, то F сепарабельно над K.

29.23. Пусть $K = K_0 \subset K_1 \subset \ldots \subset K_s = L$ — башня конечных расширений полей. Расширение $K \subset L$ сепарабельно тогда и только тогда, когда каждое расширение $K_{i-1} \subset K_i$ $(i = 1, \ldots, s)$ сепарабельно.

29.24. Пусть $K \subset L \subset F$ — башня конечных расширений полей. Тогда:

а) если элемент $a \in F$ сепарабелен над K, то a сепарабелен над L;

б) утверждение, обратное к а), верно, если расширение $K \subset L$ сепарабельно.

29.25. Пусть K — поле и $F = K(a)$ — алгебраическое расширение поля K. Тогда следующие условия эквивалентны:

а) F — сепарабельное расширение поля K;

б) элемент a сепарабелен над K;

в) для любого расширения L поля K алгебра $F \otimes_K L$ не имеет ненулевых нильпотентных элементов;

г) для любого поля $L \supseteq K$ алгебра $F \otimes_K L$ является (кольцевым) прямым произведением конечного числа экземпляров поля L.

Пусть L — алгебраическое расширение поля K характеристики p; оно называется *чисто несепарабельным* расширением, если в $L \backslash K$ нет сепарабельных элементов над K.

29.26. Для алгебраического расширения L поля K характеристики p следующие условия эквивалентны:

а) L — чисто несепарабельное расширение поля K;

б) минимальный многочлен для всякого $\alpha \in L$ над K имеет вид $x^{p^n} - a$ для некоторого $n \geqslant 0$ и $a \in K$;

в) для всякого элемента $\alpha \in L \backslash K$ существует целое число $n \geqslant 0$ такое, что $\alpha^{p^n} \in K$;

г) существует такое множество образующих $\{\alpha_i | i \in I\}$ поля L над K, что $\alpha_i^{p^{n_i}} \in K$ для некоторого целого $n_i \geqslant 0$.

29.27. Пусть $K = K_0 \subset K_1 \subset \ldots \subset K_s = L$ — башня конечных расширений полей. Расширение $K \subset L$ чисто несепарабельно тогда и только тогда, когда каждое расширение $K_{i-1} \subset K_i$ $(i = 1, \ldots, s)$ чисто несепарабельно.

29.28. Пусть E — алгебраическое расширение поля K, и пусть E_0 — композит всех подполей F поля E таких, что

$K \subset F$ и F сепарабельно над K. Тогда E_0 сепарабельно над K, E чисто несепарабельно над E_0.

29.29. Пусть расширение E нормально над K, и пусть E_0 — его максимальное сепарабельное подрасширение. Тогда E_0 также нормально над K.

29.30. Пусть E, F — конечные расширения поля K, причем $K \subset E$ — сепарабельно, $K \subset F$ — чисто несепарабельно. Предположим, что E, F — подполя некоторого общего поля. Тогда $[EF : F] = [E : K]$, $[EF : E] = [F : K]$ и $F \subset EF$ — сепарабельное, $E \subset EF$ — чисто несепарабельное расширения. Иллюстрацией служит следующая диаграмма

$$\begin{array}{ccc} EF & \overset{1}{\longleftrightarrow} & EF \\ \uparrow \text{ч.нес.} & & \uparrow \text{сеп.} \\ E & & F \\ \uparrow \text{сеп.} & & \uparrow \text{ч.нес.} \\ K & \overset{1}{\longleftrightarrow} & K. \end{array}$$

29.31. Пусть E — поле характеристики p, являющееся конечным расширением поля K. Тогда если $E^p K = E$, то E сепарабельно над K. Если E сепарабельно над K, то $E^{p^n} K = E$ для всех $n \geqslant 1$.

29.32. Пусть F — нормальное расширение поля K, $G = \operatorname{Aut} F/K$ и F^G — неподвижное поле группы G. Тогда F^G чисто несепарабельно над K и F сепарабельно над F^G. Если F_0 — максимальное сепарабельное подрасширение F, то $F = F^G F_0$ и $F_0 \cap F^G = K$. Таким образом, нормальное расширение распадается в композит чисто несепарабельного и сепарабельного расширений. Иллюстрацией служит следующая диаграмма

$$\begin{array}{ccc} F_0 F^G = F & \overset{1}{\longleftrightarrow} & F_0 F^G = F \\ \uparrow \text{ч.нес.} & & \uparrow \text{сеп.} \\ F_0 & & F^G \\ \uparrow \text{сеп.} & & \uparrow \text{ч.нес.} \\ F_0 \cap F^G = K & \overset{1}{\longleftrightarrow} & F_0 \cap F^G = K. \end{array}$$

29.33. Каждое конечное поле совершенно.

29.34. Каждое алгебраическое расширение совершенного поля совершенно.

Пусть A — конечномерная K-алгебра. Говорят, что A сепарабельна над K, если справедливы следующие условия:

а) $L \otimes_K A$ — полупростая алгебра для всех расширений L поля K;

б) L-алгебра $L \otimes_K A$ для некоторого алгебраически замкнутого поля $L \supseteq K$ является прямым произведением полных матричных алгебр над L;

в) алгебра A полупроста, а ее центр $Z(A)$ есть прямое произведение конечного числа сепарабельных расширений поля K.

29.35. Поле A является конечным сепарабельным расширением поля K в точности тогда, когда алгебра A сепарабельна над K.

29.36. Следующие свойства конечного расширения $K \subset L$ равносильны:

а) все компоненты алгебры $L_L = L \otimes_K L$ изоморфны L;

б) L имеет $[L : K]$ K-автоморфизмов;

в) для любых K-вложений $\varphi_i : L \to L'$ $(i = 1, 2)$ поля L в любое расширение $K \subset L'$ имеем $\varphi_1(L) = \varphi_2(L)$;

г) всякий неприводимый многочлен из $K[x]$, имеющий корень в L, разложим над L в произведение линейных множителей;

д) L — поле разложения некоторого многочлена из $K[x]$ (т.е. L — конечное нормальное расширение поля K).

29.37. Пусть A — конечномерная коммутативная K-алгебра. Элемент $a \in A$ сепарабелен тогда и только тогда, когда сепарабелен его минимальный многочлен.

29.38. Если A — сепарабельная коммутативная K-алгебра и $f(x) \in K[x]$ — сепарабельный многочлен, то алгебра $B = A[x]/(f(x))$ сепарабельна.

29.39. Пусть A — коммутативная K-алгебра, $B = K[a_1, \ldots, a_n]$ — подалгебра в A, порожденная $a_1, \ldots, a_n \in A$. Следующие утверждения равносильны:

а) B — сепарабельная K-алгебра;

б) всякий элемент $b \in B$ сепарабелен;

в) элементы $a_1, \ldots, a_n$ сепарабельны.

30 Конечные поля

Для каждого простого числа p и натурального n существует (с точностью до изоморфизма только одно) конечное поле F_q из $q = p^n$ элементов. Это поле в честь Э. Галуа часто обозначается через $GF(q)$. Для конечных полей коммутативность умножения следует из других аксиом поля. А именно доказано (теорема Веддерберна), что всякое конечное тело является полем.

Теорема 30.1. *Пусть $q = p^n$. Справедливы следующие утверждения.*

1) *$F = F_q$ — поле разложения многочлена $x^q - x$ в алгебраическом замыкании $\overline{F}_p$, и его элементы — корни этого многочлена, т.е. $x^q - x = \prod\limits_{t \in F} (x - t)$.*

2) *Мультипликативная группа F^* поля F является циклической порядка $q - 1$.*

3) *Группа автоморфизмов* Aut F *поля F является циклической порядка n, причем* Aut $F = \langle \Phi \mid \Phi(t) = t^p,\ t \in F \rangle$.

4) *Если F_{p^d} — подполе поля F, то $d|n$. Обратно: каждому делителю d числа n отвечает ровно одно подполе $\{t \in F \mid \Phi^d(t) = t\} = F_{p^d}$. Автоморфизмы, оставляющие это подполе поэлементно неподвижным, образуют группу* Aut $\left(F/F_{p^d}\right) = \langle \Phi^d \rangle$. *Таким образом, имеется биективное соответствие между подполями конечного поля F и подгруппами его группы автоморфизмов.*

5) *Если $F^* = \langle \theta \rangle$, то θ — примитивный элемент поля с минимальным многочленом $h(x)$ степени n и F — поле разложения над F_p многочлена $h(x)$.*

6) *Для любого натурального числа m существует хотя бы один неприводимый многочлен степени m над F_p.*

Пусть $F = F_q$ — конечное поле, где q — нечетное число. Элемент $a \in F^*$ называется *квадратичным вычетом* в F, если уравнение $x^2 - a = 0$ имеет корень в F (в противном случае элемент a называется *квадратичным невычетом*). Полагают $(a/F) = 1$, если a — квадратичный вычет в F, и -1 в противном случае. Если $q = p$, где p — нечетное простое число, то (a/F) обозначается через (a/p) и называется *символом Лежандра*.

Теорема 30.2 (квадратичный закон взаимности). *Пусть p и q — нечетные простые числа. Тогда* $(p/q)\,(q/p) = (-1)^{((p-1)/2)\,\cdot\,((q-1)/2)}$.

Теорема 30.3. *Неприводимый над полем F_p многочлен степени n тогда и только тогда делит многочлен $x^{p^m} - x$, когда n делит m.*

Теорема 30.4. *Число $\psi_m(q)$ неприводимых унитарных степени m многочленов над полем F_q, $q = p^n$, равно* $\psi_m(q) = \dfrac{1}{m} \sum\limits_{d|m} q^d \mu\left(\dfrac{m}{d}\right)$.

Например, $\psi_2(2) = \dfrac{1}{2}(2^2 - 2) = 1$, $\psi_3(2) = \dfrac{1}{3}(2^3 - 2) = 2$.

Пусть $f(x)$ — унитарный многочлен над полем F_p, $f(0) \neq 0$. Наименьшее натуральное число δ такое, что $f(x) \mid x^\delta - 1$, называется *порядком* многочлена $f(x)$ и обозначается через $o(f)$.

Теорема 30.5. *Если $f(x)$ — унитарный многочлен степени n над полем F_p, $f(0) \neq 0$, то $1 \leqslant o(f) \leqslant p^n - 1$.*

Теорема 30.6. *Пусть $f(x)$ — неприводимый унитарный многочлен над полем F_p, $f(0) \neq 0$. Тогда:*

1) *если $\theta \in F_{p^n}$ — его корень ($F_p \subseteq F_{p^n}$), то $o(f)$ совпадает с порядком элемента θ в $F^*_{p^n}$;*

2) *если $n = deg\, f(x)$, то $o(f) \mid p^n - 1$.*

Неприводимый над полем F_p многочлен называют *примитивным* над полем F_p, если $o(f) = p^{deg\, f} - 1$.

Теорема 30.7. *Число $b_p(n)$ примитивных над полем F_p многочленов степени n равно $b_p(n) = \dfrac{\varphi(p^n - 1)}{n}$, где $\varphi(m)$ — функция Эйлера.*

Задачи

30.1. Для каких чисел $n = 2, \ldots, 10$ существует поле из n элементов?

30.2. Пусть $q = p^n$. Покажите, что:

а) в $F_q[x]$ существует лишь конечное число многочленов заданной степени;

б) для каждого натурального числа m в $F_q[x]$ существует неприводимый многочлен степени m.

30.3. 1) $x^q - x = \prod\limits_{\alpha \in F_q} (x - \alpha)$.

2) Если $F_q \subseteq K$, где K — некоторое поле, то $\alpha \in K$ принадлежит F_q тогда и только тогда, когда $\alpha^q = \alpha$.

3) Если многочлен $f(x) \in F_q[x]$ делит $x^q - x$, то он имеет $d = \deg f(x)$ различных корней.

30.4. Если $q = p^n$, то произведение всех ненулевых элементов поля F_q равно -1. В частности, при $n = 1$ справедлива

теорема Вильсона $(p-1)!\ \equiv -1 \pmod p$.

30.5. Всякий многочлен вида $(x^q - x)\, f(x)$, $f(x) \in F_q[x]$, принимает для всех $a \in F_q$ значение 0. Обратно, любой многочлен $g(x)$ такой, что $g(a) = 0$ для всех $a \in F_q$, имеет вид $(x^q - x)\, f(x)$ для подходящего $f(x) \in F_q[x]$.

30.6. Для $\alpha \in F_q$, $q = p^n$, пусть

$$f\,(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\ldots(x-\alpha^{p^{n-1}}).$$

Покажите, что $f(x) \in F_p[x]$. В частности, $\alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$ и $\alpha\alpha^p \ldots \alpha^{p^{n-1}} \in F_p$. Обозначим $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$. Проверьте, что:

а) $\mathrm{tr}(\alpha) + \mathrm{tr}(\beta) = \mathrm{tr}\,(\alpha+\beta)$;

б) $\mathrm{tr}(u\alpha) = u\,\mathrm{tr}(\alpha)$ для всех $u \in F_p$;

в) существует такой $\alpha \in F_q$, что $\mathrm{tr}(\alpha) \neq 0$.

Пусть $x^p - x - \alpha \in F_q[x]$, где $\alpha \in F_q$. Покажите, что этот многочлен либо неприводим, либо является произведением линейных множителей; причем последнее имеет место тогда и только тогда, когда $\mathrm{tr}(\alpha) = 0$.

30.7. Всякое конечное расширение конечного поля является:

а) простым; б) нормальным.

30.8. Выпишите все унитарные многочлены первой, второй и третьей степени над полем F_2. Выделите среди них неприводимые.

30.9. Проверьте, что многочлены x^4+x^3+1, x^4+x+1 и $x^4+x^3+x^2+x+1$ неприводимы над полем F_2. И разложите $x^{16} - x$ в произведение неприводимых множителей в $F_2[x]$.

30.10. Разложите на неприводимые множители:

а) $x^4 + x^3 + x + 2$ в $F_3[x]$;

б) $x^3 + x^2 + 4x + 2$ в $F_5[x]$;

в) $x^5 + 5x^4 + 5x^3 + 2x^2 + 4x + 3$ в $F_7[x]$.

30.11. 1) $F_2[x]/\,(f(x)) \cong F_4$, где $f(x) = x^2 + x + 1$.

2) $F_3[x]/\,(f(x)) \cong F_9$, где $f(x) = x^2 + x + 2$.

30.12. Проверьте, что $\psi_3(p) = \dfrac{1}{3}\left(p^3 - p\right)$. Найдите $\psi_4\,(2)$, $\psi_5\,(2)$, $\psi_6\,(2)$.

30.13. Поле F_{4096} имеет четыре собственных непростых подполя: $F_2 \subset F_8 \subset F_{64} \subset F_{4096}$ и $F_2 \subset F_4 \subset F_{16} \subset F_{4096}$.

30.14. Определите порядки многочленов:

а) $x^2 + x + 1$, $x^3 + x + 1$ и $x^4 + x^3 + x^2 + x + 1$ над полем F_2;

б) $x + 1$, $x + 4$, $x + 5$ над полем F_7.

30.15. Порядок многочлена над полем F_p равен порядку этого многочлена над любым расширением поля F_p.

30.16. Если $m \in \mathbb{N}$ и f — многочлен над полем F_p, то $f \mid x^m - 1$, если и только если $o\,(f) \mid m$.

30.17. Если f и g — взаимно простые многочлены над полем F_p, то $o\,(f \cdot g) = [o\,(f)\,, o(g)]$.

30.18. Пусть $n \in \mathbb{N}$, f — многочлен над полем F_p, $g = f^n$, t — наименьшее неотрицательное целое с условием $p^t \geqslant n$. Тогда:

а) $o(g) = o\,(f^n) = p^t o\,(f)$;

б) если к тому же $t > 0$, то $o(g) < p^{\deg g} - 1$.

30.19. Докажите теорему 30.6.

30.20. Если f — многочлен над полем F_p и $o\,(f) = p^{deg\, f} - 1$, то f неприводим.

30.21. Пусть $F = F_q$ — конечное поле, где q — нечетное число, и $a \in F^*$. Тогда:

а) $a^{(q-1)/2} = \pm 1$;

б) a является квадратичным вычетом тогда и только тогда, когда $a^{(q-1)/2} = 1$;

в) $a^{(q-1)/2} = (a/F)$;

г) число квадратичных вычетов (так же, как и невычетов) равно $\dfrac{q-1}{2}$;

д) $\sum_{a \in F^*} (a/F) = 0$;

е) отображение $a \mapsto (a/F)$ является гомоморфизмом групп $F^* \to \{-1,\, 1\}$;

ж) $(a/F) = \mathrm{sgn}\,\sigma_a$, где $\sigma_a \colon x \mapsto ax$ — перестановка на множестве элементов поля F.

30.22. Пусть $F = F_q$ — конечное поле, где q — нечетное число, $-1 \in F$ является квадратичным вычетом тогда и только тогда, когда q имеет вид $4k+1$. Существует бесконечно много простых чисел вида $4k+1$.

30.23. Пусть a и b — взаимно простые числа и $\sigma\colon x \to ax$ — перестановка на множестве классов вычетов по модулю b. Докажите, что:

а) если b четно, то

$$\operatorname{sgn}\sigma = \begin{cases} 1 \text{ при } b \equiv 2 \pmod 4, \\ (-1)^{(a-1)/2} \text{ при } b \equiv 0 \pmod 4; \end{cases}$$

б) если b нечетно, $b = \prod_{i=1}^{s} p_i$ ($p_1, \ldots, p_s$ — простые числа), то $\operatorname{sgn}\sigma = \prod_{i=1}^{s} (a/p_i)$ (в этом случае $\operatorname{sgn}\sigma$ обозначается через (a/b) и называется *символом Якоби*);

в) $(a/b_1b_2) = (a/b_1)(a/b_2)$ и $(a_1a_2/b) = (a_1/b)(a_2/b)$.

Пусть p — нечетное простое число. Напомним, что множество $\{-(p-1)/2, \ldots, -1, 0, 1, 2, \ldots, (p-1)/2\}$ называется *множеством наименьших вычетов по модулю p.*

30.24. (Лемма Гаусса). Пусть $a \in \mathbb{Z}$, $p \nmid a$ и μ обозначает число тех наименьших вычетов чисел $a, \ldots, ((p-1)/2)\,a$, которые отрицательны. Тогда $(a/p) = (-1)^{\mu}$.

30.25. Пусть p — нечетное простое число. Докажите, что $(2/p) = (-1)^{(p^2-1)/8}$, т.е. 2 будет квадратичным вычетом по модулю простых чисел вида $8k+1$, $8k+7$ и квадратичным невычетом по модулю простых чисел вида $8k+3$, $8k+5$.

30.26. Если b — нечетное целое число, то:

а) $(-1/b) = (-1)^{(b-1)/2}$;

б) $(2/b) = (-1)^{(b^2-1)/8}$.

30.27. $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{((a-1)/2)\cdot((b-1)/2)}$ для любых взаимно простых нечетных чисел a и b.

30.28. Пусть F — конечное расширение поля F_q степени n. В F как векторном пространстве над F_q существует базис вида $x, x^q, \ldots, x^{q^{n-1}}$ для некоторого $x \in F$.

30.29. Элементы $x_1, \ldots, x_n \in F_{q^n}$ образуют базис над F_q тогда и только тогда, когда

$$det \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_1^q & x_2^q & \ldots & x_n^q \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \ldots & x_n^{q^{n-1}} \end{pmatrix} \neq 0.$$

30.30. Пусть $a \in F_{q^n}$. Элементы $a, a^q, \ldots, a^{q^{n-1}}$ образуют базис F_{q^n} как векторного пространства над F_q тогда и только тогда, когда в $F_{q^n}[x]$ многочлены $x^n - 1$ и

$$ax^{n-1} + a^q x^{n-2} + \ldots + a^{q^{n-2}} x + a^{q^{n-1}}$$

взаимно просты.

30.31. Если F_q — конечное поле нечетной характеристики, то уравнение $x + y = z$ в F_q^* имеет $(q-1)(q-2)$ решений.

30.32. Пусть $F = F_q$ — конечное поле, $\alpha \in F^*$, $\delta = (n, q-1)$. Уравнение $x^n = \alpha$ разрешимо в F тогда и только тогда, когда $\alpha^{(q-1)/\delta} = 1$. Если решения имеются, то их будет ровно δ.

30.33. Пусть $(n, q-1) = 1$. Покажите, что все элементы из F_q являются n-й степенью. Если n — делитель числа $q-1$, то n-ми степенями в F_q являются те и только те элементы α, для которых $\alpha^{(q-1)/n} = 1$.

30.34. Пусть $F = F_q$ — конечное поле, $a \in F^*$, $\delta = (n, q-1)$. Тогда:

а) в F_q уравнение $x^n = a$ или не имеет решений, или имеет δ решений;

б) множество тех $a \in F^*$, для которых уравнение $x^n = a$ разрешимо, является подгруппой, состоящей из $(q-1)/\delta$ элементов.

30.35. Пусть $F = F_q$ — конечное поле, причем $q \equiv 1 \pmod n$. Тогда если K — поле, содержащее F, и $[K : F] = n$, то для любого $a \in F^*$ уравнение $x^n = a$ имеет n решений в K.

30.36. Исходя из цепочки естественных включений

$$GF(p) \subset GF\left(p^{2!}\right) \subset GF\left(p^{3!}\right) \subset \ldots,$$

рассмотрите так называемое *предельное поле* $\Omega_p = GF\left(p^{\infty!}\right)$, полагая $a \in \Omega_p$ если $a \in GF\left(p^{n!}\right)$ при достаточно большом n. Опираясь на основные свойства конечных полей, докажите, что Ω_p — алгебраически замкнутое поле. Таким образом, получаются, с учетом поля комплексных чисел, примеры алгебраически замкнутых полей любой характеристики.

30.37. Если $q = p^n$, то при $p = 2$ все элементы поля F_q являются квадратами, а при $p > 2$ квадраты группы F_q^* образуют в ней подгруппу $F_q^{*\,2}$ индекса 2, причем $F_q^{*\,2} = \operatorname{Ker}(t \mapsto t^{(q-1)/2})$.

30.38. Поле F_{2^n} будем рассматривать как векторное пространство V размерности n над F_2. Наряду с операцией сложения, наследуемой из F_{2^n}, введем на V операцию умножения $(x, y) \mapsto x \circ y = \sqrt{xy}$. Здесь $x \mapsto \sqrt{x}$ — автоморфизм на F_{2^n}, обратный к $x \mapsto x^2$, так что $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Покажите, что $(V, +, \circ)$ — коммутативная (неассоциативная) алгебра над F_2, обладающая свойствами:

а) в V нет делителей нуля и нет единицы;

б) при $a \neq 0$ уравнение $a \circ x = b$ однозначно разрешимо;

в) группа автоморфизмов $\operatorname{Aut} V$ действует на $V \setminus \{0\}$ транзитивно.

31 Начала теории Галуа

Пусть K — поле, $G = \operatorname{Aut} K$ — группа автоморфизмов поля K. Обозначим через $K^G = \{a \in K \mid \varphi a = a,\ \varphi \in G\}$. Подмножество $K^G \subseteq K$ называется *неподвижным полем* (или *полем инвариантов*) группы G (K^G является подполем поля K).

Группа автоморфизмов поля F над P называется *группой Галуа* поля F над P и обозначается $\operatorname{Gal} F/P$ (она состоит из всех автоморфизмов поля F, оставляющих элементы из P неподвижными). Алгебраическое расширение F поля P называется *расширением Галуа*, если оно нормально и сепарабельно. Тогда $|\operatorname{Gal} F/P| = [F : P]$. Если F — поле разложения многочлена $f \in P[x]$, то $\operatorname{Gal} F/P$ называется также *группой Галуа многочлена* $f(x)$ над P и обозначается через $\operatorname{Gal}(f)$.

Расширение Галуа K/L называется *абелевым* (соответственно — *циклическим*), если его группа Галуа абелева (соответственно — циклическая).

Теорема 31.1. *Пусть F — расширение Галуа поля P конечной степени над P, $G = \operatorname{Gal} F/P$ — группа Галуа, $\Gamma = \{H \subseteq G\}$ — множество подгрупп в G и Σ — множество промежуточных полей между F и P. Тогда отображения*

$$H \mapsto F^H \text{ и } K \mapsto \operatorname{Gal} F/K$$

являются биекциями Γ на Σ и Σ на Γ. Кроме того, это соответствие Галуа обладает следующими свойствами:

1) $H_1 \supset H_2$ тогда и только тогда, когда $F^{H_1} \subset F^{H_2}$;

2) $|H| = [F : F^H]$, $(G : H) = [F^H : P]$;

3) $H \lhd G$ *тогда и только тогда, когда* F^H *нормально над* P. *В последнем случае* $\operatorname{Gal}(F^H/P) \cong G/H$.

Теорема 31.2. *Пусть K — расширение Галуа поля L, а F — произвольное расширение, причем K, F — подполя некоторого другого поля. Тогда композит KF является расширением Галуа над F, а K — расширение Галуа над $K \cap F$. Пусть $H = \operatorname{Gal} KF/F$ и $G = \operatorname{Gal} K/L$. Если $\sigma \in H$, то ограничение σ на K лежит в G и отображение $\sigma \mapsto \sigma|K$ дает изоморфизм H на группу Галуа поля K над $K \cap F$, т.е. $H \cong \operatorname{Gal}(K/(K \cap F))$.*

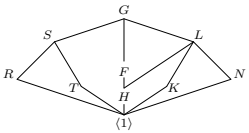
Теорема 31.3. *Пусть K_1 и K_2 — расширения Галуа над полем L с группами Галуа G_1 и G_2 соответственно. Предполагается, что K_1 и K_2 — подполя некоторого поля. Тогда K_1K_2 — расширение Галуа над L. Пусть G — его группа Галуа. Отобразим G в $G_1 \times G_2$ посредством ограничений, а именно $\sigma \mapsto (\sigma|K_1, \sigma|K_2)$. Это отображение инъективно. Если $K_1 \cap K_2 = L$, то это отображение есть изоморфизм.*

Пример 1. Рассмотрим многочлен $f(x) = x^4 - 2$ над полем $\mathbb{Q}$. Он неприводим по критерию Эйзенштейна. Пусть α — вещественный корень и $i = \sqrt{-1}$. Тогда $\pm\alpha$ и $\pm i\alpha$ — четыре корня многочлена $f(x)$ и $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Следовательно, полем разложения этого многочлена будет $K = \mathbb{Q}(\alpha, i)$. Нетрудно показать, что $[K : \mathbb{Q}] = 8$. Группа Галуа многочлена $f(x)$ имеет порядок 8.

Существует автоморфизм τ поля K, оставляющий $\mathbb{Q}(\alpha)$ неподвижным и переводящий i в $-i$, поскольку K — расширение Галуа над $\mathbb{Q}(\alpha)$ степени 2. Имеем $\tau^2 = 1_K$, где 1_K — тождественный автоморфизм. В силу мультипликативности степеней в башнях степени таковы, как указано в последовательностях:

$$Q \xrightarrow{4} Q(\alpha) \xrightarrow{2} K, \qquad Q \xrightarrow{2} Q(i) \xrightarrow{4} K.$$

Таким образом, $x^4 - 2$ неприводим над $\mathbb{Q}(i)$. Кроме того, K нормально над $\mathbb{Q}(i)$. Существует автоморфизм σ поля K над $\mathbb{Q}(i)$, отображающий корень α в $i\alpha$. Несложно проверить, что автоморфизмы 1, σ, σ^2, σ^3 различны и что $\sigma^4 = 1$. Таким образом, σ порождает циклическую группу $\langle\sigma\rangle$ порядка 4. Так как $\tau \notin \langle\sigma\rangle$ и $\langle\sigma\rangle$ имеет индекс 2 в G, то G порождается элементами σ и τ, $G = \langle\sigma, \tau\rangle$. Непосредственно проверяется, что $\tau\sigma = \sigma^3\tau$, поскольку это соотношение выполняется при действии на элементы α и i, порождающие K над $\mathbb{Q}$. Это дает строение группы G. Можно проверить, что структура подгрупп следующая



.

Здесь $H = \langle 1, \sigma^2 \rangle$, $F = \langle 1, \sigma, \sigma^2, \sigma^3 \rangle$, $K = \langle 1, \sigma\tau \rangle$, $N = \langle 1, \sigma^3\tau \rangle$, $L = \langle 1, \sigma^2, \sigma\tau, \sigma^3\tau \rangle$, $T = \langle 1, \sigma^2\tau \rangle$, $R = \langle 1, \tau \rangle$ и $S = \langle 1, \sigma^2, \tau, \sigma^2\tau \rangle$.

Пример 2. Круговые многочлены. Поле разложения Γ_n над $\mathbb{Q}$ многочлена $x^n - 1$ называется *круговым* или *циклотомическим*. Так как все корни степени n из 1 образуют циклическую группу порядка n, то круговое поле имеет вид $\Gamma_n = \mathbb{Q}(\zeta)$, где $\zeta \in \mathbb{C}$ — один из примитивных корней. *Круговым многочленом,* отвечающим Γ_n, называется многочлен $\Phi_n(x) = \prod_{\zeta} (x - \zeta)$ степени $\varphi(n)$, где произведение берется по всем примитивным корням ζ. Имеем равенства

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta^i) = \prod_{d|n} \Phi_d(x), \ \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Так как $\Phi_1(x) = x - 1$ и $\Phi_n(x) = \dfrac{x^n - 1}{\prod\limits_{d|n,\, d<n} \Phi_d(x)}$, то $\Phi_n(x)$ можно вычислить рекуррентно. Все многочлены $\Phi_n(x)$ унитарны и $\Phi_n(x) \in \mathbb{Z}[x]$. Поэтому эти формулы справедливы над любым полем, характеристика которого не делит n. Хорошо известно, что $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ неприводим для любого простого p.

Теорема 31.4. *Круговой многочлен $\Phi_n(x)$ неприводим над $\mathbb{Q}$ и, таким образом, $[\Gamma_n : \mathbb{Q}] = \varphi(n)$. Кроме того, круговое поле Γ_n обладает абелевой группой Галуа, изоморфной $U(\mathbb{Z}_n)$.*

Группа $U(\mathbb{Z}_n)$ — абелева, поэтому каждое подполе в Γ_n нормально. Если заменить $\mathbb{Q}$ на какое-то поле P, то, в общем случае, имеется лишь вложение в $U(\mathbb{Z}_n)$, но не изоморфизм.

Вычисление группы Галуа для конкретного многочлена — непростая задача. Вообще говоря, $\mathrm{Gal}(f)$ — собственная подгруппа в S_n.

Теорема 31.5. *Пусть P — поле,* $\mathrm{char}\, P \neq 2$, *$f(x) \in P[x]$ — унитарный многочлен степени $n \geqslant 1$ с различными корнями θ_i в поле разложения $F \supset P$, $\delta(f) = \prod\limits_{i<j} (\theta_i - \theta_j)$. Тогда подполем в F, отвечающим* $\mathrm{Gal}(f) \cap A_n$, *является $P(\delta(f))$. В частности,* $\mathrm{Gal}(f) \subseteq A_n$ *тогда и только тогда, когда дискриминант $\Delta(f) = (\delta(f))^2$ — квадрат элемента из P.*

Пусть P — поле нулевой характеристики.

Теорема 31.6. *Пусть корни θ_i, $i = 1, \ldots, n$, многочлена $f \in P[x]$ различны. Тогда неприводимость f над P эквивалентна транзитивности* $\mathrm{Gal}(f)$ *на $\{\theta_1, \ldots, \theta_n\}$.*

Теорема 31.7. *Полиномиальное уравнение $f(x) = 0$ разрешимо в радикалах тогда и только тогда, когда группа* $\mathrm{Gal}(f)$ *разрешима.*

Под *общим уравнением n-й степени* понимается уравнение

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots + (-1)^n a_n = 0$$

с неопределенными коэффициентами, принадлежащими основному полю P.

Можно доказать, что общее уравнение сепарабельно и имеет группой Галуа симметрическую группу S_n. Группа S_n имеет нормальную подгруппу A_n. Поскольку при $n > 4$ группа A_n проста, то нормальный ряд $S_n \supset A_n \supset e$ является композиционным. Следовательно, общее уравнение n-й степени при $n > 4$ неразрешимо в радикалах. Хорошо известно, что при $n = 2, 3, 4$ группа S_n разрешима, это обстоятельство лежит в основе формул для решений уравнений второй, третьей и четвертой степени.

Задачи

31.1. Проведите подробное доказательство примера 1 из введения к § 31.

31.2. Если P/K — абелево (соответственно — циклическое) расширение Галуа, то для любого промежуточного поля $K \subset F \subset P$ расширение F над K является абелевым (соответственно, циклическим) расширением Галуа над K.

31.3. Пусть n, m — взаимно простые целые числа $\geqslant 1$. Докажите, что $\Gamma_n \cap \Gamma_m = \mathbb{Q}$.

31.4. Найдите группу Галуа расширения:

а) $\mathbb{C}/\mathbb{R}$; б) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$;

в) L/K, где $(L:K)=2$;

г) $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$.

31.5. Пусть G — конечная группа автоморфизмов поля L и $K=L^G$ — поле неподвижных элементов. Покажите, что L/K — расширение Галуа и $\operatorname{Gal} L/K=G$.

31.6. Найдите круговые многочлены $\Phi_n(x)$ при $n=1,2,\ldots,12$. Покажите, что $\Phi_n(0)=1$ при $n>1$.

31.7. Проверьте следующие свойства круговых многочленов:

а) если p — простое число и $p|n$, то $\Phi_{pn}(x)=\Phi_n\left(x^p\right)$, если же $p\nmid n$, то $\Phi_{pn}(x)=\Phi_n\left(x^p\right)/\Phi_n(x)$;

б) если p — простое число, то $\Phi_{p^m}(x)=\Phi_p\left(x^{p^{m-1}}\right)$ для любого целого $m\geqslant 1$;

в) если $n=p_1^{m_1}\ldots p_k^{m_k}$ — каноническое разложение, то

$$\Phi_n(x)=\Phi_{p_1\ldots p_k}\left(x^{p_1^{m_1-1}\ldots p_k^{m_k-1}}\right);$$

г) если n нечетно, то $\Phi_{2n}(x)=\Phi_n(-x)$.

31.8. Пусть K — конечное расширение Галуа и F — произвольное расширение поля L. Тогда $[KF:F]$ делит $[K:L]$.

31.9. Пусть $\alpha=\sqrt[3]{2}$ — вещественный корень, ς — кубический корень из 1, не равный 1, скажем $\varsigma=\dfrac{-1+\sqrt{-3}}{2}$, и пусть $\beta=\varsigma\alpha$. Пусть, далее $E=\mathbb{Q}(\beta)$, $F=\mathbb{Q}(\alpha)$. Покажите, что:

а) $E\neq F$;

б) $[E:E\cap F]=3$ и, значит, $E\cap F=\mathbb{Q}$;

в) $EF=\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\alpha,\varsigma)=\mathbb{Q}\left(\alpha,\sqrt{-3}\right)$ и $[EF:F]=2$.

Поскольку 3 не делит 2, то этот пример показывает, что утверждение упражнения 31.8, как правило, неверно, если K не является расширением Галуа над L.

31.10. Пусть $P\supset K$ — расширение Галуа с группой G, F и L — два промежуточных поля, $N=\operatorname{Gal} K/F$ и $H=\operatorname{Gal} K/L$ (считаем, что $N,H\subseteq G$). Покажите, что:

а) $N\cap H=\operatorname{Gal} K/FL$;

б) неподвижное поле наименьшей подгруппы в G, содержащей N и H, есть $F\cap L$, т.е. $F\cap L=K^{\langle N,H\rangle}$.

31.11. Пусть $K_1,\ldots,K_n$ — расширения Галуа поля L с группами Галуа $G_1,\ldots,G_n$, причем $K_{i+1}\cap(K_1\ldots K_i)=L$ для каждого $i=1,\ldots,n-1$. Тогда группа Галуа композита $K_1\ldots K_n$ естественным образом изоморфна произведению $G_1\times\ldots\times G_n$.

31.12. Пусть K — конечное расширение Галуа поля L с группой G, причем G может быть представлена в виде прямого произведения $G=G_1\times\ldots\times G_n$, K_i — неподвижное поле группы $G_1\times\ldots\{e\}\times\ldots\times G_n$, где группа из одного элемента стоит на i-м месте. Тогда K_i — расширение Галуа поля L и $K_{i+1}\cap(K_1\ldots K_i)=L$. Кроме того, $K=K_1\ldots K_n$.

31.13. Пусть K — поле и $a\in K$, причем a не является квадратом в K. Тогда многочлен x^2-a не имеет корня в K и поэтому неприводим. Пусть $\operatorname{char}K\neq 2$. Тогда:

а) многочлен x^2-a сепарабелен;

б) если α — некоторый корень многочлена x^2-a, то $K(\alpha)$ — поле разложения, являющееся разложением Галуа с циклической группой порядка 2.

31.14. Пусть K — поле, $\operatorname{char}K\neq 2,3$, $f(x)\in K[x]$ — многочлен степени 3. Тогда при помощи выделения полного куба $f(x)$ можно привести к виду $f(x)=x^3+bx+c$. Допустим, что $f(x)$ не имеет корней в K. Тогда:

а) $f(x)$ неприводим и сепарабелен в K;

б) если α — корень многочлена $f(x)$, то $[K(\alpha):K]=3$;

в) если L — поле разложения многочлена $f(x)$ и $G=\operatorname{Gal}(f)$, то $G\cong A_3$ или $G\cong S_3$;

г) если $G\cong S_3$, то $K(\alpha)$ не является нормальным над K;

д) $G\cong S_3$ в точности тогда, когда дискриминант $\Delta=-4b^3-27c^2$ многочлена $f(x)$ не является квадратом в K.

31.15. Пусть поле K содержит корни n-й степени из 1, причем $\operatorname{char}K=0$ или $\operatorname{char}K=p$, где p не делит n. Тогда:

а) для каждого $0\neq a\in K$ группа Галуа уравнения $x^n-a=0$ циклична;

б) если P/K — циклическое расширение поля K степени n, то $P=K(\sqrt[n]{a})$ для некоторого $0\neq a\in K$.

31.16. Пусть K — поле, $0\neq a\in K$ и $\operatorname{char}K\neq p$. Тогда:

а) если поле K содержит корни p-й степени из 1, то многочлен $x^p - a$ либо неразложим, либо распадается в произведение линейных множителей;

б) если поле K не содержит корни p-й степени из 1, то либо $x^p - a$ неразложим, либо a является p-й степенью в K и имеет место равенство $x^p - a = x^p - \beta^p = (x - \beta)\left(x^{p-1} + \beta\, x^{p-2} + \ldots + \beta^{p-1}\right)$.

31.17. Найдите группы Галуа многочленов над $\mathbb{Q}$:

а) $x^3 - 12x + 8$; б) $x^3 - 3x + 1$;

в) $x^3 - 2x - 2$; г) $x^3 + x + 1$;

д) $x^4 + 4x^2 + 2$; е) $x^4 + x^2 + 1$;

ж) $x^3 + x^2 - 2x - 1$ (напомним, что дискриминант многочлена $x^3 - a_1x^2 + a_2x - a_3$ совпадает с выражением $-4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2$).

31.18. Найдите группы Галуа многочленов:

а) $x^3 - 10$ над $\mathbb{Q}\left(\sqrt{2}\right)$ и над $\mathbb{Q}\left(\sqrt{-3}\right)$;

б) $x^3 - x - 1$ над $\mathbb{Q}\left(\sqrt{-23}\right)$.

31.19. Покажите, что круговое поле $\Gamma_{17} = \mathbb{Q}(\varsigma)$, $\varsigma^{17} = 1$, имеет циклическую группу Галуа $G = \operatorname{Gal}\Gamma_{17}/\mathbb{Q} = \left\langle \Phi \,|\, \Phi^{16} = 1 \right\rangle$, порожденную отображением $\Phi\colon \varsigma \to \varsigma^3$ (3 — примитивное по модулю 17 число). Следовательно, базис поля деления круга состоит из 16 элементов: $\varsigma, \varsigma^3, \varsigma^9, \ldots$. Существуют подполя степеней 2, 4 и 8. Им соответствует ряд подгрупп:

$$G = G_1 = \langle\Phi\rangle \supset G_2 = \left\langle\Phi^2\right\rangle \supset G_3 = \left\langle\Phi^4\right\rangle \supset G_4 = \left\langle\Phi^8\right\rangle \supset G_5 = e.$$

31.20. Круговое поле Γ_{12} имеет группу Галуа, изоморфную $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, собственным подгруппам которой соответствуют подполя $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{-3}\right)$ и $\mathbb{Q}\left(\sqrt{3}\right)$.

31.21. Убедитесь, что полем разложения многочлена $x^3 - 2 \in \mathbb{Q}[x]$ является

$$F = \mathbb{Q}(\alpha, \varepsilon) = \left\langle 1, \alpha, \alpha^2, \varepsilon, \varepsilon\alpha, \varepsilon\alpha^2 \right\rangle_{\mathbb{Q}} = \mathbb{Q}(\theta),$$

где $\alpha = \sqrt[3]{2}$ — вещественный корень, $\varepsilon^2 + \varepsilon + 1 = 0$, $\theta = \alpha + \varepsilon$. Группа Галуа имеет строение

$$G = \operatorname{Gal} F/\mathbb{Q} = \left\langle \sigma, \tau \,|\, \sigma^3 = e = \tau^2, \tau\sigma\tau = \sigma^2 \right\rangle \cong S_3,$$

где $\sigma(\varepsilon) = \varepsilon$, $\sigma(\alpha) = \varepsilon\alpha$, $\sigma(\varepsilon\alpha) = \varepsilon^2\alpha$, $\tau(\alpha) = \alpha$, $\tau(\varepsilon) = \varepsilon^2$. Убедитесь, что в следующей таблице под каждой подгруппой $H \subseteq G$ выписано соответствующее ей неподвижное поле:

G	$\langle\sigma\rangle$	$\langle\tau\rangle$	$\langle\sigma\tau\rangle$	$\langle\sigma^2\tau\rangle$	e
$\mathbb{Q}$	$\mathbb{Q}(\varepsilon)$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\varepsilon^2\alpha)$	$\mathbb{Q}(\varepsilon\alpha)$	F

,

так что $\langle\sigma\rangle = \operatorname{Gal} F/\mathbb{Q}(\varepsilon)$, $\langle\tau\rangle = \operatorname{Gal} F/\mathbb{Q}(\alpha)$, $\langle\sigma\tau\rangle = \operatorname{Gal} F/\mathbb{Q}\left(\varepsilon^2\alpha\right)$, $\left\langle\sigma^2\tau\right\rangle = \operatorname{Gal} F/\mathbb{Q}(\varepsilon\alpha)$.

31.22. Найдите группу Галуа над полем $\mathbb{Q}$ уравнения $x^8 + 1 = 0$.

31.23. (Теорема о нормальном базисе). Докажите, что во всяком конечномерном расширении Галуа L поля K с группой Галуа G существует такой элемент a, что множество $\{\sigma(a) \,|\, \sigma \in G\}$ является базисом поля L над K.

31.24. Пусть $a_1, \ldots, a_n$ — алгебраически независимые элементы над полем K; $s_1, \ldots, s_n$ — элементарные симметрические многочлены от $a_1, \ldots, a_n$, $F = K(a_1, \ldots, a_n)$ и $f(x) = \prod\limits_{i=1}^{n}(x - a_i)$. Группа $G = S_n$ действует на F, переставляя $(a_1, \ldots, a_n)$. Покажите, что $P = F^G = K(s_1, \ldots, s_n)$ и $G = \operatorname{Gal} F/P$.

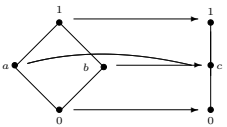
31.25. Всякая конечная группа является группой Галуа некоторого расширения полей.

31.26. Группа Галуа всякого конечного расширения L поля F_p циклическая и порождается автоморфизмом $x \mapsto x^p$ $(x \in L)$.

Глава VII. Ответы и указания

1. Решетки

1.5. Возьмем следующее отображение f решеток



$f(0)=0$, $f(a)=f(b)=c$, $f(1)=1$. f — изотонное отображение, но не гомоморфизм, поскольку $f(a+b)=f(1)\neq c=f(a)+f)b)$.

1.17. Докажем первое утверждение. Пусть P — множество всех таких $x\in L$, что $x\leqslant\varphi x$. Ясно, что $0\in P$. Поэтому $P\neq\varnothing$. Если $a=\sup P$, то $\varphi a\geqslant\varphi x\geqslant x$ для всякого $x\in P$. Отсюда $\varphi a\geqslant a$. Тогда $\varphi(\varphi a)\geqslant\varphi a$, это влечет $\varphi a\in P$ и, значит, $a\geqslant\varphi a$. Таким образом, $a\geqslant\varphi a\geqslant a$, т.е. $\varphi a=a$.

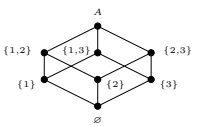
1.28. Если справедливо а), то $a(ab+c)=ab+ac$ для любых $a,b,c\in L$. Если же, кроме того, выполнены условия в), то $a=a(a+c)=a(b+c)=b+ac=b+bc=b$. Таким образом, справедливы импликации а)$\Rightarrow$ б) и а)$\Rightarrow$ в). Если выполнено б) и $a\leqslant c$, то $(a+b)c=(ac+b)c=ac+bc=a+bc$, т.е. б) $\Rightarrow$ а). Допустим, что справедливо в). Если $a\leqslant c$, то $a+b\leqslant(a+b)c+b\leqslant a+b$ и $bc\leqslant(a+bc)b\leqslant(c+bc)b=bc$. Отсюда $(a+b)c+b=(a+bc)+b=a+b$ и $(a+b)cb=(a+bc)b=bc$. Так как $(a+b)c\geqslant a+bc$, то, применяя в), получаем $(a+b)c=a+bc$, что доказывает импликацию в) $\Rightarrow$ а).

1.34. Докажем, например, эквивалентность первых трех условий. Импликация а) $\Rightarrow$ б) вытекает из равенств $(a+c)(b+c)=(a+c)b+c=ab+bc+c=ab+c$. А б) $\Rightarrow$ в) — из $ab+bc+ca=(a+bc+ca)(b+bc+ca)=(a+bc)(b+ca)=(b+a)(c+a)(b+c)(b+a)=(a+b)(b+c)(c+a)$.

в) $\Rightarrow$ а). Если $a\leqslant c$, то $ac+bc=ab+bc+ca=(a+b)(b+c)(c+a)=c(a+b)(b+c)=c(a+b)$, значит, в L справедлив модулярный закон. Положим $u=ab+bc+ac$ и $v=(a+b)(b+c)(a+c)$. По условию $u=v$. Поскольку $ac+bc\leqslant c$, то $cu=c(ab+bc+ac)=c(bc+ac)+abc=ac+bc$ и $cv=c(a+b)(b+c)(a+c)=c(a+b)$, что и требовалось.

1.35. Пусть b и c являются дополнениями некоторого элемента a. Тогда $b=b\cdot1=b(a+c)=ba+bc=0+bc=bc$ и, значит, $b\leqslant c$. Аналогично, $b\geqslant c$.

1.41.



1.44. Из единственности дополнения вытекает, что $a''=a$. Воспользуемся 1.34. Допустим, что $a+c=v=b+c$ и $ac=u=bc$. Заметим, что если $s,t\in L$ и $s\leqslant t$, то $s=(s+t')t$ и $t=s+s't$. Поэтому получаем равенства $a+(v'+cu')=a+(u+cu')+v'=(a+c)+v'=1=(b+c)+v'=b+(u+cu')+v'=b+(v'+cu')$ и $a(v'+cu')=av(v'+cu')=(ac)u'=0=(bc)u'=bv(v'+cu')=b(v'+cu')$. Следовательно, $a=(v'+cu')'=b$, что и требовалось доказать.

1.52. Для подпространства A пространства V, правого идеала J и левого идеала L кольца R положим $\operatorname{Hom}(V,A)=\{f\in R\,|\,fV\subseteq A\}$, $A^{\perp}=\{f\in R\,|\,fA=0\}$, JV — множество всех конечных сумм вида $\sum f_i(a_i)$ $(f_i\in J,a_i\in V)$ и $L^{\perp}=\{a\in V\,|\,f(a)=0$ для всех $f\in L\}$. Соответствия $A\to\operatorname{Hom}(V,A)$, $J\to JA$ являются требуемыми взаимно обратными изоморфизмами, а соответствия $A\to A^{\perp}$, $L\to L^{\perp}$ — взаимно обратными антиизоморфизмами.

1.53. Транспонирование матриц осуществляет изоморфизм решеток. Их антиизоморфизм, а также самодвойственность из 1.52 и 1.53 получаются теперь из 1.52. При этом следует учесть, что кольцо матриц порядка n изоморфно кольцу операторов векторного пространства размерности n.

2. Полугруппы

2.30. Каждому элементу $a\in S^1$ поставим в соответствие отображение L_a множества S^1 в себя по правилу: $L_a(x)=ax\quad(x\in S^1)$. Так как $(L_b\circ L_a)x=L_b(L_ax)=L_b(ax)=(ba)x=L_{ba}(x)$, то $L_b\circ L_a=L_{ba}$. Поэтому отображение $a\mapsto L_a$ есть гомоморфизм S^1 на подполугруппу из $F(S^1)$. Поскольку $L_a(1)=a$, то это инъективное отображение.

2.37. Если не все степени элемента a различны, то пусть s — наименьшее положительное целое число, такое, что $a^s=a^r$, где $r<s$. Нетрудно заметить, что такое положительное целое число r определяется однозначно. Тогда $m=s-r$. Имеем $a^{r+km}=a^r$ для каждого натурального k. Легко видеть, что каждая степень элемента a, начиная с a^r и далее, равна одному из элементов множества $Ka=\{a^r,a^{r+1},\dots,a^{r+m-1}\}$. Отсюда следует, что a имеет конечный порядок, равный $r+m-1$. Множество Ka является подполугруппой в S. Если каждому элементу $a^n\in Ka$ $(r\leqslant n\leqslant r+m-1)$ поставить в соответствие класс вычетов $n+m\mathbb{Z}$ по модулю m, содержащий n, то отображение $a^n\mapsto n+m\mathbb{Z}$ будет изоморфизмом Ka на аддитивную группу кольца $\mathbb{Z}_m$. Следовательно, Ka — циклическая группа порядка m.

2.41. Такова, например, полугруппа, порожденная преобразованием

$$\begin{pmatrix} 0 & 1 & 2 & \dots & r-1 & r & \dots & r+m-2 & r+m-1 \\ 1 & 2 & 3 & \dots & r & r+1 & \dots & r+m-1 & r \end{pmatrix}.$$

2.43. 1) Если $pq = p'q' = 1$, то $(pp')(q'q) = 1$, это доказывает, что P и Q — подполугруппы в S. Если $ap = bp$, где $a, b \in S$ и $p \in P$, то p имеет правый обратный q и $a = apq = bpq = b$. Аналогично, Q — полугруппа с левым сокращением.

2) Ясно, что $U = P \cap Q$ и потому U есть подполугруппа в S. Если $u \in U$ и $xu = uy = 1$, то $x = xuy = y$. Откуда следует, что u имеет единственный двусторонний обратный элемент u' и не имеет других левых и правых обратных элементов. Так как $uu' = u'u = 1$, то $u' \in U$, и, следовательно, U является группой.

2.45. а) Покажите, что единица f подгруппы G совпадает с e. Так как e — двусторонняя единица в G, то $G \subseteq eSe$. Откуда $G \subseteq H_e$.

2.49. б) Если $a = axa$, то $a \in aS$, значит, $aS^1 = aS$.

в) Если $axa = a$, то для $e = ax$ имеем $ea = a$. Откуда $aS^1 = eS^1$. Обратно, если $aS^1 = eS^1$, где $e^2 = e$, то $a = ex$ при некотором $x \in S^1$. Поэтому $ea = e^2x = ex = a$, $e = ay$ для некоторого $y \in S^1$, откуда $a = ea = aya$. Если $y = 1$, то $a = a^2$ и $a = aaa$.

2.51. Так как $\rho \circ \sigma \subseteq \rho \vee \sigma$, то достаточно показать, что $\rho \circ \sigma$ есть отношение эквивалентности. Из $\iota \subseteq \rho \subseteq \rho \circ \sigma$ следует рефлексивность, равенства $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1} = \sigma \circ \rho = \rho \circ \sigma$ доказывают симметричность, а $(\rho \circ \sigma) \circ (\rho \circ \sigma) = \rho \circ \sigma \circ \rho \circ \sigma = \rho \circ \rho \circ \sigma \circ \sigma = \rho \circ \sigma$ — транзитивность.

2.55. Пусть $b = xax$. Тогда $aba = a(xax)a = ax(axa) = axa = a$,

$$bab = (xax)a(xax) = x(axa)(xax) = xa(xax) = x(axa)x = xax = b,$$

т.е. b инверсен к a.

2.56. Если a и b — коммутирующие инверсные друг к другу элементы полугруппы S, то $e = ab$ $(= ba)$ есть идемпотент, причем $ea = ae = a$ и $eb = be = b$. Следовательно, a и b — обратимые элементы в eSe, принадлежащие максимальной подгруппе H_e полугруппы S, содержащей e. Так как $ab = ba = e$, то a и b — взаимно обратные в H_e. Обратное утверждение очевидно.

2.57. Пусть X и Y — два произвольных множества. На $S = X \times Y$ определим операцию

$$(x_1, y_1)(x_2, y_2) = (x_1, y_2) \quad (x_1, x_2 \in X;\ y_1, y_2 \in Y).$$

Легко проверить, что S удовлетворяет требуемому условию.

2.58. а) $\Rightarrow$ б). Каждый правый идеал полугруппы S имеет по крайней мере один порождающий идемпотент. Предположим, что идемпотенты e, f порождают один и тот же главный правый идеал: $eS = fS$. Тогда $ef = f$ и $fe = e$. Так как $ef = fe$, то $e = f$.

б) $\Rightarrow$ в). Полугруппа S регулярна. Осталось показать единственность инверсного элемента. Пусть b и c инверсны к a. Тогда $aba = a$, $bab = b$, $aca = a$, $cac = c$. Отсюда $abS = aS = acS$ и $Sba = Sa = Sca$, это влечет $ab = ac$ и $ba = ca$. Следовательно, $b = bab = bac = cac = c$.

в) $\Rightarrow$ а). Нужно показать коммутирование произвольных идемпотентов e, f. Пусть a — (единственный) инверсный к ef элемент. Тогда $(ef)a(ef) = ef$, $a(ef)a = a$. Положим $b = ae$. Тогда

$$(ef)b(ef) = efae^2f = efaef = ef, \quad b(ef)b = ae^2fae = aefae = ae = b.$$

Следовательно, b также инверсен к ef. Поэтому $ae = b = a$. Аналогично, $fa = a$. Следовательно, $a^2 = (ae)(fa) = a(ef)a = a$. Откуда $a = ef$ — идемпотент, fe также идемпотент. Они инверсны друг к другу. Итак, $ef = fe$.

2.59. Первое соотношение очевидно. Докажем второе. Имеем

$$(ab)(b^{-1}a^{-1})(ab) = a(bb^{-1})(a^{-1}a)b = a(a^{-1}a)(bb^{-1})b = ab,$$
$$(b^{-1}a^{-1})(ab)(b^{-1}a^{-1}) = b^{-1}(a^{-1}a)(bb^{-1})a^{-1} = b^{-1}(bb^{-1})(a^{-1}a)a^{-1} = b^{-1}a^{-1}.$$

Следовательно, $b^{-1}a^{-1}$ инверсен к ab.

2.66. См., например, [18, теорема 1.23].

2.67. Если G — группа левых частных полугруппы S и $a, b \in S$, то элемент $ab^{-1} \in G$ можно представить в виде $ab^{-1} = x^{-1}y$ для некоторых $x, y \in S$. Отсюда $xa = yb \in Sa \cap Sb$, что доказывает правую реверсивность S.

Пусть теперь S реверсивна справа. По 2.66 ее можно вложить в группу G. Пусть G_1 — множество всех элементов из G, имеющих вид $a^{-1}b$, где $a, b \in S$. Если $a^{-1}b \in G_1$, то $(a^{-1}b)^{-1} = b^{-1}a \in G_1$. Пусть $a^{-1}b$ и $c^{-1}d$ — произвольные элементы из G_1. По предположению существуют такие $x, y \in S$, что $xb = yc$. Тогда $bc^{-1} = x^{-1}y \in G$ и потому $a^{-1}bc^{-1}d = a^{-1}x^{-1}yd = (xa)^{-1}(yd) \in G_1$. Следовательно, G_1 — подгруппа группы G, являющаяся группой левых частных полугруппы S.

Пусть $(G, \cdot)$ и $(H, *)$ — две группы левых частных полугруппы S. В G имеет место равенство $a^{-1}b = c^{-1}d$ в точности тогда, когда каждое из равенств $xa = yc$, $xb = yd$, $x, y \in S$, влечет за собой другое. Кроме того, $(a^{-1}b)(c^{-1}d) = (xa)^{-1}(yd)$, где $x, y \in S$ — такие элементы, что $xb = yc$. Но те же самые условия для равенств и произведений выполняются и в H. Поэтому отображение $a^{-1}b \mapsto a^{-1} * b$ есть изоморфизм G на H, оставляющий элементы из S неподвижными.

3. Группы. Порождающие множества групп

3.22. Если в группе нет элементов порядка 2, то $G = \{(x, x^{-1}) \,|\, x \neq e\} \cup \{e\}$ и $|G|$ нечетен.

3.37. $p^m - p^{m-1}$.

3.38. 1) Необходимость. Пусть (A, B) — дистрибутивная пара. Если $c \in \langle A, B\rangle \setminus (A \cup B)$, то $C = \langle c\rangle = \langle C \cap A, C \cap B\rangle$, где $C \cap A, C \cap B \neq e$. Порядки n_A и n_B конечны. Пусть $c^{n_A} = a$ порождает подгруппу $\langle a\rangle = C \cap A$ и элемент $c^{n_B} = b$ порождает $\langle b\rangle = C \cap B$. Так как $\langle c\rangle = \langle a, b\rangle$, то $c = a^s b^t$ или $n_A s + n_B t \equiv 1 \pmod{\text{порядка } c}$. Отсюда следует, что n_A и n_B взаимно просты. Достаточность. Так как для циклической подгруппы $C = \langle c\rangle \subseteq \langle A, B\rangle$ следует, что $C = \langle C \cap A, C \cap B\rangle$, то отсюда вытекает справедливость подобного равенства для любой подгруппы C.

3.40. Имеем $D = \langle a\rangle \cap \langle b\rangle = e$, а если $k = |\langle ab\rangle|$, то $a^k b^k = (ab)^k = e$. Откуда $a^k = b^{-k} \in D = e$. Следовательно, $a^k = e = b^k$ и, значит, $m,\, n \,|\, k$. Из $(m, n) = 1$ следует, что $mn \,|\, k$. Но $(ab)^{mn} = e$, значит, $k \,|\, mn$. Следовательно, $k = nm$. Так как $\langle a,\, b\rangle = \{a^i b^j \,|\, 0 \leqslant i \leqslant n-1,\ 0 \leqslant j \leqslant m-1\}$, то $|\langle a,\, b\rangle| \leqslant mn$. Теперь из $\langle ab\rangle \subseteq \langle a,\, b\rangle$ и $|\langle ab\rangle| = mn$ вытекает равенство $\langle a,\, b\rangle = \langle ab\rangle$.

3.42. Пусть $n = |G|$, $d = \exp(G)$.

а) Вытекает из теоремы Лагранжа.

б) Пусть $d = p_1^{k_1} \dots p_s^{k_s}$ — разложение на простые множители. В G существует элемент x, порядок которого равен $p_1^{k_1} l$, где l и p_1 взаимно просты. Поэтому x^l имеет порядок $p_1^{k_1}$. Аналогично получаются элементы $x_2, \dots, x_s$. Произведение $x_1 \dots x_s$ имеет порядок d.

3.43. 2) $\mathbb{Z}_{p^n}$; 3) $\bigcup\limits_{n=1}^{\infty} \left\langle \frac{1}{n!} \right\rangle$.

3.45. Хорошо известно, что бесконечная циклическая группа содержит бесконечное (счетное) множество подгрупп. Допустим, что в группе G все ее циклические подгруппы конечны, причем только следующие $\{\langle g_i\rangle \,|\, i = 1, \dots n\}$ среди них — различны. Тогда $G = \bigcup\limits_{i=1}^{n} \langle g_i\rangle$ — конечная группа.

3.51. 1) $S \subseteq \Phi(G)$. Действительно, если G не содержит максимальных подгрупп, то утверждение тривиально. Пусть теперь $x \in S$, H — максимальная подгруппа из G. Если $x \notin H$, то $\langle x, H\rangle = G$, $H \neq G$. Это противоречит включению $x \in S$. Следовательно, $x \in H$ и, значит, $x \in \Phi(G)$.

$\Phi(G) \subseteq S$. Пусть, напротив, существует элемент $x \in \Phi(G)$, который вместе с множеством M порождает G, но $\langle M\rangle \neq G$. По лемме Цорна существуют подгруппы H, максимальные среди подгрупп, содержащих M и не содержащих x. Ясно, что эти подгруппы просто максимальны. Но тогда они содержат $\Phi(G)$, а вместе с ней x, вопреки построению.

3.53. Циклическая группа.

3.54. а) Делаем подстановку $x \to 1 - x$ и записываем систему

$$\begin{cases} 2f(1-x) + 1 &= x\, f(x), \\ 2f(x) + 1 &= (1-x) f(1-x). \end{cases}$$

Ее решением служит функция $f(x) = \frac{x-3}{x^2-x+4}$.

б) $f(x) = \frac{4x^2-x+1}{5x(x-1)}$. в) $f(x) = \frac{6x-2}{7x}$.

4. Изоморфизмы групп. Смежные классы

4.6. Других автоморфизмов нет.

4.24. 3) Если бы подгруппа из 6 элементов содержалась в A_4, то по 1) она была бы изоморфна $\mathbb{Z}_6$ или S_3. Но никакая подстановка на 4 символах не может быть порядка 6, поэтому первый случай невозможен. Невозможен и второй, так как в S_3 существуют неперестановочные элементы порядка 2, а в A_4 их нет. В самом деле, A_4 содержит три элемента порядка 2: (12)(34), (13)(24), (14)(23), и все они попарно перестановочны.

4.27. 2) Допустим, что $f\colon \mathbb{Q} \to \mathbb{Q}_+^*$ — изоморфизм. Тогда $f(b) = 2$ для некоторого $b \in \mathbb{Q}$. Если теперь $f(b/2) = a \in \mathbb{Q}_+^*$, то $f(b) = f(\frac{b}{2} + \frac{b}{2}) = a^2 = 2$. Противоречие с иррациональностью $\sqrt{2}$.

4.29. Пусть $K = G \setminus H$ и $a \in K$. Тогда $aH = K$ и $aK = H$. Откуда $a^2 \in H$.

4.38. а) $G = e$ или $G \cong \mathbb{Z}_p$; б) $G \cong \mathbb{Z}_{p^2}$;

в) $G \cong \mathbb{Z}_{p^3}$ или $G \cong \mathbb{Z}_{pq}$;

г) $G \cong \mathbb{Z}_{p^4}$ или $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4.39. $G \cong \mathbb{Z}_{p^m}$ $(G \cong \mathbb{Z}_{p^m q^n})$.

4.40. 2) $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ c & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ c & 1 \end{pmatrix}$, $\begin{pmatrix} a & b \\ (1-a^2)/b & -a \end{pmatrix}$, где $a, b, c \in \mathbb{C}$, $b \neq 0$.

4.43. Пусть U — подгруппа в G индекса j, $K_1 = U$, $K_2, \dots, K_j$ — все левые смежные классы по подгруппе U. Для всякого $g \in G$ переход к системе $gK_1, \dots, gK_n$ определяет перестановку, поэтому получаем гомоморфное отображение φ группы G в группу S_j. Гомоморфизм φ вполне определяется заданием образов элементов $a_1, \dots, a_n$, значит, существует не более $(j!)^n$ различных гомоморфизмов группы G в S_j. Гомоморфизм φ однозначно определяет подгруппу U, поэтому G содержит не больше $(j!)^n$ подгрупп индекса j.

5. Гомоморфизмы. Факторгруппы

5.3. а) $\Rightarrow$ б). Пусть $ab \in H$. Тогда $a(ab)a^{-1} = a^2ba^{-1} \in H$. Откуда $(a^2ba^{-1})(ab) = a^2b^2 \in H$. б) $\Rightarrow$ а). Из $a^{-1}(ah) = h \in H$ следует $a^{-2}(ah)^2 = a^{-1}hah \in H$ и, значит, $a^{-1}ha \in H$.

5.34. Группы порядка 2.

5.36. 2) Группа S_4 действует на кубе. Если занумеровать три пары противоположных граней куба числами 1, 2, 3, то получим действие группы на множестве $\{1, 2, 3\}$. Ядром этого действия является подгруппа V_4.

3) Воспользуйтесь 5.35. Ясно, что $\pm E$ — нормальная подгруппа в Q_8 (она совпадает с центром). Других подгрупп порядка 2 нет. А остальные подгруппы (индекса 2) нормальны. Аналогичным образом рассмотрите подгруппы в $\mathbb{Z}_2 \times Q_8$.

5.37. $|G|$ равен p^2 или pq.

5.39. Пересечение N всех подгрупп группы G, сопряженных с H, является нормальной в G подгруппой. Покажите, что отображение $\sigma_g\colon aH \mapsto gaH$ есть перестановка на множестве M всех левых смежных классах группы G по подгруппе H. Тогда $f\colon gN \mapsto \sigma_g$ вкладывает G/N в некоторую подгруппу группы $S(M) \cong S_k$.

5.40. Пусть $N \trianglelefteq G$ — такая же, как в 5.39. Тогда $p!$ делится на $|G/N|$ и $|G/N| \geqslant p$, ибо $N \subseteq H$. Но по условию p — минимальный простой делитель числа $|G|$, значит, у числа $|G/N|$ не может быть простых делителей $< p$. Поэтому $|G/N| = p$, т.е. индексы, а следовательно, и порядки подгрупп N и H совпадают. Следовательно, $N = H$.

5.42. 1) Пусть $|M| = k$, m — наименьшее общее кратное порядков всех элементов из M и $A = \langle M\rangle$. Всякий элемент из A может быть записан в виде произведения элементов из M. Достаточно показать, что среди этих записей для каждого $a \in A$ найдутся такие, которые состоят не более чем из $k(m-1)$ множителей. Пусть дана запись (1): $a = a_1 \dots a_s$ и $s > k(m-1)$. В этом случае хотя бы один из элементов, например a_0, встречается в (1) не менее m раз. Если a_i есть первый из элементов записи (1), равный a_0, то, полагая $a_0^{-1}a_ja_0 = a'_j$, получим $a = a_0a'_1 \dots a'_{i-1}a_{i+1} \dots a_s$, где $a'_j \in M$. Применяя этот же прием к первому из элементов $a_{i+1}, \dots, a_s$, равному a_0, и т.д., через конечное число шагов получим запись $a = a_0^m\overline{a}_1 \dots \overline{a}_{s-m}$, что ввиду $a_0^m = e$ приводит к записи с $s - m$ множителями.

6. Центр и коммутант. Прямые произведения. Силовские подгруппы

6.15. 2) Вытекает из 6.14 2).

6.34. A и C сопряжены, так как имеют одинаковую жорданову форму, а A и B не сопряжены.

6.36. 5) Пусть $|G| = p^lm$ и $|H| = p^st$, где m и t не делятся на p. Порядок p-подгруппы PH/H в G/H не больше p^{t-s}, поэтому порядок ядра $P \cap H$ канонического гомоморфизма $P \to PH/H$ не меньше p^s, что и требовалось доказать.

6.37. 4) Для группы порядка 36 и ее силовской 3-подгруппы примените 5.39. Пусть теперь G — группа порядка 80. Если силовская 5-подгруппа не является нормальной, то должно быть 16 различных 5-подгрупп. Поскольку их попарные пересечения тривиальны, в группе не больше, чем $80 - 16 \cdot 4 = 16$ элементов, порядки которых степени двойки, они могут образовывать лишь одну силовскую 2-подгруппу, которая, следовательно, нормальна. К другим группам примените подобные рассуждения.

5) Если $p > q$, то число m подгрупп порядка p^2 сравнимо с 1 по модулю p только при $m = 1$. Если $p < q$, то число q-подгрупп сравнимо с 1 по модулю q и делит p или p^2. Так как p оно делить не может, оно равно p^2; следовательно, элементов порядка q будет $p^2(q-1)$. Однако подгруппа порядка p^2 существует, поэтому она единственна ($p^2q = p^2(q-1) + p^2$).

6.38. Пять силовских 2-подгрупп и одна силовская 5-подгруппа.

6.39. 4) Элемент лежит в центре, если и только если он совпадает со всеми сопряженными ему элементами. Поэтому, если в центре лежит лишь одна единица, то $p^n = 1 + p^{k_1} + \dots + p^{k_s}$ ($k_i \geqslant 1$) (число элементов любого класса сопряженности делит порядок группы). Противоречие.

6.42. $p^2 + p - 1$, причем p классов состоит из одного элемента, а остальные — из p элементов. Центр $Z(G)$ имеет порядок p. Централизатор любого элемента $g \notin Z(G)$ имеет порядок p^2, так как он содержит $Z(G) \cup \{g\}$ и не совпадает со всей группой. Число сопряженных с g элементов равно p.

6.43. Произведения $a_0b_1 \dots a_{n-1}b_na_n$ элементов максимальных подгрупп A и B составляют подгруппу C, строго содержащую A и B. Поэтому $C = G$. Элементы из $A \cap B$ перестановочны с элементами из C, так как A и B коммутативны.

6.45. Учесть свойство сохранения порядка элемента при сопряжении.

6.48. 2) а) $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$; б) $\mathbb{Z}_6$, S_3; в) $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_8; г) $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$; д) D_5, $\mathbb{Z}_5 \times \mathbb{Z}_2$.

Таблица, указывающая число групп G заданного непростого порядка $|G| \leqslant 33$.

$\lvert G\rvert$	4	6	8	9	10	12	14
число групп	2	2	5	2	2	5	2
$\lvert G\rvert$	15	16	18	20	21	22	24
число групп	1	14	5	5	2	2	15
$\lvert G\rvert$	25	26	27	28	30	32	33
число групп	2	2	3	4	4	51	1

6.51. 1) Рассмотрите группу S_3.

6.55. Число $p!$ делится на p, но не делится на p^2, поэтому каждая силовская p-подгруппа состоит из степеней одного цикла $(i_1 \dots i_p)$. Число таких циклов равно $(p-1)!$, а число различных порождающих в циклической подгруппе порядка p равно $p - 1$.

6.56. 1) Покажите, что $|\operatorname{SL}(2, F_p)| = p(p-1)(p+1)$ и $|\operatorname{GL}(2, F_p)| = p(p^2-1)(p-1)$, значит, силовская p-подгруппа имеет порядок p.

2) Нормализатор состоит из всех матриц вида $\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}$, где $x \neq 0$; а в $\mathrm{GL}(2, F_p)$ из всех матриц вида $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$, где $x, z \neq 0$.

3) $p+1$ (совпадает с индексом соответствующего нормализатора).

6.57. В $\mathrm{GL}(n, F_q)$: $(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$. При подсчете числа невырожденных матриц заметить, что если выбраны i первых строк, то для выбора $(i+1)$-й строки имеется q^n-q^i возможностей: действительно, всего существует q^n различных строк длины n над полем из q элементов, но в качестве $(i+1)$-й строки подходят лишь те из них, которые не являются линейными комбинациями i строк, выбранных раньше. Число таких линейных комбинаций — это число упорядоченных наборов, составленных из i коэффициентов, т.е. q^i.

В $\mathrm{SL}(n, F_q)$: $\dfrac{1}{q-1}(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$. Подгруппа $\mathrm{SL}(n, F_q)$ есть ядро гомоморфизма $A \to \det A$ группы $\mathrm{GL}(n, F_q)$ на мультипликативную группу поля F_q (состоящую из $q-1$ элементов), поэтому $|\mathrm{GL}(n, F_q)/\mathrm{SL}(n, F_q)| = q-1$. Остается применить теорему Лагранжа.

Последнее утверждение вытекает из того, что порядок подгруппы и максимальная степень числа q, делящая $|\mathrm{GL}(n, F_q)|$ и $|\mathrm{SL}(n, q)|$, равны $q^{n(n-1)/2}$.

6.60. $n_1 n_2$.

6.65. $\mathbb{Z}_{p^n}$ при $n \geqslant 0$, $\mathbb{Z}_p \times \mathbb{Z}_p$ и Q_8.

6.67. Диагональная подгруппа; $\mathrm{UT}(2, F_q) \times Z(G)$, где $\mathrm{UT}(2, F_q)$ — унитреугольная подгруппа группы $G = \mathrm{GL}(2, F_q)$.

6.69. 2) Число инволюций равно q^2-1 при четном q и равно q^2+q+1 при нечетном q.

7. Ряды подгрупп. Разрешимые и нильпотентные группы

7.4. 6) Группа порядка 12 или 20 разрешима, так как имеет нормальную силовскую подгруппу по 6.37. В группе порядка 42 силовская 7-подгруппа нормальна, а в группе порядка 100 нормальна силовская 5-подгруппа.

7.9. 5) Коммутативные группы: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ и $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. При $p=2$ — некоммутативные группы: группа диэдра и группа кватернионов. При $p>2$ — некоммутативные группы: $\langle a, b \,|\, a^{p^2} = b^p = e,\ b^{-1}ab = a^{1+p}\rangle$ и $\langle a, b, c \,|\, a^p = b^p = c^p = e,\ [a,b]=c,\ [a,c]=[b,c]=e\rangle$.

7.10. 1) Для разрешимых групп утверждение вытекает из того, что расширение разрешимой группы при помощи разрешимой группы разрешимо. Пусть $G = G_1 \times \ldots \times G_s$, где все G_k — нильпотентные группы. Выберем в этих группах по одному центральному ряду, причем считаем, что длины этих рядов совпадают, допуская, если нужно, ряды с повторениями. Пусть $e = G_{k0} \subseteq \ldots \subseteq G_{kn} = G_k$ — центральный ряд группы G_k. Подгруппы $A_i = G_{1i} \times \ldots \times G_{si}$, $i = 0, \ldots, n$, будут составлять центральный ряд группы G.

3) Предположим, что A не нормальна в G. Тогда существует сопряженная с A подгруппа $B \neq A$. Имеем $\langle A, B\rangle = G$ (в силу квазинормальности этой подгруппы и максимальности A). Но это невозможно, ибо из $b^{-1}a^{-1}Aab = B$ вытекает, что $A = a^{-1}Aa = bBb^{-1} = B$.

7.11. Пусть $a \in G$ и $H = \langle a, G'\rangle$. Так как $G' \subseteq Z_{s-1}(G) \cap H \subseteq Z_{s-1}(H)$, то группа $H/Z_{s-1}(H)$ циклическая. Поскольку факторгруппа по центру не может быть циклической, отличной от e, то $Z_{s-1}(H) = H$, что и требовалось.

7.12. Пусть $Z_i = Z_i(G)$, $H_0 = H$, $H_{j+1} = N_G(H_j)$. Достаточно проверить, что $Z_i \subseteq H_i$. Для $i=0$ это очевидно. Перейдем от i к $i+1$. Так как $[G, Z_{i+1}] \subseteq Z_i \subseteq H_i$, то $H_i^{Z_{i+1}} \subseteq H_i[H_i, Z_{i+1}] \subseteq H_i$. Это означает, что Z_{i+1} нормализует H_i, т.е. $Z_{i+1} \subseteq H_{i+1}$.

7.13. а) Пусть $e = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ — центральный ряд группы G, и H — подгруппа в G. Если $H_i = G_i \cap H$, то $[H_{i+1}, H] \subseteq [G_{i+1}, G] \cap H = H_i$ и поэтому подгруппы H_i составят после удаления повторений центральный ряд для H. Пусть теперь $\varphi\colon G \to \overline{G}$ — эпиморфизм, $\overline{G}_i = \varphi(G_i)$, $\overline{g}_{i+1} \in \overline{G}_{i+1}$, $\overline{g} \in \overline{G}$, $\varphi(g_{i+1}) = \overline{g}_{i+1}$, $\varphi(g) = \overline{g}$. Так как $[g_{i+1}, g] \in G_i$, то $[\overline{g}_{i+1}, \overline{g}] \in \overline{G}_i$, и поэтому подгруппы $\overline{G}_i$ составят после удаления повторений центральный ряд группы $\overline{G}$.

б) Индукцией по ступени нильпотентности. Пусть $e \neq H \trianglelefteq G$, $Z_i = Z_i(G)$ и $H \not\subseteq Z_1 = Z(G)$. По индуктивному предположению, примененному к G/Z_1, пересечение $HZ_1 \cap Z_2$ содержит некоторый элемент $a \notin Z_1$. Так как $a = hz$, $h \in H$, $z \in Z_1$, то $h \in H \cap Z_2$, $h \notin Z_1$. Пусть элемент $g \in G$ таков, что $[h, g] \neq e$, тогда $[h, g] \in H \cap [Z_2, G] \subseteq H \cap Z_1$ и, значит, $H \cap Z_1 \neq e$.

в) Используйте 7.11.

7.14. Допустим, что $A \neq G$. Положим $A_i = AZ_i$, где $Z_i = Z_i(G)$, $i = 0, 1, \ldots$. Очевидно, $A_i \trianglelefteq A_{i+1}$. Пусть $A_m \subset G$, $A_{m+1} = G$. Так как фактор A_{m+1}/A_m коммутативен, то $G' \subseteq A_m$, значит, $AG' \subseteq A_m \subset G$. Противоречие. Утверждение о подгруппе Фраттини вытекает из ее описания как множества непорождающих элементов.

7.15. Обозначим $H = C_G(A)$, $Z_i = Z_i(G)$. Пусть уже доказано, что $H \cap Z_i \subseteq A$, и пусть $x \in H \cap Z_{i+1}$. Для всякого $g \in G$ имеем $[x, g] \in H \cap Z_i \subseteq A$, значит, $\langle x, A\rangle$ — коммутативная нормальная подгруппа. Поэтому $x \in A$, т.е. $H \cap Z_{i+1} \subseteq A$. Так как $\mathbb{Z}_n = G$ при некотором n, то $H = A$.

7.16. Индукцией по ступени нильпотентности. Пусть a, b — периодические элементы из G, и $A = \langle a, G'\rangle$, $B = \langle b, G'\rangle$. По индуктивному предположению $t(A)$ и $t(B)$ — подгруппы в A и B соответственно. Так как $t(A)$ — вполне инвариантная подгруппа в A, а A нормальна в G, то $t(A)$ нормальна в G. Аналогично, $t(B)$ нормальна в G. Любой элемент из $t(A) \cdot t(B)$ при возведении в подходящую степень попадает сначала в $t(B)$, а затем в e, поэтому группа $t(A) \cdot t(B)$ периодическая. В частности, элементы ab, a^{-1} периодические, что и требовалось доказать.

7.17. Индукцией по ступени нильпотентности. Будем считать, что G некоммутативна. Подгруппа $\langle a, G'\rangle$ нормальна в G и имеет меньшую ступень нильпотентности. Так как a, $a^b \in \langle a, G'\rangle$, то из $(a^b)^n = a^n$ следует $a^b = a$. Откуда $(ab^{-1})^n = e$ и, значит, $a = b$.

7.18. Из $(y^{-n}xy^n)^m = x^m$ получаем $y^{-n}xy^n = x$ и т.д.

7.22. а) Достаточно показать, что любая силовская подгруппа P группы $A = \Phi(G)$ нормальна в A или, что равносильно, в G, т.е. $N_G(P) = G$. Но это равносильно соотношению $G = A \cdot N_G(P)$. Докажем это равенство.

Пусть $g \in G$, подгруппа P^g снова является силовской в A, значит, P и P^g сопряжены некоторым элементом $a \in A$, т.е. $P^g = P^a$, откуда $ga^{-1} \in N_G(P)$, $g \in A \cdot N_G(P)$. Попутно доказано б).

7.36. По лемме Цорна всякий элемент из G лежит в некоторой максимальной локально нильпотентной подгруппе H. Достаточно показать, что H нормальна в G (поскольку произведение таких подгрупп есть локально нильпотентная подгруппа). Пусть $N = N_G(H)$. Если $N^g = N$, то H^g, H нормальны в N. Произведение H^gH локально нильпотентно, поэтому $H^gH = H$. Ввиду максимальности $H^g = H$ и, значит, $g \in N$. Таким образом, N совпадает со своим нормализатором. Следовательно, $N = G$.

7.37. По индуктивным соображениям можно считать, что любой периодический элемент g из G лежит во втором центре группы G. Если $g^m = e$, то $[g, x^m] = [g, x]^m = [g^m, x] = e$ для произвольного $x \in G$. Ввиду полноты G элемент x^m пробегает всю группу, следовательно, $g \in Z(G)$.

7.40. 2) Поскольку подгруппы полициклических групп снова полициклические, то они, в частности, конечно порождены. Отсюда следует достаточность. Докажем необходимость. Пусть G удовлетворяет условию максимальности и имеет разрешимый ряд, его факторы G_{i+1}/G_i тоже удовлетворяют условию максимальности, поэтому они конечно порождены и, значит, представимы в виде прямых произведений циклических групп. Это позволяет уплотнить данный ряд до полициклического ряда.

7.41. 1) Поскольку в группе произведение разрешимых нормальных подгрупп является разрешимой нормальной подгруппой, то в силу конечности группа G имеет единственную максимальную разрешимую нормальную подгруппу.

4) Пусть $x \in K$. Так как $x^{-1} = ex^{-1}e$, то достаточно показать, что $x^n \in K$ для любого $n \in \mathbb{N}$. Приведем доказательство, когда n четно. Для нечетного n доказательство аналогично. При $n = 2$ имеем $x^2 = xex \in K$. Предположим, что $x^k \in K$ для любого четного натурального $k < n$. По индукции $x^{n-2} \in K$. Значит, $x^{-(n-2)} \in K$. Тогда $x^n = x(x^{-(n-2)})^{-1}x \in K$.

8) $K = \{a^kb^sa^k \mid k, s \in \mathbb{Z}\}$ — скрученное подмножество, не являющееся подгруппой.

8. Автоморфизмы и эндоморфизмы

8.4. а) $\operatorname{Aut}\mathbb{Z}_5$ — циклическая группа порядка 4, состоящая из автоморфизмов возведения в степень $k = 1, 2, 3, 4$;

б) $\operatorname{Aut}\mathbb{Z}_6$ — группа второго порядка, в которую кроме тождественного автоморфизма входит автоморфизм возведения в пятую степень.

8.5. 3) $\operatorname{Aut}\mathbb{Z} \cong \mathbb{Z}_2 \cong \operatorname{Aut}\mathbb{Z}_3$.

4) Группа автоморфизмов мультипликативной группы положительных рациональных чисел имеет мощность континуума — любое взаимно однозначное отображение множества всех простых чисел на себя индуцирует некоторый автоморфизм этой группы.

8.22. $|G| \leqslant 2$.

8.28. Пусть $G = \mathrm{GL}(2, \mathbb{Q})$. Если a — матрица из группы G, то ее определитель может быть записан в виде $\frac{s}{t}2^{n(a)}$, где числа s и t нечетны, а $n(a)$ — целое число. Из свойств определителей вытекает равенство $n(ab) = n(a)+n(b)$. Нетрудно проверить, что отображение $f\colon a \mapsto \begin{pmatrix} 1 & n(a) \\ 0 & 1 \end{pmatrix}$ является эндоморфизмом группы G. Однако $f\colon \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, т.е. матрица из центра группы G переходит в матрицу, лежащую вне центра.

8.29. Пусть $\varphi \in Z(\operatorname{Aut}G)$ и $\varphi a = a' \neq a$ для $a \in G$. Тогда $a^{-1}\varphi ga = \varphi(a^{-1}ga) = a'^{-1}(\varphi g)a'$ для всякого $g \in G$. Так как φg вместе с g пробегает всю группу G, то элементы a и a' производят в группе G один и тот же внутренний автоморфизм. Это противоречит тому, что $Z(G) = e$.

8.33. а) $\operatorname{Aut}\mathbb{Z}_9 \cong \mathbb{Z}_6$, порождается автоморфизмом возведения в квадрат;

б) $\operatorname{Aut}\mathbb{Z}_8 \cong V_4$.

8.40. Пусть автоморфизмы α, $\beta \in \operatorname{Aut}A$ лежат в стабилизаторе S. Для $a \in A$ при некоторых b, $c \in B$ имеем $\alpha a = a+b$ и $\beta a = a+c$, откуда $\alpha\beta a = a+b+c$. Отображения $\overline{\alpha}\colon a+B \mapsto (\alpha-1)a = b$, $\overline{\beta}\colon a+B \mapsto (\beta-1)a = c$ являются такими гомоморфизмами из A/B в B, что $\overline{\alpha\beta}\colon a+B \mapsto b+c$. Значит, сопоставление $\alpha \mapsto \overline{\alpha}$ является мономорфизмом $S \to \operatorname{Hom}(A/B, B)$. При данном $\eta \in \operatorname{Hom}(A/B, B)$ отображение $\alpha\colon a \mapsto a + \eta(a+B)$ принадлежит S, поэтому $S \cong \operatorname{Hom}(A/B, B)$. Второе утверждение легко проверяется.

8.41. Всякий автоморфизм $\alpha \in \operatorname{Aut}A$ индуцирует некоторые автоморфизмы $\alpha_B \in \operatorname{Aut}B$ и $\alpha_C \in \operatorname{Aut}A/B = \operatorname{Aut}C$. Соответствие $\alpha \mapsto (\alpha_B, \alpha_C)$ является таким гомоморфизмом $\varphi\colon \operatorname{Aut}A \to \operatorname{Aut}B \times \operatorname{Aut}C$, что $\operatorname{Ker}\varphi = S$ и $S \cap \operatorname{Im}\varphi = 1$.

8.42. $\frac{1}{2}(1+\varepsilon)$ и $\frac{1}{2}(1-\varepsilon)$.

8.44. Используйте то, что группа $\operatorname{Aut}A$ содержит центральный автоморфизм порядка 2: $a \mapsto -a$, $a \in A$.

8.46. а) Если для $\eta \in \operatorname{End}A$ выполняется $\eta^2 = 0$, то эндоморфизмы $1+\eta$ и $1-\eta$ являются взаимно обратными, значит, принадлежат группе $\operatorname{Aut}A$. Но $(1+\eta)^n = 1+n\eta \neq 1$, так как аддитивная группа кольца $\operatorname{End}A$ — группа без кручения.

б) При любом $\beta \in \operatorname{End}A$ эндоморфизмы $\varphi = (1+\alpha)\beta(1-\alpha)$ и $\psi = (1-\alpha)\beta(1+\alpha)$ являются нильпотентными, значит, $\varphi = 0 = \psi$. Так как $2(\alpha\beta - \beta\alpha) = \varphi - \psi$, то $\alpha\beta = \beta\alpha$.

8.49. 1) Пусть $a \in A$ есть π'-автоморфизм группы P. Используя индукцию, можно считать, что $[a, P_1] = e$. Так как

$[a, P] \subseteq P_1$, то для $x \in P$ имеем $x^a = xy$, где $y \in P_1$. Тогда $x^{a^2} = xy^2$, ..., $x^{a^{o(a)}} = xy^{o(a)} = x$. Откуда $y = e$ и $[a, P] = e$. Следовательно, $a = 1$.

2) Группа A стабилизирует цепь $P \supseteq [P, A] \supseteq [P, A, A] = e$.

8.50. Покажем сначала, что свойство в) и характеристичность C в P вместе приводят к свойству г). Предположим для этого, что $[a, C] = e$, где a — заданный p'-автоморфизм. Тогда $[a, C, P] = e$ и $[C, P, a] \subseteq [C, a] = e$. Таким образом, $[P, a, C] = e$ и $[P, a] \subseteq C_P(C) = Z(C)$ по в). Откуда $[P, a, a] = e$ и по 8.49 2) $[P, a] = e$.

Докажем существование C. Если какая-либо подгруппа $A \in SCN(P)$ характеристична в P, то полагаем $A = C$. Ясно, что условия а), б), в) выполняются, поэтому можно предположить, что ни одна максимальная коммутативная подгруппа в P не характеристична. Пусть D — максимальная характеристическая коммутативная подгруппа в P. Пусть $C/D = \Omega_1(Z(P/D)) \cap C_P(D)/D$. Тогда $D \subset C$ и C — характеристическая подгруппа в P. Так как $D \subseteq Z(C)$ и $Z(C)$ — коммутативная характеристическая подгруппа в P, то из максимальности D следует $D = Z(C)$.

а) Так как C/D — элементарная коммутативная группа, то $C/Z(C)$ элементарна и $C' \subseteq D \subseteq Z(C)$. Откуда $cl\, C \leqslant 2$.

б) Поскольку $C/D \subseteq Z(P/D)$, то $[P, C] \subseteq D = Z(C)$.

в) Предположим, что $Q = C_P(C) \not\subseteq C$. Так как $Q \cap C = Z(C) = D$, то $Q/D \subset P/D$ и $Q/D \cap C/D = e$. Разумеется, $Q \subseteq C_P(C) \subseteq C_P(D)$. Если $Q \neq D$, то Q/D имеет с $\Omega_1(Z(P/D)) \cap C_P(D)/D$ нетривиальное пересечение. Противоречие.

8.51. в) Запишем P аддитивно. Покажем, что $C_P(A) \cap [P, A] = 0$. Пусть θ — эндоморфизм группы P, определенный равенством $\theta = \frac{1}{|A|} \sum\limits_{a \in A} a$. Ясно, что $b\theta = \theta\, b = \theta$ для всех $b \in A$. Таким образом, $\theta^2 = \theta$. Откуда $P = \theta\, P \oplus \operatorname{Ker} \theta$. Если $x \in C_P(A)$, то $\theta\, x = \frac{1}{|A|} \sum\limits_{a \in A} ax = x$. Значит, $C_P(A) \subseteq \theta\, P$. Наконец, если $[x, a] \in [P, A]$, то $\theta(-x + xa) = -\theta x + \theta x = 0$, так что $[x, a] \in \operatorname{Ker} \theta$. Таким образом, $C_P(A) \cap [P, A] = 0$. Теперь утверждение вытекает из того, что $P = [P, A]\, C_P(A)$.

8.54. См. [11, теорема 2.4] или [13].

9. Упорядоченные группы

9.13. 2) $(p_1q_1)(p_2q_2) = (p_1q_1p_2q_1^{-1})(q_1q_2) = p_3q_3$, где $p_3 \in P$, $q_3 \in Q$. Следовательно, PQ — подполугруппа. Далее, $e = e \cdot e \in PQ$. Из $pq = e$ следует $p = q^{-1} \in P \cap Q^{-1} = e$, т.е. $p = q = e$. Поэтому из $e = (p_1q_1)(p_2q_2) = p_3q_3$ следует, что $p_3 = q_3 = e$ и, так как подполугруппы P и Q обладают свойством в), $q_1 = q_2 = p_1 = q_1p_2q_1^{-1} = p_2 = e$. Наконец, для любого $x \in G$

$$x^{-1}(pq)x = (x^{-1}px)(x^{-1}qx) = p'q' \in PQ.$$

9.14. Необходимость. $a \in P$ или $a \in P^{-1}$, поэтому а) выполнено. Если $b, c \in P_a$, $b \neq e$, $c \neq e$, но $P_b \cap P_c = e$, то по п. 2) из 9.13 $P_bP_c^{-1}$ будет подполугруппой со свойствами б) – г) из 9.8. Частичная упорядоченность, определяемая этой подполугруппой, по условию может быть продолжена до линейной с подполугруппой положительных элементов P. Имеем $b, c^{-1} \in P$. Откуда $e \neq c \in P^{-1} \cap P_a$ и $e \neq b \in P \cap P_a$, но для любого $a \neq e$ или $P_a \subseteq P$, или $P_a \subseteq P^{-1}$. Это доказывает б).

Достаточность. Пусть P — подполугруппа со свойствами б) – г) из 9.8. Заметим, что если $P \cap P_a \neq e$, то $P \cap P_a^{-1} = e$. В самом деле, пусть $x \in P \cap P_a$, $x \neq e$, и $y \in P \cap P_a^{-1}$, $y \neq e$. Тогда $x^{-1} \in P_{a^{-1}}$, $y \in P_a^{-1} = P_{a^{-1}}$, а поэтому $P_{x^{-1}} \cap P_y \neq e$. Однако $x^{-1} \in P^{-1}$, $y \in P$, т.е. $P_{x^{-1}} \subseteq P^{-1}$, $P_y \subseteq P$, значит, $P^{-1} \cap P \neq e$, что противоречит б).

Возьмем в G любую подполугруппу P, определяющую максимальную упорядоченность. Если эта упорядоченность не линейная, то существует $a \in G$ такой, что $a \notin P$ и $a^{-1} \notin P$. В силу а) существует подполугруппа P_a, причем в виду вышедоказанного можно считать (заменяя, если нужно, a на a^{-1}), что $P \cap P_a^{-1} = e$. Поэтому по 2) из 9.13 PP_a будет подполугруппой, строго большей чем P, что противоречит выбору P.

9.15. Если $a \neq e$, то P_a состоит из всех степеней a^n, $n = 0, 1, \ldots$, поэтому а) из 9.14 выполнено. Выполняется и условие б), так как если $b = a^k$, $c = a^l$, $k \geqslant 1$, $l \geqslant 1$, то $e \neq a^{kl} \in P_b \cap P_c$.

9.28. Все указанные элементы должны принадлежать всякой выпуклой подгруппе, содержащей a. Пусть $e \leqslant x \leqslant a^k$, $e \leqslant y \leqslant a^l$ при некоторых натуральных k и l. Тогда $e \leqslant xy \leqslant a^{k+l}$, т.е. $xy \in A$. Так как $a^{-l} \leqslant y^{-1} \leqslant e$, то $a^{-l} \leqslant xy^{-1} \leqslant a^k$. Если $xy^{-1} \geqslant e$, то $xy^{-1} \in A$. Если же $xy^{-1} < e$, то $e \leqslant (xy^{-1})^{-1} \leqslant a^l$, т.е. $(xy^{-1})^{-1} \in A$, а тогда $xy^{-1} \in A$.

9.29. Так как $AP(G) = P(G)A$, то $AP(G)$ и $AP^{-1}(G)$ — подполугруппы в G, а тогда $AP(G) \cap AP^{-1}(G)$ — подполугруппа и, поскольку $AP(G) \cap AP^{-1}(G) = AP(G) \cap (AP(G))^{-1}$, то $AP(G) \cap AP^{-1}(G)$ есть подгруппа в G. Если $e < x < c$, где $c \in AP(G) \cap AP^{-1}(G)$, то $x = ex \in AP(G)$ и $x = c(x^{-1}c)^{-1} \in AP^{-1}(G)$, следовательно, $x \in AP(G) \cap AP^{-1}(G)$, откуда следует, что $AP(G) \cap AP^{-1}(G)$ выпукла. Если же $ax = by^{-1} \in AP(G) \cap AP^{-1}(G)$, где $a, b \in A$, то $a \leqslant ax = by^{-1} \leqslant b$, откуда $AP(G) \cap AP^{-1}(G) \subseteq H$.

9.35. Пусть для определенности $\varphi(a_1)$: $\varphi(a_2) < a_1 : a_2$. Тогда существует рациональное число $m : n$ такое, что $\varphi(a_1) : \varphi(a_2) < m : n < a_1 : a_2$, откуда получаем противоречивые неравенства $ma_2 < na_1$, $m\varphi(a_2) > n\varphi(a_1)$.

9.37. Пусть $G = \prod\limits_{i \in I} A_i$ — прямое произведение линейно упорядоченных групп, множество I вполне упорядочено. Проверьте, что лексикографический порядок в G: $a = (\ldots, a_i, \ldots) \in P(G)$, если $a_i \geqslant e$ в A_i и $a_j = e$ в A_j для всех $j < i$, будет линейным.

9.40. в) Пусть $H = \langle a, b \rangle$, $|a| > |b|$ и $B \subset A$ — скачок выпуклых подгрупп из H, определяемый элементом a. Из выпуклости A и $|a| > |b|$ следует $b \in A$ и, значит, $A = H$. Коммутативность A/B влечет $[a, b] \in B$, откуда по б) $||[a, b]|| << |a|$.

9.41. Пусть $G = \{a_1, \ldots, a_n\}$ и $|a_1| \geqslant |a_i|$, $i = 2, \ldots, n$. Тогда наибольшая выпуклая подгруппа, не содержащая a_1, ввиду б) – в) из 9.40 будет требуемой.

9.46. В силу 9.43 группу можно считать нильпотентной. Верхний центральный ряд группы в этом случае удовлетворяет условиям 9.44.

9.47. В свободной группе F возьмем систему Σ из членов нижнего центрального ряда и их пересечения, равного, как известно, единичной подгруппе. Система Σ удовлетворяет условиям 9.44, так как факторгруппы F_n/F_{n+1} являются коммутативными группами без кручения.

9.48. Пусть G — линейно упорядоченная группа, она изоморфна факторгруппе F/H некоторой свободной группы F. Введем в F/H такой порядок, чтобы F/H была у-изоморфна G, а H линейно F-упорядочим (это можно сделать по 9.47). Осталось применить 9.45.

9.50. Если H содержит выпуклую подгруппу N, то H открыта, так как $N = \bigcup\limits_{x\in N}(x^{-1}, x)$ открыта. Если H открыта, то H есть объединение открытых интервалов (a, b). Предположим, что $a^{-1}b$ лежит в скачке выпуклых подгрупп $N_1 \supset N_2$, $N_2 \neq e$. Тогда вместе с a в H лежат элементы ax, где $x \in N_2$, $x > e$ и, следовательно, $N_2 \subset H$. Если же H открыта и всякий интервал (a, b) таков, что $a^{-1}b$ лежит в наименьшей выпуклой подгруппе N, то $N \cap H \neq e$. Покажем, что в этом случае $N \subseteq H$. Пусть $h \in N$. Так как $N \cap H \neq e$ и подгруппа $N \cap H$ открыта в G, то найдется окрестность единицы $(x, y) \subset N \cap H$; пусть $c \in (x, y)$, $c \neq e$. Так как N — наименьшая выпуклая подгруппа в G, то она архимедова, и поэтому найдется такое n, что $c^n < h < c^{n+1}$. Тогда $e < c^{-n}h < c$, откуда следует $c^{-n}h \in (x, y)$, т.е. $c^{-n}h \in H$ и $h \in H$. Итак, $N \subseteq H$.

9.51. Если группа G связна, то она архимедова ввиду 9.50 и теоремы Гельдера. Но архимедова группа связна лишь в том случае, если изоморфна аддитивной группе вещественных чисел с естественным порядком.

9.52. Если группа G содержит наименьшую выпуклую подгруппу H, изоморфную группе вещественных чисел, то G локально компактна.

Обратно, пусть G локально компактна. Тогда найдется окрестность единицы (a, b) с компактным замыканием $\overline{(a, b)} = \{x \,|\, a \leqslant x \leqslant b\}$, $\overline{(a, b)}$ не может содержать выпуклой подгруппы. Поэтому в G имеется наименьшая выпуклая подгруппа H, $a, b \in H$. Если H не изоморфна группе вещественных чисел, то не связна по 9.51, тогда она не полна по Дедекинду и поэтому не локально компактна.

9.53. Если бы порядково полная группа G была не архимедовой, то в G имелась бы выпуклая подгруппа H. Тогда множество всех таких элементов $x \in G$, что $x \leqslant h$ для некоторого $h \in H$, было бы ограниченным сверху, но не имеющим верхней грани. Обратное утверждение очевидно.

9.54. См. [19, глава VII, § 4, теорема 1].

10. Действия групп на множествах. Представления групп

10.5. а) Две орбиты: одна состоит только из одного нулевого вектора, другая — из всех ненулевых векторов.

б) Каждая орбита состоит из всех векторов одинаковой длины.

в) Каждому подмножеству $I \subseteq \{1, \ldots, n\}$ отвечает орбита O_I, состоящая из тех векторов x, у которых координата x_i равна 0 в точности тогда, когда $i \in I$. Всего 2^n различных орбит.

г) Всего $n+1$ различных орбит $O, O_1, \ldots, O_n$, где O состоит из нулевого вектора, а O_i — из всех таких векторов $x = \sum\limits_{t=1}^{n} x_t e_t$, для которых $x_i \neq 0$ и $x_j = 0$ для всех $j > i$.

10.6. 1) Орбита группы G равна X.

2) G_U состоит из всех матриц вида $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, где A — обратимая матрица порядка k, C — обратимая матрица порядка $n-k$ и B — матрица размера $k \times (n-k)$.

10.7. а) Центр $Z(G)$ группы G;

б) орбитой служит класс сопряженных элементов x^G, содержащий x, стационарной подгруппой — централизатор $C_G(x)$.

10.9. Ker $L^H = \bigcap\limits_{g\in G} g^{-1}Hg$ — наибольшая нормальная подгруппа группы G, содержащаяся в H.

10.14. а) Имеем $\sum\limits_{g\in G} N(g) = \sum\limits_{j=1}^{n} \Gamma(j)$ ($\Gamma(j)$ — число элементов в G, оставляющих на месте символ j). Другими словами, $\Gamma(j) = |G_j|$, где $G_j = St\,(j)$. В силу транзитивности $|G_j| = |g_j G_1 g_j^{-1}| = |G_1|$ ($j = g_j(1)$). Стало быть, $\sum\limits_{g\in G} N(g) = \sum\limits_{j=1}^{n} |G_j| = \sum\limits_{j=1}^{n} |G_1| = n|G_1| = |G|$.

б) Условие 2-транзитивности означает, что на множестве $\Omega_1 = \Omega \setminus \{1\}$ стационарная подгруппа G_1 действует транзитивно, т.е. G_1-орбитами будут $\{1\}$ и Ω_1. Пусть $N'(x)$ — число точек в Ω_1, неподвижных при действии $x \in G_1$. Имеем $\sum\limits_{x\in G_1} N'(x) = |G_1|$. Так как $N(x) = 1 + N'(x)$, то $\sum\limits_{x\in G_1} N(x) = 2\,|G_1|$. Такие же соотношения справедливы для других G_j: $\sum\limits_{x\in G_j} N(x) = 2\,|G_j| = 2|G_1|$. Тогда $\sum\limits_{j=1}^{n} \sum\limits_{x\in G_j} N(x) = 2\,n|G_1| = 2|G|$ ($N(x)$ считается по одному для каждой подгруппы G_j, в которой содержится x). Но x оставляет на месте $N(x)$ точек, следовательно, содержится ровно в $N(x)$ подгруппах G_j. Это означает, что каждый элемент x вносит в сумму слагаемое $N(x)^2$. С другой стороны, любой элемент $y \in G$, не содержащийся в $\bigcup\limits_j G_j$, переставляет все точки, так что $N(y) = 0$. Откуда $\sum\limits_{g\in G} N(g)^2 = \sum\limits_{j=1}^{n} \sum\limits_{x\in G_j} N(x) = 2\,|G|$.

10.15. г) Пусть $x \in \Omega$. Так как G действует 2-транзитивно на Ω, то G_x транзитивна на $\Omega \setminus \{x\}$. Поэтому для любых $e \neq h_1, h_2 \in H$ существует такой $g \in G_x$, что $g(h_1 x) = h_2 x$. Откуда $gh_1 g^{-1} x = h_2 x$. Так как H регулярна на Ω, то

$gh_1g^{-1} = h_2$. В частности, все неединичные элементы из H имеют одинаковый порядок. В частности, H — p-группа. В силу регулярности $|\Omega| = |H|$.

10.20. По условию Ω есть объединение $t = r(G:\Omega)$ орбит $G(x_1), \ldots, G(x_t)$. Пусть $M = \{(x, g) \,|\, x \in \Omega,\, g \in G \text{ и } gx = x\}$. Тогда

$$\sum_{g\in G} |\operatorname{Fix}(g)| = |M| = \sum_{x\in\Omega} |G_x| = \sum_{x\in\Omega} \frac{|G|}{|G(x)|} = \sum_{i=1}^{t} |G(x_i)| \frac{|G|}{|G(x_i)|} = t|G|.$$

10.31. $V = \left\langle \sum\limits_{i\in\Omega} e_i \right\rangle \oplus \left\{ \sum\limits_{\lambda_1+\ldots+\lambda_n=0} \lambda_i e_i \,|\, \lambda_i \in P \right\}$ — разложение в прямую сумму одномерного и $(n-1)$-мерного инвариантных подпространств.

10.32. 1) Если $\Phi\colon G \to P^*$, то $G' \subseteq \operatorname{Ker}\Phi$.

2) Если $G = \mathbb{Z}_4$ и $P = \mathbb{Z}_{11}$, то $2\mathbb{Z}_4 \subseteq \operatorname{Ker}\Phi$.

3) $G \cong \mathbb{Z}$. Представление $k \mapsto \lambda^k$ при $1 \neq |\lambda| \in \mathbb{C}$ точно. Если $|\lambda| = 1$, то $\lambda = e^{2\pi i\theta}$, $\theta \in \mathbb{R}$, и ядро отображения $k \mapsto e^{2\pi i\theta k}$ отлично от нуля только при $\theta \in \mathbb{Q}$. $G = \langle a \,|\, a^n = e\rangle$. Пусть $\varepsilon = exp(2\pi\, i/n)$ — примитивный корень степени n из 1. Из n одномерных представлений $\Phi^{(m)}\colon a^k \mapsto \varepsilon^{mk}$, $m = 0, 1, \ldots, n-1$, точными будут $\varphi(n)$.

4) Рассмотрите отображение $k \mapsto J_{m,\,1}^k = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ 0 & 0 & 0 & \ldots & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}^k$ и используйте теорему о жордановой нормальной форме матрицы.

5) Нужно убедиться лишь в том, что у конечной циклической группы нет неприводимых над $\mathbb{C}$ представлений размерности > 1. Для этого заметим, что любой линейный оператор конечного порядка диагонализируем над $\mathbb{C}$. Действительно, матрица A этого оператора приводится к жордановой нормальной форме $J(A)$ — прямой сумме жордановых клеток $J_{m,\,\lambda}$. Если $A^q = E$, то $J_{m,\,\lambda}^q = E$, а это возможно только тогда, когда $m = 1$ и λ — корень степени q из 1, т.е. $J(A)$ — диагональная матрица. В данном случае это равносильно полной приводимости представления Φ. Если $\dim\Phi = r$, то Φ распадается в прямую сумму r одномерных представлений.

6) следует из 5).

10.33. Над $\mathbb{R}$ представление неприводимо, поскольку характеристический многочлен $\lambda^3 + \lambda + 1$ этой матрицы не имеет вещественных корней. Если V рассматривать над $\mathbb{C}$, то V представимо в виде прямой суммы одномерных G-подпространств

$$V = \langle v_1 + \varepsilon^{-1}v_2\rangle \oplus \langle v_1 + \varepsilon v_2\rangle, \quad C\Phi_a C^{-1} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix},$$
$$\varepsilon = \frac{-1+\sqrt{-3}}{2}, \quad C = \begin{pmatrix} 1 & -\varepsilon^{-1} \\ 1 & -\varepsilon \end{pmatrix}.$$

10.34. В обоих случаях $U = \langle e_1\rangle$ — инвариантное подпространство. Если бы для Φ существовало инвариантное подпространство, дополнительное к U, то в подходящем базисе оно было бы представлено матрицей $\begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix}$, т.е. было бы единичным, что не соответствует действительности. Второе представление приводимо, и в базисе $\{e_1,\, e_1 - e_2\}$ имеет матрицу $\begin{pmatrix} e^t\,0 \\ 0\;1 \end{pmatrix}$.

10.37. Пусть $V_0 = \operatorname{Ker}\sigma \subset V$. Тогда $\Phi(g)V_0 \subseteq V_0$. Ввиду неприводимости $V_0 = 0$, следовательно, $\operatorname{Ker}\sigma = 0$. Аналогичным образом показывается, что $\operatorname{Im}\sigma = W$, т.е. справедливо а). Пусть λ — одно из собственных значений оператора σ, и $\sigma_0 = \sigma - \lambda I$. Так как $\Psi(g)\,\sigma_0 = \sigma_0\,\Phi(g)$ и $\operatorname{Ker}\sigma_0 \neq 0$, то $\sigma_0 = 0$ и $\sigma = \lambda I$.

10.38. 4) Равенство $g^m = e$ влечет $\Phi(g)^m = I$, и если $\lambda_1, \ldots, \lambda_n$ — характеристические корни оператора $\Phi(g)$, то $\lambda_1^k, \ldots, \lambda_n^k$ — характеристические корни оператора $\Phi(g)^k$. В частности, $\lambda_i^m = 1$ и, значит, $|\lambda_i| = 1$, $\overline{\lambda}_i = \lambda_i^{-1}$. Откуда $\chi_\Phi(g^{-1}) = \operatorname{tr}\Phi(g^{-1}) = \sum\limits_i \lambda_i^{-1} = \sum\limits_i \overline{\lambda}_i = \overline{\sum\limits_i \lambda_i} = \overline{\chi_\Phi(g)}$.

10.39. а) Имеем $\chi_V = \chi_{V_1} + \ldots + \chi_{V_k}$. Откуда $(\chi_V,\, \chi_W)_G = (\chi_{V_1},\, \chi_W)_G + \ldots + (\chi_{V_k},\, \chi_W)_G$. Справа стоит сумма из нулей и единиц, причем число единиц совпадает с числом G-подпространств V_i, изоморфных W. Теперь справедливость утверждения вытекает из независимости скалярного произведения от разложения V.

б) Два G-пространства V, V' с одним и тем же характером $\chi = \chi_V = \chi_{V'}$ содержат в своих разложениях слагаемое, изоморфное данному неприводимому G-пространству W, одинаковое число раз, а именно $(\chi,\, \chi_W)_G$. Поэтому в разложениях $V = \bigoplus\limits_{i=1}^{k} V_i$, $V' = \bigoplus\limits_{j=1}^{l} V_j'$ на неприводимые прямые слагаемые можно считать $l = k$, $V_i \cong V_i'$. Значит, изоморфны и сами V, V'.

в) Из доказанного следует, что $\chi_\Phi = \sum\limits_{i=1}^{s} m_i\chi_i$, где m_i — кратность, с которой неприводимое представление (Φ_i, V_i) входит в разложение (Φ, V). Из соотношения ортогональности вытекает, что $(\chi_\Phi,\, \chi_\Phi)_G = \sum\limits_{i=1}^{s} m_i^2$.

10.40. Считаем, что G — матричная группа: $G \subset \mathrm{GL}(n, \mathbb{C})$, где n — степень представления. Пусть $C(G)$ — централизатор группы G в $M(n, \mathbb{C})$. Тогда $C(G)$ — подкольцо, содержащее $Z(G)$. По лемме Шура каждая матрица в $C(G)$, отличная от

нулевой, невырожденная, т.е. $C(G)$ — тело. Его центр K является полем и $Z(G) \subseteq K$, значит, $Z(G)$ — конечная подгруппа мультипликативной группы поля. Как известно, такая подгруппа всегда циклическая.

10.41. Пусть R_h — матрица линейного оператора $\rho(h)$ в данном базисе $\{e_g \,|\, g \in G\}$. Так как $\rho(h)e_g = e_{hg}$, то $\mathrm{tr}R_h = 0$ при $h \neq e$, значит, $\chi_\rho(h) = 0$ и $\chi_\rho(e) = |G|$. Пусть теперь (Φ, V) — неприводимое представление группы G. Кратность вхождения Φ в ρ равна скалярному произведению $(\chi_\rho, \chi_\Phi)_G$. Имеем (1): $(\chi_\rho, \chi_\Phi)_G = \frac{1}{|G|}\sum\limits_{h\in G}\chi_\rho(h)\overline{\chi_\Phi(h)} = \frac{1}{|G|}\chi_\rho(e)\overline{\chi_\Phi(e)} = \frac{1}{|G|}|G|\chi_\Phi(e) = \dim V$. Если r — число классов сопряженности группы G, то имеется r попарно неэквивалентных неприводимых представлений $\Phi^{(1)}, \ldots, \Phi^{(r)}$, которым соответствуют характеры $\chi_1, \ldots, \chi_r$ степеней $n_1, \ldots, n_r, n_i = \chi_i(e)$. Соотношение (1) показывает, что $\rho = n_1\Phi^{(1)}\oplus\ldots\oplus n_r\Phi^{(r)}$. Откуда $\chi_\rho = n_1\chi_1+\ldots+n_r\chi_r$. В частности, $|G| = \chi_\rho(e) = n_1\chi_1(e)+\ldots+n_r\chi_r(e) = n_1^2+\ldots+n_r^2$.

10.42. Число r классов сопряженности коммутативной группы A совпадает с ее порядком, откуда вытекают первые два утверждения. Если все неприводимые представления имеют степень 1, то согласно 10.41 $r = |A|$, это равносильно коммутативности группы.

10.43. Группа A допускает разложение $A = A_1 \times \ldots \times A_k$ в прямое произведение циклических групп $A_i = \langle a_i\rangle$. Если $|A_i| = s_i$ и ε_i — примитивный корень s_i-й степени из 1, то каждому элементу $a = a_1^{t_1}\ldots a_k^{t_k}$ из A отвечает характер $\chi_a \in \widehat{A}$, определенный соотношением $\chi_a(a_1^{r_1}\ldots a_k^{r_k}) = \varepsilon_1^{r_1t_1}\ldots\varepsilon_k^{r_kt_k}$. Очевидно, что $\chi_a\chi_b = \chi_{ab}$. Если $a = a_1^{t_1}\ldots a_k^{t_k} \neq a_1^{l_1}\ldots a_k^{l_k} = b$, то существует индекс i с $t_i \neq l_i$. Тогда $\chi_a(a_i) = \varepsilon_i^{t_i} \neq \varepsilon_i^{l_i} = \chi_b(a_i)$. Следовательно, все характеры χ_a попарно различны и отображение $a \mapsto \chi_a$ устанавливает требуемый изоморфизм A и $\widehat{A}$.

10.44.

V_4	e	a	b	ab
χ_1	1	1	1	1
χ_2	1	−1	1	−1
χ_3	1	1	−1	−1
χ_4	1	−1	−1	1

10.45. Для доказательства последнего утверждения рассмотрите таблицу характеров группы S_3.

10.47. Значение $\chi_\Phi(g)$ совпадает с числом $N(g)$ базисных векторов e_i, остающихся неподвижными при действии g. По свойствам 2-транзитивных групп $\sum\limits_{g\in G}\chi_\Phi(g)\overline{\chi_\Phi(g)} = \sum\limits_{g\in G}\chi_\Phi(g)^2 = \sum\limits_{g\in G}N(g)^2 = 2|G|$, что переписывается в виде $(\chi_\Phi, \chi_\Phi)_G = 2$. Поэтому Φ — прямая сумма двух неприводимых представлений ($2 = 1+1$ — единственная запись 2 в виде суммы квадратов натуральных чисел). Имеем $\Phi = \Phi^{(1)}\oplus\Psi$, где $(\Phi^{(1)}, U)$ — единичное представление, а Ψ — $(n-1)$-мерное представление, действующее на пространстве $W = \langle e_1 - e_n, \ldots, e_{n-1} - e_n\rangle$. Если бы разложение $V = U \oplus W$ можно было продолжить за счет разложения W, то неприводимых слагаемых получилось бы больше двух.

В частности, каждая из групп S_n, $n > 2$; A_n, $n > 3$, обладает неприводимым представлением Ψ над $\mathbb{C}$ степени $n-1$ с характером χ_Ψ, вычисляемым по формуле $\chi_\Psi(g) = N(g) - 1$.

10.50. Заметить, что группы порядков p и p^2 коммутативны.

10.51. p^2 одномерных представлений и $p-1$ p-мерных. Заметить, что центр данной группы имеет порядок p и число классов сопряженных элементов равно $p^2 + p - 1$. Так как факторгруппа по центру коммутативна, то коммутант данной группы имеет порядок p. Этим определяется число одномерных представлений. Заметить еще, что в данной группе есть нормальная подгруппа индекса p и доказать, что размерность неприводимого представления не может быть больше p.

10.52. Группа A_4 имеет четыре класса сопряженных элементов. Представители классов и их мощности указаны в двух верхних строках таблицы

12	1	3	4	4
A_4	e	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ε	ε^{-1}
χ_3	1	1	ε^{-1}	ε
χ_4	3	−1	0	0

Коммутант $A_4' = V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ имеет индекс 3 в A_4. Поэтому A_4 обладает тремя одномерными представлениями: $\Phi^{(1)} = \chi_1$, $\Phi^{(2)} = \chi_2$, $\Phi^{(3)} = \chi_3$ (с ядром A_4' и с $\varepsilon^3 = 1$, $\varepsilon \neq 1$), и одним трехмерным представлением $\Phi^{(4)}$ ($12 = 1^2 + 1^2 + 1^2 + 3^2$).

24	1	3	6	8	6
S_4	e	(12)(34)	(12)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	1	−1	1	−1
χ_3	2	2	0	−1	0
χ_4	3	−1	−1	0	1
χ_5	3	−1	1	0	−1

8	1	1	2	2	2
Q_8	e	a^2	a	b	ab
χ_1	1	1	1	1	1
χ_2	1	1	−1	−1	1
χ_3	1	1	−1	1	−1
χ_4	1	1	1	−1	−1
χ_5	2	−2	0	0	0

Z_n	e	g	g^2	...	g^{n-1}
χ_1	1	1	1	...	1
χ_2	1	z	z^2	...	z^{n-1}
χ_3	1	z^2	z^4	...	$z^{2(n-1)}$
...	...	...	...	...	...
χ_n	1	z^{n-1}	$z^{2(n-1)}$	...	$z^{(n-1)(n-1)}$

где $z = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$.

11. Общие свойства колец

11.1. а) Имеем равенства $0 = (x+y) + (-(x+y))$ и $0 = (x+y) + (-(y+x))$. Откуда $-(x+y) = -(y+x)$ и $x+y = y+x$.

б) Пусть R — некоммутативная группа. Назовем операцию в R «сложением», а «произведение» любых двух элементов из R положим равным единичному элементу группы — «нулю».

в) Можно взять множество $\mathbb{N}$ с обычными операциями сложения и умножения.

11.5. 1) 4; 2) 2; 3) 6.

11.8. 2) Если $rs = 1$, то $(sr-1)\,s = 0$.

11.25. 1) Воспользуйтесь тем, что сумма и разность двух нильпотентных элементов будет нильпотентным элементом.

2) Возьмем кольцо $R = \prod_{k=1}^{\infty} \mathbb{Z}_{p^k}$ — прямое произведение (см. § 12) колец вычетов $\mathbb{Z}_p, \mathbb{Z}_{p^2}, \mathbb{Z}_{p^3}, \ldots$, а в нем элементы $a_1 = (\overline{p}, 0, 0, \ldots)$, $a_2 = (0, \overline{p}, 0, \ldots)$, $a_3 = (0, 0, \overline{p}, \ldots)$, ... Искомым рядом будет $\sum_{n=1}^{\infty} a_n x^n \in R\,[[x]]$.

11.31. г) Если $(1+ab)\,u = 1$, то $1 - abu = u$. Откуда $(1+ba)\,(1-bua) = 1 - bua + b\,(1-abu)\,a = 1$ и так как $u\,(1+ab) = 1$, то $(1-bua)\,(1+ba) = 1 + ba - bu\,(1+ab)\,a = 1$.

д) Если $a^n = 0$ $\left(a^{n-1} \neq 0\right)$, то $(1+a)\left(1 - a + a^2 - \ldots + (-1)^{n-1} a^{n-1}\right) = 1$.

11.32. Пусть $0 \neq x$ — необратимый элемент. Если $|xR| < \infty$, то R содержит бесконечное число делителей нуля (которые необратимы), в противном случае используйте предыдущее упражнение.

11.34. ($\Rightarrow$). $b = a\,(a-1)^{-1}$. ($\Leftarrow$). Для $1-a$ найдется $c \in R$ со свойствами $(1-a)+c = (1-a)\,c = c\,(1-a)$, $1 - a + c = c - ac = c - ca$. Откуда $a\,(1-c) = (1-c)\,a = 1$.

11.39. Покажите, что если $a = a \cdot e$, то e — единица.

11.40. а) Отображение $x \mapsto ax$ ($a \in R, a \neq 0$) — биекция, поэтому $ax = a$ при некотором $x \in R$; любой $b \in R$ представим в виде $b = ya$, и тогда $bx = b$, т.е. x — правая единица. Аналогично, существует и левая единица (совпадающая с правой). Итак, $1 \in R$. Отсюда $av = 1$ и $ua = 1$, $u, v \in R$, и, значит, a обратим.

б) Элемент a, обратимый справа, не является правым делителем нуля, и поэтому $x \mapsto xa$ — биекция.

в) Если $ab = 0$ ($b \neq 0$), но a не является правым делителем нуля, то $1 = xa$. Откуда $b = xab = 0$.

г) Вытекает из предыдущего.

д) Используйте следствие теоремы Лагранжа о том, что порядок элемента делит порядок группы.

11.41. 4.

11.42. 1) $0 = (a+b)^2 = a^2 + ab + ba + b^2 = ab + ba$.

2) Тождество а) доказывается методом математической индукции относительно числа m. При $m = 1$ равенство $[x^m, y] = mx^{m-1}[x, y]$ верно. Пусть $[x^m, y] = mx^{m-1}[x, y]$. Тогда $[x^{m+1}, y] = x^m[x, y] + [x^m, y]x = x^m[x, y] + mx^{m-1}[x, y]x = (m+1)x^m[x, y]$.

Так как

$$[x^n y^m, x^s y^t] = x^n[y^m, x^s]y^t + x^s[x^n, y^t]y^m = smx^{n+s-1}[y, x]y^{m+t-1} + ntx^{s+n-1}y^{t+m-1}[x, y] = (nt - ms)x^{n+s-1}y^{m+t-1}[x, y],$$

то б) доказано.

Тождество в) следует из тождества б) при $m = n$, $t = s$.

3) Импликации а) $\Rightarrow$ б), в), д) очевидны. Эквивалентность а) и г) вытекает из свойства $[a, b, c] = [ab, c] - [ba, c]$. б) $\Rightarrow$ а). Имеем $[[b, c], a] = bca - cba - abc + acb$, $[b, [c, a]] = bca - bac - cab + acb$. Приравнивая правые части, получаем $0 = cba + abc - bac - cab = [[a, b], c]$. Откуда $[a, b] \in Z(R)$. в) $\Rightarrow$ а). Как и выше, из равенства $[c, a, b] = [c, b, a]$ получаем $cab - cba + bac - abc = 0$ или $c[a, b] = [a, b]c$, т.е. $[a, b] \in Z(R)$. При $c = 1$ из д) получаем $[[a, b], d] = 0$, т.е. д) $\Rightarrow$ а).

11.46. 1) $\delta = 0$; б) $\delta = f\,(x)\,d$, где d — обычное дифференцирование, $f(x) \in \mathbb{Z}\,[x]$; в) $\delta = \sum f_i d_i$, где $f_i \in \mathbb{Z}\,[x_1, \ldots, x_n]$, d_i — частные дифференцирования по переменным.

11.47. 1) Для $a, b \in R$ имеем $(a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$ и $ab+ba=0$. Если $b=a$, то $a=-a$. Откуда $2a=0$ и $ab=-ba=ba$. 2) $(a-1)\,a=0$. Поэтому $a^2=a$.

11.50. $U(\mathbb{Z}_4)$ и $U(\mathbb{Z}_6)$ — да, $U(\mathbb{Z}_8)$ — нет.

12. Факторгруппы и гомоморфизмы

12.7. Положим $T=(R,\mathbb{Z})$, где $(a,n)+(b,m)=(a+b,n+m)$ и $(a,n)(b,m)=(ab+ma+nb,nm)$. Тогда T — кольцо с единицей $(0,1)$. Отображение $r\mapsto(r,0)$ будет вложением кольца R в кольцо T (умножение целого числа на элемент кольца определено в 11.9).

12.13. Если $0\neq a\in R$, то $0\neq aR=R$ $(1\in R)$. Поэтому a обратим. Кольцо с нулевым умножением, аддитивная группа которого имеет простой порядок, не имеет нетривиальных идеалов, но полем не является.

12.14. 1) Для каждого $0\neq a\in R$ левый идеал $Ra\neq 0$. Поэтому $Ra=R$. Аналогично, $aR=R$. Следовательно, R — тело (см. 11.7). 2) $Ra\supseteq Ra^2\supseteq\dots$ $(0\neq a\in R)$. Поэтому $Ra^n=Ra^{n+1}$ для некоторого n. Откуда $ba^{n+1}=a^n$ и, значит, $ba=1$. Теперь достаточно применить 11.8 2).

12.18. Если $ab=cd=0$ $(b,d\neq 0)$, то $(ra)\,b=0$ для всех $r\in R$. Так как $bR\cap dR\neq 0$, то $bx=dy\neq 0$ для некоторых $x,y\in R$. Откуда $(a-c)\,bx=0$, т.е. $a-c$ — делитель нуля.

12.22. б) Если $A_1=r\,(B_1)$, $A_2=r\,(B_2)$, то (см. 12.20) $A_1\cap A_2=r\,(B_1+B_2)\in M$.

в) Множество $L=\{A\in M\,|\,A\supseteq A_1,A_2\}$ не пусто, что позволяет записать $C=\bigcap_{A\in L}A=\bigcap_{r(B)\in L}r(B)=r(\sum_{r(B)\in L}B)\in L$. Ясно, что C является точной верхней гранью для A_1,A_2.

12.25. $R=M(2,\mathbb{Z})$, $a=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $b=\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $a^2=b^2=0$, $(a+b)^2=e$ — единичная матрица.

12.31. 3) Если $R=eR\oplus(1-e)R$, где $e^2=e\in R$, то $\ell\,(eR)=R\,(1-e)$.

12.35. Сумма левых идеалов порождается суммой соответствующих идемпотентов.

12.40. Пусть $R\subseteq S\subseteq Q$ и I — идеал в S. Покажите, что $I=aS$, где a порождает идеал кольца R, состоящий из числителей всех элементов из I.

12.49. Рассмотрите отображения: а) $f(x)\mapsto(f\,(1),f\,(-1))$; б) $\overline{a+bx}\mapsto a+b\sqrt{3}$, где $a+bx$ — остаток от деления многочлена $f(x)\in\mathbb{Q}[x]$ на x^2-3, $f(x)+\left(x^2-3\right)=\overline{a+bx}\in\mathbb{Q}[x]/\left(x^2-3\right)$.

12.68. Над $\mathbb{R}$. а) $\mathbb{R}\oplus\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}\,[x]\,/\left(x^2\right)$. б) Кроме алгебр в а), $\mathbb{R}e\oplus\mathbb{R}e$, где $e^2=0$; $\mathbb{R}e\oplus\mathbb{R}f$, где $e^2=0$, $f^2=f$; $\mathbb{R}e\oplus\mathbb{R}f$, где $e^2=ef=fe=0$, $f^2=e$.

Над $\mathbb{C}$. а) $\mathbb{C}\oplus\mathbb{C}$, $\mathbb{C}\,[x]\,/\left(x^2\right)$. б) Кроме алгебр в а), $\mathbb{C}e\oplus\mathbb{C}e$, где $e^2=0$; $\mathbb{C}e\oplus\mathbb{C}f$, где $e^2=0$, $f^2=f$; $\mathbb{C}e\oplus\mathbb{C}f$, где $e^2=ef=fe=0$, $f^2=e$.

12.77. Если $f(a)=0$, причем коэффициенты многочлена $f(x)$ содержатся в центре кольца K, то $f\left(v^{-1}av\right)=0$ для $v\in U(K)$; см. также 12.72.

13. Специальные идеалы

13.3. Если (x) прост и $(x)\subset(y)$, то $x=yz\in(x)$. Откуда $z\in(x)$, $z=tx$. Тогда $x=yz=ytx$, значит, $yt=1$ и $(y)=(1)$.

13.4. Множество всех собственных (правых) идеалов кольца, содержащих данный идеал, удовлетворяет условиям леммы Цорна и, следовательно, содержит максимальный элемент.

13.7. Пусть $I^2\neq 0$, т.е. $xI\neq 0$ для некоторого $x\in I$. Откуда $xI=I$ и найдется $e\in I$ с $xe=x$, $xe^2=xe$, $x\left(e^2-e\right)=0$. Правый идеал $J=\{y\in I\,|\,xy=0\}\neq I$, значит, $J=0$ и $e^2-e=0$, $e^2=e$. Для идемпотента e будет $0\neq eR\subseteq I$ и $eR=I$.

13.8. Воспользоваться 13.7.

13.9. $I+rR=R$ для $r\in R\backslash I$, что эквивалентно максимальности I.

13.14. См. 13.11.

13.15. 1) Допустим, что $xy\in P$, но $x,y\notin P$. В таком случае $(P+xR)\cap T\neq\varnothing$ и $(P+yR)\cap T\neq\varnothing$. Получаем $a+xr=c$, $b+ys=d$, где $a,b\in P$, $r,s\in R$, $c,d\in T$, что невозможно.

3) Пусть ненильпотентный элемент $x\in R$ лежит во всяком простом идеале кольца R, и пусть $T=\{1,x,x^2,\dots\}$. Для идеалов, не пересекающихся с T, справедлива лемма Цорна. Таким образом, существует максимальный идеал P с таким свойством. Согласно 1) P — простой, однако $x\notin P$.

13.38. а) $n\mathbb{Z}$; б) $f(x)P[x]$.

13.39. Для $0\neq a\in K$ рассмотрите идеал $I=(a,x)$ области главных идеалов $K[x]$. Поскольку $a\in I$, то $I=(f)$ для некоторой константы f, а так как $x\in I$, то f — обратимый элемент кольца K, т.е. $I=K[x]$. Поэтому $1=u(x)x+v(x)a$. Откуда $1=v\,(0)\,a$.

13.52. $a\in M$.

13.53. Обозначим через $J(R)$ пересечение всех максимальных правых идеалов. Включение $a\in J(R)$ равносильно тому, что для всех максимальных правых идеалов M следует, что $1\notin aR+M$, последнее справедливо в точности тогда, когда $1-ax\notin M$ при всех $x\in R$, т.е. $1-ax$ — обратимый справа элемент.

13.54. Положим $t=1+rsa$. Тогда $(1-ra)\,(1+rsa)=1+rsa-r\,(1+ars)\,a=1$.

13.56. Нужно лишь показать, что $J(R)$ — левый идеал, т.е. если $a \in J(R)$, то для всех $r, s \in R$ элемент $1 - ras$ обратим справа. Поскольку $as \in J(R)$, то достаточно показать, что $1 - ra$ обратим справа, а это следует из 13.55.

13.58. Для произвольного $a \in J(R)$ найдем $u \in R$ такое, что $(1-a)u = 1$, т.е. $-au = 1 - u$. Отсюда $1 - u \in J(R)$ и $1 - (1-u)$ — обратимый справа элемент кольца R: для некоторого $v \in R$ выполняется $uv = 1$. Далее получаем обратимость $1 - a$ слева: если $(1-a)u = 1$, то $(1-a)uv = v$, откуда $1 - a = v$ и поэтому $u(1-a) = uv = 1$. Значит, a лежит в пересечении всех максимальных левых идеалов. Поменяв слова «левый» и «правый», получаем обратное включение: пересечение максимальных левых идеалов содержится в $J(R)$.

13.60. а) $\Rightarrow$ б). Пусть I — максимальный левый идеал. Если r и $1 - r$ — необратимые элементы, то из включений $Rr, R(1-r) \subseteq I$ следует, что $1 \in Rr + R(1-r) \subseteq I$, откуда $I = R$.

б) $\Rightarrow$ в). Пусть a обратим слева: $ba = 1$. Если $cab = 1$ для некоторого c, то $caba = a = ca$, откуда $ab = 1$, т.е. a — обратимый элемент. Если допустить, что ab необратим слева, то по условию $c(1-ab) = 1$ для некоторого c, откуда $a = c(1-ab)a = ca - caba = 0$, противоречие с тем, что $ba = 1$.

в) $\Rightarrow$ г). Предположим, что для $a, b \in I$ элемент $a + b$ обратим. Тогда $c(a+b) = 1$ для некоторого c, откуда $ca = 1 - cb$. Из импликации б) $\Rightarrow$ в) вытекает, что каждый обратимый слева элемент обратим. Поэтому из $a \in I$ и $r \in R$ следует, что и $ra \in I$ (ибо если $ra \notin I$, то ra обратимый слева, откуда a обратимый слева и поэтому $a \notin I$). Таким образом, $ca, cb \in I$. С другой стороны, из условия $cb \in I$, в силу в), вытекает, что $ca = 1 - cb \notin I$.

г) $\Rightarrow$ д). Покажем сначала, что каждый обратимый слева (справа) элемент обратим. Пусть $ba = 1$. Если $ab \notin I$, то $abc = 1$ для некоторого c, откуда $b = babc = bc$ и поэтому $ab = 1$, что и требовалось. Если допустить, что $ab \in I$, то $1 - ab \notin I$, так как в противном случае $1 - ab + ab = 1 \in I$. Далее, так как $1 = (1-ab)c$, то $b = b(1-ab)c = bc - babc = (b-b)c = 0$, противоречие с тем, что $ba = 1$.

По предположению I аддитивно замкнуто, поэтому остается лишь показать, что $xr, rx \in I$ для всех $x \in I$ и $r \in R$. Допустим, что $rx \notin I$. Тогда $zrx = 1$ для некоторого z. Откуда по только что доказанному, $xzr = 1$, противоречие с тем, что $x \in I$. Для xr доказательство аналогично.

Эквивалентность д) $\iff$ е) очевидна.

д) $\Rightarrow$ ж). Поскольку $1 \notin I$, то $I \neq R$. Пусть J — левый идеал ($\neq R$) и $y \in J$. Тогда $Ry \subseteq J$, откуда y не имеет левого обратного, в частности, y не имеет обратного, значит, $y \in I$. Поэтому $J \subseteq I$.

Импликация ж) $\Rightarrow$ а) очевидна.

13.61. а) Кольцо P $[[x]]$ локально, ибо его необратимые элементы — это в точности ряды со свободным членом, равным 0, а множество таких рядов замкнуто относительно сложения; (x) — максимальный идеал.

г) См. 11.54.

13.67. Пусть I — идеал, содержащий P, и $I \neq P$. Если $x \in I \backslash P$, то из $x\left(1 - x^{n-1}\right) = 0 \in P$ следует, что $1 - x^{n-1} \in P$, $1 = \left(1 - x^{n-1}\right) + x^{n-1} \in I$ и $I = R$.

13.69. ($\Rightarrow$). Поскольку максимальный идеал I прост, то кольцо является локальным. В I содержатся все необратимые элементы кольца, которые нильпотентны в силу единственности простого идеала (см. 13.15 3)).

($\Leftarrow$). Множество всех нильпотентных элементов кольца образует идеал I. Из условия следует, что I — максимальный идеал. С другой стороны, I содержится в каждом простом идеале кольца. Поэтому I является единственным простым идеалом.

13.70. Если делителей нуля в кольце нет, то простым является нулевой идеал. Если a — делитель нуля, то идеал aR состоит из делителей нуля. Во множестве всех идеалов, состоящих из делителей нуля, по лемме Цорна есть максимальные элементы. Выберем такой идеал P и покажем, что он простой. Пусть $x, t \notin P$. В идеалах $P + xR$, $P + tR$ найдутся неделители нуля $a + xr$ и $b + ts$, где $a, b \in P$, $r, s \in R$. Поскольку произведение $w = (a + xr)(b + ts)$ является неделителем нуля, то $w \notin P$. Так как $c = ab + ats + bxr \in P$, то $w - c = xtrs \notin P$ и $xt \notin P$.

13.71. Пусть $I \subseteq \bigcup_{i=1}^{n} P_i$. Допустим, что $I \not\subset P_i$ $(i = 1, \ldots, n)$. Тогда можно предполагать, что $I \cap P_j \not\subset \bigcup_{i \neq j} P_i$ для всех j. Пусть $a_j \in I \cap P_j$, но $a_j \notin \bigcup_{i \neq j} P_i$. Тогда элемент $a_1 + a_2 \ldots a_n \in I$, но не принадлежит ни одному P_i.

13.72. Докажем более общее утверждение, а именно, если идеал A содержится в простом идеале B, то множество всех простых идеалов P со свойством $A \subseteq P \subseteq B$ содержит минимальные элементы. В силу леммы Цорна достаточно показать, что любое линейно упорядоченное по включению семейство $\{P_i \,|\, A \subseteq P_i \subseteq B\}_{i \in I}$ простых идеалов обладает нижней гранью. Пусть $P = \bigcap_{i \in I} P_i$ и $ab \in P$, где $a \notin P$. Тогда $a \notin P_i$ для некоторого i. Для любого $j \in I$ имеем $P_j \subset P_i$ либо $P_i \subset P_j$. В первом случае $a \notin P_j$ и, следовательно, $b \in P_j$. Во втором случае $b \in P_i \subset P_j$. Таким образом, $b \in P$, т.е. идеал P прост. Наше утверждение вытекает из доказанного (при $A = 0$).

13.73. Идеал $I = (4) + (x)$ состоит из многочленов, чьи свободные члены делятся на 4. Единственный идеал $J \supset I$, $J \neq I, R$, — это идеал $(2) + (x)$. Из $2 \notin I$, $4 \in I$ следует, что I не простой, а из $J^2 \neq I$ получается неразложимость I в произведение простых.

13.79. Всякое поле артиново и нетерово, $\mathbb{Z}$ — неартиново подкольцо поля $\mathbb{Q}$. Кольцо $\mathbb{Q}[x_1, x_2, \ldots]$ не является ни артиновым, ни нетеровым. Однако эта коммутативная область вкладывается в свое поле частных.

13.83. Пусть $\{x_i \,|\, i \in \mathbb{N}\}$ — счетное множество элементов из R, линейно независимых над K, если $a_i = \begin{pmatrix} 0 & x_i \\ 0 & 0 \end{pmatrix}$, то $Sa_i = \begin{pmatrix} 0 & Kx_i \\ 0 & 0 \end{pmatrix}$. Поэтому $Sa_1 \subset Sa_1 + Sa_2 \subset Sa_1 + Sa_2 + Sa_3 \subset \ldots$ — строго возрастающая, а $\sum_{i=1}^{\infty} Sa_i \supset \sum_{i=2}^{\infty} Sa_i \supset \sum_{i=3}^{\infty} Sa_i \supset \ldots$ — строго убывающая цепь левых идеалов.

Пусть $I_1 = \begin{pmatrix} 0 & R \\ 0 & 0 \end{pmatrix}$ и $I_2 = \begin{pmatrix} 0 & 0 \\ 0 & R \end{pmatrix}$; эти правые идеалы минимальны (так как R — поле) и $I_1 \cap I_2 = 0$. Поскольку $(I_1 + I_2)/I_1 \cong I_2$, то идеал I_1 максимален в $I_1 + I_2$. Имеем $0 \subset I_1 \subset I_1 + I_2 \subset S$. Осталось показать, что идеал $I_1 + I_2$ максимален в S. Пусть $h = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \notin I_1 + I_2$. Тогда $a \neq 0$ и для $J = I_1 + I_2 + hS$ имеем $\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1-c \end{pmatrix} \right) \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in J$. Следовательно, $J = S$.

13.84. Пусть I — максимальный среди нильпотентных идеалов, $I^k = 0$. Так как из $J^m = 0$ следует $(I+J)^{k+m} = 0$, то I — наибольший нильпотентный идеал, откуда $(r) \subseteq I$ для каждого нильпотентного элемента $r \in R$.

13.85. С возрастающей цепью правых идеалов $I_1 \subseteq I_2 \subseteq \ldots$, где $I_k = r(J_k)$, J_k — левый идеал, можно связать убывающую цепь левых идеалов $\ell(I_1) \supseteq \ell(I_2) \supseteq \ldots$ и возрастающую цепь правых идеалов $r(\ell(I_1)) \subseteq r(\ell(I_2)) \subseteq \ldots$. Первая и третья последовательности совпадают (см. 12.21), а вторая с какого-то места обрывается.

13.88. Пусть P — простой идеал в R, $r \in R \backslash P$. Тогда $(r^n) = \left(r^{n+1}\right)$ для некоторого n; $r^n = r^{n+1}s$, $s \in R$. Так как $r^{n+1}s + P = r^n + P$, а R/P — область целостности, то $rs + P = 1 + P$, т.е. R/P — поле и поэтому идеал P максимален.

13.89. Пусть $0 \neq a \in R$. Так как $(a^n) = \left(a^{n+1}\right)$ при некотором n, то $a^n = a^{n+1}b$, $b \in R$. Откуда $a^n(1-ab) = 0$ и $1 = ab$, т.е. a обратим.

13.90. Каждый простой идеал в таком кольце максимален (13.88). Рассмотрим множество всевозможных конечных пересечений максимальных идеалов. В этом множестве есть минимальный элемент: $J = I_1 \cap \ldots \cap I_n$. Тогда $J \subseteq I$ для любого максимального идеала I. Так как $I_1 \ldots I_n \subseteq J$, то $I_k \subseteq I$ для некоторого k. В силу максимальности $I_k = I$.

14. Разложение на простые множители

14.1. Кольцо целых алгебраических чисел K; если $a \in K$, то $a = \sqrt{a}\sqrt{a} = \ldots$.

14.6. б) Если $m = a'a$, то $ab = dm = da'a$, откуда $b = da'$, т.е. $d \,|\, b$. Аналогично, $d \,|\, a$. Далее, пусть $a = fa''$, $b = fb''$. Обозначим $c = fa''b''$. Тогда $c = ab'' = ba''$ и, значит, $c = c'm$. Откуда $ab = fc = fc'm = md$, это дает $fc' = d$, т.е. $f \,|\, d$. Таким образом, $d = (a, b)$.

14.12. а) Если $\delta(b) = \delta(a)$, то $b = qa + r$, где $\delta(r) < \delta(a)$ и $r \neq 0$ ввиду неассоциированности a и b. Тогда $r = b - qa = b(1 - qc)$ и $\delta(r) \geqslant \delta(b) = \delta(a)$. Противоречие. б) Очевидно. в) Вытекает из алгоритма Евклида.

д) Если $au + bv = 1$ и $ax + cy = 1$, то $a(aux + cuy + bvx) + bc(vy) = 1$. е) Если $b \,|\, a$ и $c \,|\, a$, то $[b, c] \,|\, a$. Так как $bc = (b, c)[b, c]$ и $(b, c) = 1$, то $[b, c] = bc$. ж) Если $au + bv = 1$, то $(ac)u + (bc)v = c$. Так как $bc = aw$, то $c = a(cu + wv)$, т.е. $a \,|\, c$.

14.14. Пусть $p = p_1 \ldots p_r$ — разложение на простые множители в $\mathbb{Z}[i]$. Тогда $p^2 = \delta(p) = \delta(p_1) \ldots \delta(p_r)$, где $\delta(p_i) \in \mathbb{Z}$. Поэтому $r = 2$, $p = p_1 p_2$ и $\delta(p_1) = \delta(p_2) = p$. Если $p_1 = m + ni$, то $p = \delta(p_1) = m^2 + n^2 = (m + ni)(m - ni)$, поэтому $p_2 = m - ni$. Так как $t^2 \equiv 0$ или $1 \pmod 4$ для любого $t \in \mathbb{Z}$, то для нечетного простого числа p, не являющегося простым в $\mathbb{Z}[i]$, получаем $p = m^2 + n^2 \equiv 0, 1$ или $2 \pmod 4$, откуда $p = 4k + 1$. Покажем, что простое число вида $p = 4k + 1$ не является простым в $\mathbb{Z}[i]$. Положим $t = (2k)!$. Так как $t = (-1)^{2k}(2k)! = (-1)(-2)\ldots(-2k) \equiv (p-1)(p-2)\ldots(p-2k) \equiv ((p+1)/2)\ldots(p-2)(p-1) \pmod p$, то $t^2 \equiv (2k)!((p+1)/2)\ldots(p-2)(p-1) \equiv (p-1)! \pmod p$. Применяя теорему Вильсона, $((p-1)! + 1 \equiv 0 \pmod p)$, получаем $t^2 + 1 \equiv 0 \pmod p$. Если допустить, что p — простой элемент в $\mathbb{Z}[i]$, то из равенства $(t + i)(t - i) = t^2 + 1 = lp$, $l \in \mathbb{Z}$, следует делимость на p одного из элементов $t + i$, $t - i$. Но $t \pm i = p(m + ni)$, откуда $\pm 1 = pn$, $n \in \mathbb{Z}$, что невозможно в $\mathbb{Z}$. Так как $2 = (1 + i)(1 - i)$ не является простым в $\mathbb{Z}[i]$, то доказано, что простое число $p \in \mathbb{Z}$ остается простым в $\mathbb{Z}[i]$ в точности тогда, когда $p = 4k - 1$. Всякое простое число $p = 4k + 1$ представимо в виде $p = m^2 + n^2$ для некоторых $m, n \in \mathbb{Z}$.

4) К вышедоказанному достаточно показать, что если $(m, n) = 1$ и $p \,|\, m^2 + n^2$, то $p = 4k + 1$. Так как $(m, n) = 1$ и $m^2 + n^2 \equiv 0 \pmod p$, то $p \nmid mn$, откуда $m^{p-1} \equiv 1 \pmod p$. Поэтому $\left(m^{p-2}n\right)^2 = m^{2p-4}n^2 \equiv -m^{2p-2} \equiv -1 \pmod p$. Таким образом, существует $s \in \mathbb{Z}$ такое, что $s^2 \equiv -1 \pmod p$, $s^4 \equiv 1 \pmod p$. Поэтому порядок $p - 1$ группы $\mathbb{Z}_p^*$ делится на 4 (в силу цикличности) и $p = 4k + 1$.

14.15. Число n — простое вида $p = 4k - 1$, оно является простым элементом в $\mathbb{Z}[i]$. Поэтому идеал (p) максимален. Поле $\mathbb{Z}[i]/(p)$ содержит p^2 элементов.

14.16. Если допустить, что $x^2 + 1 = (x + a)(x + b)$, то $a + b \equiv 0 \pmod p$, $a^2 b^2 \equiv 1 \pmod p$. Отсюда $a \equiv -b \pmod p$ и $a^4 \equiv b^4 \equiv 1 \pmod p$. Откуда следует, что порядок $p - 1$ группы $\mathbb{Z}_p^*$ делится на 4, значит, 4 делит 2. Противоречие.

14.21. Пусть, например, $p = 2$. Равенства $2 = 2^{1/2} \cdot 2^{1/2} = 2^{1/2} \cdot 2^{1/4} \cdot 2^{1/4} = \ldots$ показывают, что в кольце не выполнено условие разложения на простые множители.

14.23. а) Положим $\delta(m + in) = m^2 + n^2$, т.е. $\delta(a) = N(a)$ — норма a. Тогда $\delta(ab) = \delta(a)\delta(b) \geqslant \delta(a)$ для $a, b \in \mathbb{Z}[i]$. Пусть $b \neq 0$. Тогда $ab^{-1} = \alpha + i\beta \in \mathbb{Q}(i)$. Возьмем ближайшие к α, β целые числа k, l такие, что $\alpha = k + \nu$, $\beta = l + \mu$, $|\nu|, |\mu| \leqslant 1/2$. Имеем $a = b[(k + \nu) + i(l + \mu)] = bq + r$, где $q = k + il \in \mathbb{Z}[i]$, $r = b(\nu + i\mu)$. Так как $r = a - bq$, то $r \in \mathbb{Z}[i]$, причем $\delta(r) = |r|^2 = |b|^2(\nu^2 + \mu^2) \leqslant \delta(b)(1/4 + 1/4) = 1/2\delta(b) < \delta(b)$. Далее, включение $u = m + in \in U(\mathbb{Z}[i])$ равносильно равенству $\delta(u) = 1$, т.е. $m^2 + n^2 = 1$. Откуда $U(\mathbb{Z}[i]) = \langle i \rangle$ — циклическая группа.

б) Для $a = m + n\omega \in \mathbb{Z}[\omega]$, $\delta(a) = m^2 - mn + n^2 = a\bar{a}$. Пусть $0 \neq b \in \mathbb{Z}[\omega]$. Тогда $ab^{-1} = a\bar{b}/b\bar{b} = \alpha + \beta\omega$, где $\alpha, \beta \in \mathbb{Q}$. Возьмем ближайшие к α, β целые числа k, l такие, что $\alpha = k + \nu$, $\beta = l + \mu$. Имеем $a = b[(k + \nu) + \omega(l + \mu)] = bq + r$, где $q = k + \omega l \in \mathbb{Z}[\omega]$, $r = b(\nu + \omega\mu) \in \mathbb{Z}[\omega]$, $\delta(r) = \delta(b)\delta(\nu + \omega\mu) = \delta(b)(\nu^2 - \nu\mu + \mu^2) \leqslant 3/4\delta(b) < \delta(b)$. $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$.

в) $\delta(m + n\sqrt{-2}) = m^2 + 2n^2$. $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$.

Пусть $K = \mathbb{Z}[\sqrt{-3}]$, $0 \neq a = m + n\sqrt{-3} \in K$, $N(a) = m^2 + 3n^2 \in \mathbb{N}$. Если a обратим, то $N(a^{-1}) = N(a)^{-1} \in \mathbb{N}$, значит, $N(a) = 1$, $n = 0$, $m = \pm 1$. Если $a = a_1 \ldots a_r$, то $N(a) = N(a_1) \cdot \ldots \cdot N(a_r)$, где $1 < N(a_i) \in \mathbb{N}$. Значит, r не может

неограниченно расти. Следовательно, разложение на простые множители в K возможно. Далее, $4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3})$, $N(2)=N(1\pm\sqrt{-3})=4$. Поэтому из разложения $a=a_1a_2$ для $a=2$ или $1\pm\sqrt{-3}$ следовало бы $4=N(a)=N(a_1)N(a_2)$, т.е. $N(a_i)=2$, что невозможно, поскольку уравнение $x^2+3y^2=2$ с $x,y\in\mathbb{Z}$ неразрешимо. Простота 2 и $1\pm\sqrt{-3}$ доказана.

14.25. Предположим, что $f(x)=g(x)h(x)$, где $f(x)\in K[x]$, с $g(x),h(x)\in Q[x]$. Умножим обе части этого равенства на квадрат наименьшего общего кратного знаменателей всех коэффициентов многочленов $g(x)$ и $h(x)$. Тогда $af(x)=bg_0(x)h_0(x)$, где $a,b\in K$ и $g_0(x),h_0(x)$ — многочлены с содержанием, равным 1. По лемме Гаусса $ad(f(x))=b$, откуда $f(x)=d(f(x))g_0(x)h_0(x)$ над K, что противоречит неприводимости $f(x)$ над K.

14.26. Предположим противное. Воспользовавшись предыдущим упражнением, запишем $f(x)$ в виде произведения двух многочленов над $\mathbb{Z}$: $f(x)=(x^s+b_1x^{s-1}+\ldots+b_s)(x^t+c_1x^{t-1}+\ldots+c_t)$, это разложение сохранится в факторкольце $\mathbb{Z}[x]/(p)\cong\mathbb{Z}_p[x]$. По условию $\overline{a}_i=\overline{0}$ (вычет по модулю p). Так как $x^sx^t=(x^s+\overline{b}_1x^{s-1}+\ldots+\overline{b}_s)(x^t+\overline{c}_1x^{t-1}+\ldots+\overline{c}_t)$, то $\overline{b}_i=\overline{c}_j=\overline{0}$, т.е. $p\,|\,b_i,c_j$, откуда $p^2\,|\,a_n=b_sc_t$. Противоречие.

14.27. Например, $x^3=x(x-4)^2=(x-2)(x^2+2x+4)=(x-6)(x^2-2x+4)$.

14.28. Если $a=p_1\cdot\ldots\cdot p_n$, то $(a)=(p_1)\cdot\ldots\cdot(p_n)$.

14.30. Предположим, что в кольце K содержится точно n классов простых ассоциированных элементов с представителями $p_1,\ldots,p_n$. Заметим, что в этом случае все элементы вида $g_i=(p_1\cdot\ldots\cdot p_n)^i-1$, $i\in\mathbb{N}$, различны и обратимы. Действительно, $g_i\neq 0$, а необратимость какого-то g_i влечет существование у него простого делителя, который не может принадлежать ни одному из имеющихся n классов простых ассоциированных элементов. Предположение же $g_l=g_k$ для некоторых $k<l$ ведет к невозможному равенству $(p_1\cdot\ldots\cdot p_n)^{l-k}=1$. Поэтому случай конечности $U(K)$ невозможен. Если допустить, что $U(K)\bigcup\{0\}$ — подгруппа в K^+, то $g_1+1=p_1\cdot\ldots\cdot p_n\in U(K)$, что также исключено.

15. Основные понятия теории модулей

15.1. б) Пусть M — левый R-модуль. Для $r\in R$ положим $\lambda_r(a)=ra$, $a\in M$. Тогда $\lambda_r\in\operatorname{End}M$. Требуемый гомоморфизм f из а) действует как $f(r)=\lambda_r$, $r\in R$.

15.2. Пусть f (соответственно, g) определяет модульное умножение $\circ$ (соответственно, $*$) на M, и $\varphi\colon\langle M,*\rangle\to\langle M,\circ\rangle$ — изоморфизм этих модулей. Тогда $\varphi(r*a)=r\circ\varphi(a)$, $f(r)(a)=r\circ a$ и $g(r)(a)=r*a$, $r\in R$, $a\in M$. Далее, $\varphi(g(r)(a))=\varphi(r*a)=r\circ\varphi(a)=f(r)(\varphi(a))$, $(\varphi g(r))(a)=(f(r)\varphi)(a)$, $\varphi g(r)=f(r)\varphi$ и $g(r)=\varphi^{-1}f(r)\varphi=\phi(f(r))=(\phi f)(r)$, $g=\phi f$, где ϕ — внутренний автоморфизм кольца $\operatorname{End}M$, соответствующий φ (т.е. $\phi(\alpha)=\varphi^{-1}\alpha\varphi$, $\alpha\in\operatorname{End}M$). Обратно, пусть $g=\phi f$. Если ϕ соответствует автоморфизм φ группы M, то φ будет изоморфизмом R-модулей $\langle M,*\rangle$ и $\langle M,\circ\rangle$.

15.6. Пусть B — R-модуль, $\varphi\colon A\to B$ — аддитивный изоморфизм, не являющийся R-модульным. Формула $r\circ a=\varphi^{-1}(r\varphi(a))$, $r\in R$, $a\in A$, задает на A структуру R-модуля $\circ$, отличную от данной. Из $\varphi(r\circ a)=r\varphi(a)$ следует изоморфизм R-модулей $\langle A,\circ\rangle$ и B. Обратно, если на A имеется R-модульная структура $\circ$, отличная от исходной, то тождественное отображение группы A будет аддитивным и не R-модульным изоморфизмом A на $\langle A,\circ\rangle$.

15.8. Умножение получается с помощью формулы $r\circ(b+a)=(rb+(rf(a)-f(ra))+ra$, где $r\in R$, $b\in B$, $a\in A$.

15.9. Умножение дает формула $r\circ(b+a)=(rb+\delta(r)(a))+ra$, где $r\in R$, $b\in B$, $a\in A$.

15.12. 1) Если $f\colon R\to S$ — мультипликативный и не аддитивный изоморфизм, то другое сложение $\dot{+}$ на R определяется по формуле $x\dot{+}y=f^{-1}(f(x)+f(y))$, $x,y\in R$.

15.14. Новое сложение $\dot{+}$ на M можно задать формулой

$$a\dot{+}b=f^{-1}(f(a)+f(b)),\ a,b\in M.$$

Если $\langle M,+,\cdot\rangle$ и $\langle M,\dot{+},\cdot\rangle$ — две структуры R-модуля на M с разными сложениями и одинаковыми модульными умножениями, то нужно рассмотреть тождественное отображение множества M.

15.18. Неразложимость пространства V как модуля над $F[x]$ равносильна тому, что минимальный многочлен $m(x)$ оператора α равен степени некоторого неприводимого многочлена.

15.21. Изоморфизм получится, если гомоморфизму $f\in\operatorname{Hom}_R(R,A)$ поставить в соответствие элемент $f(1)$. Обратный изоморфизм элемент $a\in A$ отображает в такой гомоморфизм $g\in\operatorname{Hom}_R(R,A)$, что $g(r)=ra$, $r\in R$.

15.22. а) Возьмем элементы $e_1=(1,0,\ldots,0),\ldots,e_n=(0,0,\ldots,1)$ R-модуля $R^n=R\oplus\ldots\oplus R$. Пусть $f\in\operatorname{End}_R(R^n)$ и $f(e_i)=r_{i1}+\ldots+r_{in}$, $r_{ij}\in R$, $i,j=1,\ldots,n$. Отображение $f\mapsto(r_{ji})$, где (r_{ji}) — $n\times n$-матрица, является нужным изоморфизмом.

б) Удобнее элементы из R^n записывать в виде векторов-столбцов длины n, $R^n=\begin{pmatrix}R_1\\ \ldots\\ R_n\end{pmatrix}$, где все $R_i=R$. Пусть $f\in\operatorname{End}_{R_n}(R^n)$. Если f оставляет на месте каждое R_i, то f действует на R_i как умножение справа на некоторый элемент $r_i\in R$ (см. 15.21 и а)). На самом деле, $r_1=\ldots=r_n=r$ и f есть умножение на r. Верно и обратное.

15.24. Отображение $x+s^{-1}M\mapsto sx+M$, $x\in R$, является изоморфизмом правых R-модулей $R/s^{-1}M\cong R/M$. Теперь, если J — правый идеал кольца R, содержащий $s^{-1}M$, то $sJ+M$ — правый идеал, содержащий M. Значит, $sJ+M=M$ или $sJ+M=R$. Поэтому $J=s^{-1}M$ или $J=R$, что означает максимальность $s^{-1}M$.

15.28. Эквивалентность б) $\Longleftrightarrow$ в) проверяется непосредственно.

а) $\Rightarrow$ б). Пусть $f=m+n$, $T=mR\cap nR$. Так как $fR=fR\cap mR+fR\cap nR$, то существуют такие $b,d\in R$, что $fb\in mR$, $fd\in nR$, $f=fb+fd$. Поэтому $nb=fb-mb\in T$ и $md=fd-nd\in T$. Пусть $a=1-b$, $z=a-d$. Тогда $1=a+b$ и $fz=f-fb-fd=0$. Поэтому $ma=md+mz=md+fz-nz=md-nz$ и $nz=-mz\in T$. Тогда $ma\in T$ и a — требуемый элемент.

б) $\Rightarrow$ а). Пусть $A, B, G \in L(M)$, $f \in A \cap (B+G)$ и $f = m+n$, где $m \in B$, $n \in G$. По условию существуют такие $a, b \in R$, что $1 = a+b$, $ma \in nR$, $nb \in mR$. Тогда $fb = mb+nb \in fR \cap mR \subseteq A \cap B$, $fa = ma+na \in fR \cap nR \subseteq A \cap G$, $f = fb+fa \in A \cap B + A \cap G$.

а) $\Rightarrow$ г). Пусть $B = \{a \in R \,|\, ma \in (m+n)R\}$, B — правый идеал в R. Тогда $(m+n)R \cap mR = mB$. Если $b \in B$, то $nb = (m+n)b - mb \in (m+n)R$. Поэтому $B = \{a \in R \,|\, na \in (m+n)R\}$ и $(m+n)R \cap nR = nB$. Тогда $(m+n)R = (m+n)R \cap mR + (m+n)R \cap nR = mB + nB$.

г) $\Rightarrow$ а). По условию $(m+n)R = mB + nB$. Откуда $mR \cap (m+n)R = mR \cap (mB+nB) = mB$, $nR \cap (m+n)R = nR \cap (mB+nB) = nB$, $(m+n)R = mR \cap (m+n)R + nR \cap (m+n)R$. Поэтому M — дистрибутивный модуль.

15.29. а) следует из 15.28. б) Пусть $f \in \operatorname{Hom}_R(G, H)$, $n = f(m)$, $m \in G$. Так как существует такое $a \in R$, что $ma = n(1-a) = 0$, то $n = na = f(m)a = f(ma) = f(0) = 0$.

в) следует из б) и из того, что все подфакторы дистрибутивного модуля дистрибутивны.

г) Поскольку $G/(G \cap H) \cong M/H$ и $H/(G \cap H) \cong M/G$, то утверждение следует из б).

15.34. ($\Rightarrow$). $M = \operatorname{Ker} f \oplus M_1$. Пусть $e\colon M_1 \to M$ — вложение M_1 в M. Если $f_1 = f \,|\, M_1$, то f_1 — изоморфизм. Тогда $g = ef_1^{-1}$.

($\Leftarrow$). Поскольку $fg = 1_N$, то f — эпиморфизм и $\operatorname{Ker} f \cap \operatorname{Im} g = 0$. Так как $x - gf(x) \in \operatorname{Ker} f$ для $x \in M$ и $gf(x) \in \operatorname{Im} g$, то $M = \operatorname{Ker} f \oplus \operatorname{Im} g$.

15.39. Рассмотрите отображение $m + N \to (a+X) + (b+Y)$, где $m = a+b$, $a \in A$, $b \in B$.

15.40. а) Вложением будет отображение $m + (A \cap B) \to (m+A, m+B)$, $m \in M$. б) Отображение $A \cap B \to A \oplus B$ есть $a \to (a, -a)$, отображение $A \oplus B \to A + B$ есть $(a, b) \to a + b$, $a \in A$, $b \in B$.

15.41. Пусть β — изоморфизм. Тогда для $x \in X$ существует такой $b \in B$, что $\beta(b) = \varphi(x)$. Поэтому $\gamma g(b) = \psi\beta(b) = \psi\varphi(x) = 0$. Откуда $g(b) = 0$ и $b \in \operatorname{Ker} g = \operatorname{Im} f$. Тогда $f(a) = b$ для некоторого $a \in A$. Поэтому $\varphi\alpha(a) = \beta f(a) = \beta(b) = \varphi(x)$. Откуда $\alpha(a) = x$ и, значит, α — сюръекция. Таким образом, α — изоморфизм.

Пусть $z \in Z$. Тогда $\psi(y) = z$ для некоторого $y \in Y$. Найдется $b \in B$ со свойством $\beta(b) = y$. Откуда $\gamma g(b) = \psi\beta(b) = \psi(y) = z$. Значит, γ — сюръекция и, следовательно, — изоморфизм.

Пусть α и γ — изоморфизмы и $y \in Y$. Тогда $\gamma(c) = \psi(y)$ для некоторого $c \in C$. Найдется $b \in B$ со свойством $g(b) = c$. Откуда $\psi\beta(b) = \gamma g(b) = \gamma(c) = \psi(y)$. Поэтому $\psi(y - \beta(b)) = 0$ и, значит, $\varphi(x) = y - \beta(b)$ для некоторого $x \in X$. Далее, найдется такой $a \in A$, что $\alpha(a) = x$. Откуда $\beta f(a) = \varphi\alpha(a) = \varphi(x) = y - \beta(b)$, а это влечет $\beta(f(a) + b) = y$. Следовательно, β — сюръекция и, значит, — изоморфизм.

15.43. M — множество всех элементов с конечным числом ненулевых компонент.

15.44. 2) Если $x \in t(M)$, $a \in R$ и $xb = 0$ для неделителя нуля b, причем $ac = bd$ (c — неделитель нуля), то $(xa)c = (xb)d = 0$ и, значит, $xa \in t(M)$ для всех $a \in R$. Если теперь $y \in t(M)$, то по доказанному $yb \in t(M)$. Поэтому $(yb)r = 0$ для некоторого неделителя нуля r. Откуда $(x-y)br = 0$. 1) следует из 2).

15.45. 1) ($\Rightarrow$). Пусть $M_1 \subseteq M_2 \subseteq \ldots$ — цепь подмодулей модуля M, $Q = \bigcup M_i$. По условию Q порождается конечным множеством элементов $\{x_1, \ldots, x_n\} \subseteq M_k$. Поэтому $Q = M_k$. ($\Leftarrow$). Допустим противное. Пусть M_1 — циклический подмодуль в M. Так как $M \neq M_1$, то существует циклический подмодуль $N_1 \not\subseteq M_1$. Пусть $M_2 = M_1 + N_1$. Так как $M \neq M_2$, то существует циклический подмодуль $N_2 \not\subseteq M_2$. Повторяя эти рассуждения, получим строго возрастающую цепь $M_1 \subset M_2 \subset \ldots$ подмодулей модуля M, противоречие.

2) Пусть $M = \langle x_1, \ldots, x_n \rangle$ и $\{M_i \,|\, i \in I\}$ — цепь подмодулей в M, $\bigcup\limits_{i \in I} M_i = M$. Тогда $x_j \in M_{i_j}$ для некоторого i_j. Поэтому существует k такой, что все $x_j \in M_{i_k}$. Значит, $M = M_{i_k}$. Обратно, среди множеств, порождающих модуль M, выберем имеющее наименьшую мощность, скажем, m, и рассмотрим его как вполне упорядоченное множество $\{x_i \,|\, i < \alpha\}$, где α — первое ординальное число мощности m. Пусть M_i — подмодуль, порожденный множеством $\{x_j \,|\, j < i\}$. Если m — бесконечное число, то α — предельное ординальное число, и подмодуль M_i — собственный (т.к. порожден менее, чем m элементами). Но тогда подмодуль $M = \bigcup M_i$ также собственный, противоречие.

15.48. Предположим, что $g^*h = hg = 0$, где $h \in \operatorname{Hom}(C, Y)$. Так как g — эпиморфизм, то $h = 0$, т.е. g^* — мономорфизм. Поскольку $f^*g^* = (gf)^* = 0^* = 0$, то осталось только проверить включение $\operatorname{Ker} f^* \subseteq \operatorname{Im} g^*$. Пусть $h \in \operatorname{Ker} f^*$, т.е. $hf = 0$. Тогда для эпиморфизма $e\colon B \to B/\operatorname{Im} f$ имеем $h = ge$. Изоморфизм $C \cong B/\operatorname{Im} f$ влечет существование такого $d \in \operatorname{Hom}(C, Y)$, что $dg = h$, т.е. $h \in \operatorname{Im} g^*$. б) доказывается аналогично.

15.49. Эквивалентность а) и б) легко устанавливается. Пусть $x \in B$. Тогда $x - h(g(x)) \in \operatorname{Ker} g$. Значит, $B = \operatorname{Ker} g + \operatorname{Im} h$. Если $x = y + z$, где $y \in \operatorname{Ker} g$ и $z \in \operatorname{Im} h$, то $z = h(w)$ для некоторого $w \in C$. Откуда $w = g(x)$. Таким образом, w (значит, и y) однозначно определяются элементом x. Это доказывает, что $B = \operatorname{Ker} g \oplus \operatorname{Im} h$. Аналогичным образом доказывается справедливость второго прямого разложения.

15.51. а) ($\Rightarrow$). По условию $f = g \,|\, I$ для некоторого $g\colon R_R \to M$. Если $m = g(1)$, то $f(x) = g(1 \cdot x) = mx$ для всех $x \in I$. ($\Leftarrow$). Отображение $g(z) = mz$ задает гомоморфизм $g\colon R_R \to M$, являющийся продолжением f.

б) Пусть P — максимальный подмодуль в N со свойством $P \cap A = 0$, $B = A \oplus P$. Тогда $f\colon B \to M$ — такой гомоморфизм, что $f(x+y) = h(x)$ для всех $x \in N$, $y \in P$.

15.54. R-модуль G можно отождествить с модулем векторов-столбцов $K = \begin{pmatrix} F \\ F \end{pmatrix}$. Если один из элементов $a, b \in F$ отличен от нуля, то R-подмодуль, порожденный $\begin{pmatrix} a \\ b \end{pmatrix}$ в K, совпадает с K.

15.55. Пусть F — поле, $R = M(n, F)$ $(n \geqslant 2)$. Левый R-модуль $K = \begin{pmatrix} F \\ \vdots \\ F \end{pmatrix}$ векторов-столбцов длины n является простым (см. 15.54). Простой R-модуль A изоморфен фактормодулю R/L для некоторого максимального левого идеала L. Это влечет $A \cong K$.

15.57. Необходимость очевидна. Достаточность. Пусть A — подмодуль в M и B — максимальный подмодуль в M среди его подмодулей, имеющих нулевое пересечение с A. Тогда $A \oplus B$ — существенный подмодуль в M, откуда $A \oplus B = M$ и поэтому модуль M полупрост.

15.58. 1) Пусть $C \subset B$ и C' — д.п.с. к C в $L(A)$. Подмодуль $C' \cap B$ является д.п.с. к C в $L(B)$, так как $C \cap (C' \cap B) = 0$ и $C + (C' \cap B) = (C + C') \cap B = B$.

2) Пусть $0 \neq a \in A$ и M — максимальный подмодуль среди подмодулей модуля A, не содержащих элемента a. Подмодуль M будет максимальным в A. Действительно, пусть $M \subseteq N \subseteq A$ и N' — д.п.с. к N в $L(A)$. Так как $a \notin M$ и $N \cap (M + N') = M$, то либо $a \notin N$, либо $a \notin M + N'$. В силу максимальности M либо $M = N$, либо $N' = 0$, т.е. $N = A$. 3) следует из 15.56.

15.60. 1), 2), 3) вытекают из определения. Обозначим через A пересечение всех существенных подмодулей модуля M, через B — сумму гомоморфных образов всех полупростых модулей в модуль M. Если U — простой, а X — существенный подмодули в M, то $U = U \cap X$, значит, $U \subseteq X$. Откуда $\operatorname{Soc} M \subseteq A$. Так как гомоморфный образ полупростого модуля полупрост, то $B \subseteq \operatorname{Soc} M$. Пусть $C \subseteq A$ и G — максимальный подмодуль в M со свойством $C \cap G = 0$. Тогда $C \oplus G$ — существенный подмодуль в M. Откуда $A \subseteq C \oplus G$. Следовательно, $A = C \oplus (G \cap A)$. Значит, A полупрост. Поэтому, если $f\colon A \to M$ — вложение, то $A = \operatorname{Im} f \subseteq B$.

15.63. Импликация а) $\Rightarrow$ б) очевидна. б) $\Rightarrow$ в). Поскольку ${}_RR$ — полупростой модуль, то ${}_RR = \bigoplus\limits_{i=1}^{n} L_i = \bigoplus\limits_{i=1}^{n} Re_i$, где $L_i = Re_i$ — простые подмодули в ${}_RR$, $e_i \neq 0$, $e_ie_j = \delta_{ij}e_i$, $1 = \sum\limits_{i=1}^{n} e_i$. Поэтому $R = \bigoplus\limits_{i=1}^{n} e_iR$. Пусть e — один из e_i и $0 \neq a = ea \in eR$. Тогда $aR \subseteq eR$. Поскольку $ea \neq 0$ и Re прост, то $f\colon Re \ni re \mapsto rea = ra \in Ra$ — изоморфизм. Если ${}_RR = Ra \oplus U$, то $g\colon R \ni ra + u \mapsto f^{-1}(ra) \in R$ есть эндоморфизм ${}_RR$. Этот эндоморфизм действует как умножение справа на некоторый элемент $b \in R$. Таким образом, $e = g(a) = ab$. Откуда $e \in aR$ и, значит, $eR = aR$, т.е. eR — простой модуль. Аналогично, в) $\Rightarrow$ б).

в) $\Rightarrow$ г). Если $M = M_R$, $0 \neq m \in M$, то mR есть образ эпиморфизма $R_R \to mR$. Поэтому модуль $M = \sum\limits_{m \in M} mR$ полупрост как сумма полупростых модулей. Аналогично, б) $\Rightarrow$ а). А так как г) $\Rightarrow$ в) $\Rightarrow$ б), то утверждение доказано.

15.64. Каждый циклический правый R-модуль $M = mR$ является образом эпиморфизма $R_R \to mR$. Поэтому $M \cong R/A$, где $A \subset R_R$. Если M прост, то A должен быть максимальным правым идеалом. Следовательно, $J(R) \subseteq A$. Тогда $M \cong R/A \cong (R/J(R))\,/\,(A/J(R))$. Поскольку $\overline{R} = R/J(R)$ полупрост, то $\overline{A} = A/J(R)$ — его прямое слагаемое: $\overline{R} = \overline{A} \oplus \overline{B}$, откуда $M \cong \overline{R}/\overline{A} \cong \overline{B}$.

15.66. а) Отображение $eRe \mapsto f_r \in \operatorname{End}_R(eR)$, где $f_r(ex) = (ere)(ex) = erex$, как легко видеть, является искомым изоморфизмом.

б) Если eR — простой модуль, то по лемме Шура $eRe \cong \operatorname{End}_R(eR)$ является телом, что доказывает необходимость. Достаточность. Пусть eRe — тело и $er \neq 0$. Так как R — полупервичное кольцо, то $erRer \neq 0$. Значит, $erse \neq 0$ для некоторого $s \in R$, откуда $ersete = e$ для некоторого $ete \in eRe$. Поэтому $erR = eR$, т.е. eR — простой модуль.

в) следует из а) и б).

15.67. а) Отображение $fre \mapsto g_r \in \operatorname{Hom}_R(eR, fR)$, где $g_r(ex) = frex$, является искомым изоморфизмом.

б) ($\Rightarrow$). Пусть $eR \cong fR$ и $u = fue$ — элемент, соответствующий, в силу а), изоморфизму $eR \to fR$, а $v = evf$ — элемент, соответствующий обратному изоморфизму $fR \to eR$. Тогда $vu = e$ и $uv = f$.

в) вытекает из б) в силу симметричности условий $vu = e$ и $uv = f$.

15.68. Вытекает из 13.7.

15.69. Цоколь S модуля R_R совпадает с $\sum eR$, где e пробегает множество всех таких идемпотентов, что eRe — тело. Цоколь S' модуля ${}_RR$ равен аналогичной сумме $\sum Re$. Поскольку S — вполне инвариантный подмодуль в R_R, то S является идеалом и, следовательно, $S' \subseteq S$. Аналогично, $S \subseteq S'$.

15.70. 2) Пусть R — примитивное кольцо, I — его максимальный правый идеал. Тогда R/I — точный простой модуль. Обратно, пусть M_R — точный простой модуль. Если $0 \neq m \in M$, то $mR = M$. Поэтому отображение $R \to M$, $r \mapsto mr$, является эпиморфизмом. Пусть I — ядро этого эпиморфизма. Так как R/I изоморфен подмодулю модуля M, то I — максимальный правый идеал. Включение $Rr \subseteq I$ равносильно тому, что $Mr = 0$, т.е. $r = 0$. Следовательно, R — примитивное кольцо. 3) проверяется непосредственно.

15.71. Обозначим $G^r = \{x \in R \,|\, Gx = 0\}$ и $S^\ell = \{m \in M \,|\, mS = 0\}$, где S — произвольное подмножество в R. Докажем индукцией по числу образующих подмодуля G, что: (1) существует $r \in R$ с $G(e - r) = 0$ и (2) $G^{r\ell} = G$. Допустим, что (1) и (2) справедливы для G. Рассмотрим $G + Dm$, где $m \notin G$. Пусть $G(e - r) = 0$. Будем искать элемент $s \in R$, для которого $(G + Dm)(e - r - s) = 0$. Положим $b = m(e - r)$. Достаточно добиться того, что $Gs = 0$ и $ms = b$. Существование такого элемента очевидно, если $mG^r = M$. Если же $mG^r \neq M$, то $mG^r = 0$, откуда $m \in G^{r\ell} = G$, что противоречит предположению. Таким образом, для $G + Dm$ выполнено (1).

Осталось показать, что $G + Dm = (G + Dm)^{r\ell} = (G^r \cap m^r)^\ell$. Очевидно, что $G + Dm \subseteq (G + Dm)^{r\ell}$. Пусть теперь $b \in (G^r \cap m^r)^\ell$, т.е. $br = 0$, если $Gr = 0$ и $mr = 0$. Рассмотрим отображение $d\colon mG^r \to bG^r$, $mr \mapsto br$. Так как M_R прост, то либо

$aG^r = 0$, либо $mG^r = M$. В первом случае, $bG^r = 0$ и потому $b \in G^{r\ell} = G \subseteq G + Dm$. Во втором, — $d \in D$ и $br = dmr$ при всех $r \in G^r$. Отсюда следует, что $b - dm \in G^{r\ell} = G$ и потому $b \in G + Dm$.

15.72. 1) Очевидно. 2) Если I — первичный идеал и $aRb \subseteq I$, то $(RaR)\,(RbR) \subseteq I$. Тогда $a \in RaR \subseteq I$ или $b \in RbR \subseteq I$. Обратно, пусть выполнено условие упражнения и $AB \subseteq I$. Если $a \in A \backslash I$, то $aRb \subseteq I$ для любого $b \in B$. Следовательно, $B \subseteq I$.

3) Пусть I примитивен в R. Тогда $I = \{r \in R \,|\, Rr \subseteq J\}$, где J — некоторый максимальный правый идеал. Пусть теперь A и B — идеалы в R, для которых $AB \subseteq I \subseteq J$. Тогда если $M = \{r \in R \,|\, rB \subseteq J\}$, то $A, J \subseteq M$. Поскольку M — правый идеал, то $M = J$ или $M = R$. В первом случае, $A \subseteq M = J$, во втором, $B \subseteq MB \subseteq J$.

15.76. а) $\Rightarrow$ б). Пусть $a_0 = a \neq 0$. Так как идеал Ra_0R не является нильпотентным, то существует $0 \neq a_1 \in a_0Ra_0$. Продолжая этот процесс, убеждаемся, что a не является строго нильпотентным, т.е. $a \notin \operatorname{rad} R$.

б) $\Rightarrow$ в). Если $AB = 0$, то $AB \subseteq I$ для любого первичного идеала I. Поэтому $A \subseteq I$, либо $B \subseteq I$. Значит, $A \cap B \subseteq I$. Отсюда $A \cap B \subseteq \operatorname{rad} R = 0$.

в) $\Rightarrow$ а). Если $I^n = 0$, то $I = I \cap \ldots \cap I = 0$.

15.77. а) Если $r \in J(R)$, то $r \in I$ для каждого максимального правого идеала I, т.е. $1 \notin I + rR$. Следовательно, $r \in J(R)$ в точности тогда, когда $1 - rx$ не принадлежит никакому максимальному правому идеалу при всех $x \in R$, т.е. $1 - rx$ — обратимый справа элемент.

б) В силу а) $J(R)$ содержит любой такой идеал K. Согласно 13.56 $J(R)$ — идеал кольца R. Поэтому осталось лишь показать обратимость элемента $1 - r$ для любого $r \in J(R)$. Ввиду а) $(1 - r)\,u = 1$ для некоторого $u \in R$. Имеем $u = 1 - (1 - u)$, где $1 - u = -ru \in J(R)$. Поэтому найдется $v \in R$ со свойством $uv = 1$. Тогда $v = (1 - r)\,uv = 1 - r$ и $u\,(1 - r) = 1$.

в) Следует из 13.58.

г) Так как $J(R)$ — идеал, то $r \in J(R)$ равносильно тому, что $Rr \subseteq I$ для любого максимального правого идеала I, т.е. $r \in \{x \in R \,|\, Rx \subseteq I\} = P$ для любого примитивного идеала P.

д) Пусть Q — пересечение аннуляторов всех правых простых R-модулей, Q — идеал в R и $Q = RQ$. Если I — максимальный правый идеал, то $M = R/I$ — простой R-модуль, $MQ = 0$, значит, $Q = RQ \subseteq I$, т.е. $Q \subseteq J(R)$. Обратно, если $x \in R \backslash Q$, т.е. $Vx \neq 0$ для некоторого простого модуля V, то $VxR = V$. Поэтому $VxRx = Vx \neq 0$. Значит, найдутся такие $v \in V$ и $a \in R$, что $vxax \neq 0$. Тогда $vxaR = V$. Следовательно, отображение $f\colon R \to V$, $f\colon r \mapsto vxar$ есть эпиморфизм. Так как $f(x) = vxax \neq 0$, то $x \notin J(R)$. Поэтому $J(R) \subseteq Q$.

е) Следует из того, что если r — нильпотентный элемент, то элемент $1 - r$ обратим.

15.79. Эквивалентность а) $\iff$ б) следует из 15.77. Эквивалентность б) $\iff$ в) проверяется непосредственно. а) $\Rightarrow$ г). Покажем, что MA — малый подмодуль в M. Допустим, что $Q \in L(M)$ и $M = \sum_{i=1}^{n} m_iR = Q + MA = Q + \sum_{i=1}^{n} m_iA$. Существуют такие $q \in Q$ и $a_1, \ldots, a_n \in A$, что $m_1 = q + \sum_{i=1}^{n} m_ia_i$. Достаточно показать индукцией по n, что $Q = M$. Если $n = 1$, то $m_1 = m_1(1 - a_1)(1 - a_1)^{-1} = q(1 - a_1)^{-1} \in Q$, откуда $M = m_1R = Q$. Допустим, что $n > 1$. Имеем $m_1 = m_1(1 - a_1)(1 - a_1)^{-1} = (q + \sum_{i=2}^{n} m_ia_i)(1 - a_1)^{-1} \in Q + \sum_{i=2}^{n} m_iA$. Поэтому $M = Q + \sum_{i=2}^{n} m_iA$ и $M = Q$ по предположению индукции.

г) $\Rightarrow$ в). Пусть B — такой правый идеал кольца R, что $R = A + B$. Тогда если $M = (R/B)_R$, то $MA = M$. По условию $M = 0$. Откуда $B = R$.

15.80. 1) Применить индукцию по n. 2) Пусть $f(A) + U = N$ и $m \in M$. Тогда $f(m) = f(a) + u$ для некоторых $a \in A$ и $u \in U$. Так как $f(m - a) = u$, то $m - a \in f^{-1}(U)$ и, значит, $m \in A + f^{-1}(U)$. Следовательно, $A + f^{-1}(U) = M$. Откуда $f^{-1}(U) = M$ и $f(M) = ff^{-1}(U) = U \cap \operatorname{Im} f$. Поэтому $f(A) \subseteq f(M) \subseteq U$ и $U = f(A) + U = N$.

3) ($\Leftarrow$). Если C — максимальный подмодуль в M и $a \notin C$, то $aR + C = M$. Поэтому aR не является малым в M. ($\Rightarrow$). Пусть $\Gamma = \{B \,|\, B \subset M,\ (B \neq M)$ и $aR + B = M\}$. Так как aR не является малым подмодулем, то $\Gamma \neq \varnothing$, Γ удовлетворяет условию леммы Цорна, значит, Γ обладает максимальным элементом C, который является максимальным подмодулем в M. Действительно, если $C \subset U \subseteq M$, то из $U \notin \Gamma$ и $aR + U = M$ следует равенство $U = M$.

15.82. 1) Пусть $A = \sum U$, $B = \bigcap \operatorname{Ker} f$, где U пробегает все малые подмодули, а f — все гомоморфизмы модуля M в полупростые модули. Пусть, далее, $a \in J(M)$, и предположим, что aR не является малым подмодулем в M. Тогда найдется максимальный подмодуль C в M такой, что $a \notin C$ и, значит, $a \notin J(M)$. Следовательно, aR — малый подмодуль и потому $aR \subseteq A$, т.е. $J(M) \subseteq A$. Пусть G — максимальный подмодуль в M, и $M \to M/G$ — канонический эпиморфизм модуля M на простой модуль M/G. Откуда следует, что $B \subseteq J(M)$. Для каждого гомоморфизма $g\colon M \to N$ из того, что U — малый подмодуль в M следует малость подмодуля $g(U)$ в N. Если N полупрост, то единственным малым подмодулем в N является 0 и потому $g(M) = 0$. Следовательно, $A \subseteq B$.

2) следует из определения.

3) Пусть $M = \bigoplus\limits_{i \in I} M_i$ и $\pi_i\colon M \to M_i$ — канонические проекции. Так как $J(M)$— вполне инвариантный подмодуль, то $\pi_i\,(J\,(M)) \subseteq J(M)$. Откуда $J\,(M) = \bigoplus\limits_{i \in I} (M_i \cap J(M))$. Очевидно, что $M_i \cap J(M) = J\,(M_i)$ для всех $i \in I$.

4) Пусть N — такой собственный подмодуль модуля M, что $N + J(M) = M$. Так как M — конечно порожденный модуль, то N содержится в некотором максимальном подмодуле P модуля M. Поэтому $P + J(M) = M$. Так как $J(M) \subseteq P$, то $P = M$, противоречие.

5) $J(M) = \sum U$, где U пробегает все малые подмодули модуля M, $f\,(J(M)) = f\left(\sum U\right)$. Поскольку каждый $f(U)$ — также малый подмодуль в N, то $f\,(J(M)) \subseteq J(N)$. Пусть теперь U — малый подмодуль в N и $A + f^{-1}(U) = M$ для некоторого подмодуля $A \subseteq M$. Так как $f(A) + U = N$, то $f(A) = N$ и потому $A + \operatorname{Ker} f = M$. Тогда $A = M$, т.е. $f^{-1}(U)$ — малый

подмодуль в M. Откуда $f^{-1}(U) \subseteq J(M)$ и, значит, $f\left(f^{-1}(U)\right) = U \subseteq f(J(M))$. Таким образом, $J(N) \subseteq f(J(M))$, т.е. $J(N) = f(J(M))$. Из этого равенства, с учетом включения $\operatorname{Ker} f \subseteq J(M)$, получаем $J(M) = J(M) + \operatorname{Ker} f = f^{-1}f(J(M)) = f^{-1}(J(N))$.

б) Так как отображение $f_m\colon R_R \ni r \mapsto mr \in M_R$ есть гомоморфизм, то $mJ(R_R) = f_m(J(R_R)) \subseteq J(M)$. Откуда $\sum_{m\in M} mJ(R_R) = MJ(R) \subseteq J(M)$.

$J(\mathbb{Z}) = 0$, но $J(\mathbb{Z}/4\mathbb{Z}) = 2\mathbb{Z}/4\mathbb{Z}$ и $J(\mathbb{Q}_\mathbb{Z}) = \mathbb{Q}_\mathbb{Z}$.

15.84. а) Поскольку $(M/MJ(R))\,J(R) = 0$, то $M/MJ(R)$ можно рассматривать как $R/J(R)$-модуль. При этом R-подмодули и $R/J(R)$-подмодули в $M/MJ(R)$ совпадают. По условию $M/MJ(R)$ как модуль над $R/J(R)$ полупрост. Поэтому $J(M/MJ(R)) = 0$ и, значит, $J(M) \subseteq MJ(R)$. Обратное включение справедливо всегда.

б) Обозначим $U = \{m \in M \mid mJ(R) = 0\}$. Имеем $(\operatorname{Soc} M)\,J(R) \subseteq J(\operatorname{Soc} M) = 0$. Поэтому $\operatorname{Soc} M \subseteq U$. С другой стороны, U полупрост как $R/J(R)$-модуль, а значит, и как R-модуль. Следовательно, $U \subseteq \operatorname{Soc} M$.

15.88. Пусть $y = u^2 - u \in I$, где I — ниль-идеал кольца R. Найдем элемент $x \in R$, для которого $e = u + x(1-2u)$ — идемпотент в R, перестановочный с u. Уравнение $e^2 = e$ равносильно уравнению $\left(x^2 - x\right)(1+4y) + y = 0$. Это квадратное уравнение относительно x, формальное решение которого имеет вид $x = \frac{1}{2}\left(1 - (1+4y)^{-\frac{1}{2}}\right)$ или, после разложения в ряд,

$$x = \frac{1}{2}\left(2y - \binom{4}{2} y^2 + \binom{6}{3} y^3 - \dots\right).$$

Так как y — нильпотентный элемент, то эта формула определяет x как многочлен от y с целыми коэффициентами. Поэтому $x \in I$ и $xu = ux$, значит, $e - u \in I$.

16. Локальные, нетеровы и артиновы модули

16.1. Допустим, что $0, 1 \neq e \in S$ — идемпотент. Тогда $1 - e$ — также идемпотент. Так как e и $1 - e$ необратимы, то $1 = 1 - e + e$ — также должен быть необратим.

16.5. Очевидно, что а) $\Rightarrow$ б).

б) $\Rightarrow$ а). Пусть $A_1 \supseteq A_2 \supseteq \dots$ — убывающая цепь подмодулей $A_i \subset M$, $\pi\colon M \to M/A$ — канонический эпиморфизм. Положим $\Gamma = \{A_i\}$, $\pi\Gamma = \{\pi A_i\}$, $\Gamma_A = \{A_i \cap A\}$ $(i = 1, 2, \dots)$. По предположению в $\pi\Gamma$ и Γ_A существуют максимальные элементы: πA_k, $A_m \cap A$. Пусть $n = \max(k, m)$. Достаточно показать, что $A_n = A_{n+i}$. Действительно, $\pi A_n = \pi A_{n+i}$ дает $A_n + A = A_{n+i} + A$. Откуда, учитывая равенство $A_n \cap A = A_{n+i} \cap A$, получаем $A_n = (A_n + A) \cap A_n = (A_{n+i} + A) \cap A_n = A_{n+i} + (A \cap A_n) = A_{n+i} + (A \cap A_{n+i}) = A_{n+i}$.

в) $\Rightarrow$ г). Обозначим $U = \bigcap_{i\in I} A_i$. Тогда $\bigcap_{i\in I}(A_i/U) = 0$. Так как M/U — конечно копорожденный модуль, то $\bigcap_{j\in J}(A_j/U) = 0$ для некоторого конечного $J \subseteq I$. Ясно, что $\bigcap_{i\in I} A_i = \bigcap_{j\in J} A_j$. Аналогично доказывается импликация г) $\Rightarrow$ в).

а) $\Rightarrow$ г). В множестве всех возможных конечных пересечений подмодулей A_i, $i \in I$, существует минимальный элемент. Пусть это будет $D = \bigcap_{j\in J} A_j$. В силу минимальности для каждого $i \in I$ имеем $D \cap A_i = D$, поэтому $D = \bigcap_{i\in I} A_i$. Очевидно, что г) $\Rightarrow$ а).

16.9. а) Пусть $N = mR + nR \in L(M)$. Так как mR и nR сравнимы по включению, то $N = mR$, либо $N = nR$.

б) Так как M — конечно порожденный модуль, то M обладает максимальным подмодулем N, который должен быть единственным (т.к. M — цепной модуль). По а) M — модуль Безу, поэтому он циклический.

в) Пусть $G \neq 0$ — циклический подмодуль модуля M, G обладает максимальным подмодулем H. Значит, G/H — требуемый простой подфактор.

г) Пусть G и H — не сравнимые по включению подмодули модуля M, $\pi\colon M \to M/(G \cap H)$ — канонический эпиморфизм. Ненулевые модули πG и πH обладают простыми подфакторами S_1 и T_1 по в). Поэтому верно г).

16.10. Импликация ($\Leftarrow$) справедлива всегда. ($\Rightarrow$). Из условия и 15.29 в) следует, что M не имеет подфакторов вида $S \oplus T$, где S и T — простые модули. По 16.9 г) M — цепной модуль.

16.11. По 16.3 в) все простые правые R-модули изоморфны. Поэтому из 16.10 следует эквивалентность а) $\Longleftrightarrow$ в). Импликация в) $\Rightarrow$ б) верна всегда.

б) $\Rightarrow$ в). Пусть $m, n \in M$. Достаточно доказать, что либо $m \in nR$, либо $n \in mR$. По 15.31 в) существуют такие $a, b, c, d \in R$, что $m(1 - ac) = nbc$ и $n(1 - bd) = mad$. Так как R локально, то либо $1 - ac \in U(R)$, либо $ac \in U(R)$. В первом случае, $m = nbc(1 - ac)^{-1} \in nR$. Во втором случае, $a, c \in R \setminus J(R)$, откуда $a, c \in U(R)$. Если $d \in U(R)$, то $ad \in U(R)$ и $m = n(1 - bd)(ad)^{-1} \in nR$. Если $d \in R \setminus U(R) = J(R)$, то $1 - bd \in U(R)$ и $n = mad(1 - bd)^{-1} \in mR$.

16.13. Покажем, что д) $\Rightarrow$ а), так как остальные импликации проверяются непосредственно. Допустим, что существует бесконечная убывающая цепь $M \supset M_1 \supset \dots$ подмодулей модуля M. Без ограничения общности, можно считать, что $\bigcap_{i=1}^{\infty} M_i = 0$. Модуль M является существенным расширением конечномерного полупростого модуля N, N артинов. Поэтому существует $n \in \mathbb{N}$ такое, что $N \cap M_i = N \cap M_n$ для всех $i > n$. Откуда $0 = \bigcap_{i=1}^{\infty}(N \cap M_i) = \bigcap_{i=1}^{n}(N \cap M_i) = N \cap M_n$. Существенность N в M влечет $M_n = 0$, противоречие.

16.14. 3) Пусть $F(M)$ — множество всех таких подмодулей X модуля M, что X не является нетеровым. Допустим, что $F(M) \neq \varnothing$. Так как M — артинов, то $F(M)$ обладает минимальным элементом P. По предположению существует простой фактормодуль P/Q. Поскольку P минимален в $F(M)$, то Q — нетеров модуль. Поэтому нетеровость P/Q влечет нетеровость P, противоречие. Остальные условия проверяются непосредственно.

16.17. Пусть $M = x_1R + \ldots + x_nR$. Существует гомоморфизм $f\colon R_R^n \to M$, при котором $f(a_1, \ldots, a_n) = x_1a_1 + \ldots + x_na_n$. Поскольку f сюръективен, то $(R^n/I)_R \cong M$. Если теперь R — нетерово (артиново) кольцо, то нетеров (артинов) R-модуль R^n. Следовательно, нетеров (артинов) модуль $(R^n/I)_R$.

16.20. Пусть $f \in S$. Тогда существует $n \in \mathbb{N}$ со свойством $M = \operatorname{Im} f^n \oplus \operatorname{Ker} f^n$. Откуда $\operatorname{Ker} f^n = 0$, либо $\operatorname{Im} f^n = 0$. Условие $\operatorname{Ker} f^n = 0$ влечет, что f — мономорфизм, значит, f — автоморфизм, т.е. f обратим. Условие $\operatorname{Im} f^n = 0$ влечет $f^n = 0$. Следовательно, $1 - f$ обратим. Поэтому S — локальное кольцо, каждый необратимый элемент которого по доказанному нильпотентен.

16.21. а) Пусть M артинов и Γ — множество всех прямых слагаемых $B \neq 0$ в M. Так как $M \in \Gamma$, то $\Gamma \neq \varnothing$. Пусть B_0 — минимальный подмодуль из Γ, B_0 неразложим. Обозначим через Λ множество всех подмодулей $G \subseteq M$, для которых существует конечное число неразложимых модулей $B_1, \ldots, B_k \neq 0$ таких, что $M = B_1 \oplus \ldots \oplus B_k \oplus G$. Пусть G_0 — минимальный подмодуль из Λ. Ясно, что G_0 не может быть ненулевым разложимым модулем. Для нетеровости рассуждения двойственны к вышеприведенным.

б) вытекает из а) и из предыдущего упражнения.

16.22. M — прямая сумма бесконечного числа неизоморфных простых модулей.

16.29. а) Пусть N — максимальный нильпотентный правый идеал, $N^k = 0$. Если $N_1^m = 0$, то $(N + N_1)^{k+m} = 0$. Поэтому N — наибольший нильпотентный правый идеал, N содержится в первичном радикале $\operatorname{rad} R$. Кроме того, N — двусторонний идеал. Действительно, если $r \in R$, то rN — нильпотентный правый идеал, значит, $rN \subseteq N$. Если теперь A — правый идеал со свойством $A^n \subseteq N$ для некоторого $n \in \mathbb{N}$, то A — нильпотентный правый идеал, значит, $A \subseteq N$. Отсюда следует, что $\operatorname{rad} R \subseteq N$, т.е. $N = \operatorname{rad} R$. Пусть теперь N — левый ниль-идеал. Достаточно показать, что $N \subseteq \operatorname{rad} R$. Предположим сначала, что $\operatorname{rad} R = 0$, т.е. R — полупервично. Если $N \neq 0$, то выберем $0 \neq x \in N$, для которого $r(x)$ является максимальным, и пусть $y \in R$, $yx \neq 0$, а $k \in \mathbb{N}$ — наименьшее со свойством $(yx)^k = 0$. В силу максимальности $r(x) = r\left((yx)^{k-1}\right)$, откуда $yx \in r(x)$, т.е. $xyx = 0$. Таким образом, $xRx = 0$. Поскольку R полупервично, то $x = 0$, т.е. $N = 0$. Переходя к общему случаю, заметим, что образ левого ниль-идеала N при каноническом гомоморфизме в нетерово справа кольцо $R/\operatorname{rad} R$ в силу показанного выше равен нулю. Следовательно, $N \subseteq \operatorname{rad} R$.

б) вытекает из а).

16.30. 1) Так как $J(N/J(N)) = 0$, то можно считать, что $J(N) = 0$. Поэтому в силу артиновости N найдутся такие его максимальные подмодули $F_1, \ldots, F_n$, что $F_1 \cap \ldots \cap F_n = 0$. Поэтому N изоморфен подмодулю конечной прямой суммы простых модулей N/F_i, значит, N сам представим в таком виде.

2) есть следствие 1).

16.31. 1) Среди степеней радикала $J(R)$ найдется наименьший идеал, скажем, $B = J(R)^n$. Откуда $B^2 = B$. Допустим, что $B \neq 0$. Пусть A — минимальный элемент в множестве правых идеалов C со свойством $C \subseteq B$ и $CB \neq 0$. Тогда $aB \neq 0$ для некоторого $a \in A$. Так как $(aB)B = aB^2 = aB \neq 0$, то $aB = A$, значит, $ab = a$ для некоторого $b \in B$. Поскольку $b \in J(R)$, то существует $c \in R$, для которого $(1 - b)c = 1$. Откуда $a = a(1 - b)c = 0$, противоречие. Следовательно, радикал $J(R)$ нильпотентен, он является идеалом, содержащим любой другой нильпотентный идеал.

2) Согласно а) $R/J(R)$ — классически полупростое кольцо, поэтому по 15.84 $J(M) = MJ(R)$ (соответственно, $J(M) = J(R)M$). Далее, $J(R)^n = 0$. Поэтому если $M = U + MJ(R)$, то $M = U + MJ(R)^n = U$, т.е. $J(M) = MJ(R)$ — малый подмодуль в M_R.

16.32. Достаточно доказать эквивалентность а) $\iff$ б). Положим для краткости $U = J(R)$, и определим для каждого модуля M число $e(M)$ формулой $e(M) = \min\{i \in \mathbb{N} \mid MU^i = 0\}$. Такое число существует, так как U — нильпотентный идеал. Докажем эквивалентность а) $\iff$ б) индукцией по $e(M)$ для всех $M \neq 0$.

Пусть $e(M) = 1$, т.е. $MU = 0$. Полагая $\overline{m}(r + U) = mr$, превращаем M в $\overline{R} = R/U$-модуль, причем R-модули совпадают с $\overline{R}$-модулями. Поэтому из полупростоты $\overline{R}$ следует полупростота модуля M, для которого условия а) и б) равносильны.

Пусть теперь утверждение доказано для всех модулей с $e(M) \leqslant k$, и пусть $e(M) = k + 1$. Тогда $e(MU^k) = 1$. Так как $(M/MU^k)U^k = 0$, то $e(M/MU^k) \leqslant k$. Поэтому условия а) и б) равносильны для MU^k и M/MU^k, но тогда а) и б) равносильны и для M.

16.34. ($\Rightarrow$). Вместе с M конечно порожден и любой его эпиморфный образ. Пусть $J(M) + U = M$. Если $U \neq M$, то так как M конечно порожден, U содержится в некотором максимальном подмодуле B, откуда $J(M) + U \subseteq B$. Противоречие. Следовательно, $J(M)$ мал в M.

($\Leftarrow$). Пусть $\overline{x}_i = x_i + J(M)$ $(i = 1, \ldots, n)$ — система образующих для $M/J(M)$. Тогда $x_1R + \ldots + x_nR + J(M) = M$. Так как $J(M)$ мал в M, то $x_1R + \ldots + x_nR = M$.

16.36. ($\Rightarrow$). Покажем, что каждый ненулевой подмодуль U модуля M содержит простой подмодуль E (следовательно, $U \cap \operatorname{Soc} M \neq 0$). Пусть $\Gamma = \{U_i \mid i \in I\}$ — множество всех ненулевых подмодулей модуля U. Упорядочим Γ так, что $U_i \leqslant U_j$ в точности тогда, когда $U_j \subseteq U_i$. Пусть $\Lambda = \{A_j \mid j \in J\}$ — произвольное вполне упорядоченное подмножество в Γ. Поскольку $D = \bigcap_{j\in J} A_j = \bigcap_{j\in J_0} A_j$ для некоторого конечного подмножества $J_0 \subseteq J$, то $D \neq 0$ и, следовательно, является верхней гранью для Λ в Γ. По лемме Цорна в Γ существует максимальный элемент E. Ясно, что E — простой подмодуль в U.

($\Leftarrow$). Из $\bigcap_{i\in I} A_i = 0$, где A_i — подмодули в M, следует, что $\bigcap_{i\in I} \operatorname{Soc} A_i = 0$. Поскольку $\operatorname{Soc} A_i \subseteq \operatorname{Soc} M$ и $\operatorname{Soc} M$ конечно копорожден, существует конечное подмножество $I_0 \subseteq I$ такое, что $\bigcap_{i\in I_0} \operatorname{Soc} A_i = 0$. Следовательно,

$$0 = \textstyle\bigcap_{i\in I_0} \operatorname{Soc} A_i = \bigcap_{i\in I_0} (A_i \cap \operatorname{Soc} M) = \left(\bigcap_{i\in I_0} A_i\right) \cap \operatorname{Soc} M.$$

Так как $\operatorname{Soc} M$ — существенный подмодуль, то $\bigcap_{i\in I_0} A_i = 0$.

17. Проективные и инъективные модули

17.2. Единственным малым подмодулем свободного $\mathbb{Z}$-модуля служит нулевой подмодуль.

17.6. а) $\Rightarrow$ б). $M_R \cong P/Q$, где P — свободный модуль. Так как R классически полупросто, то M — полупростой модуль. Поэтому $P = Q \oplus A$, где $M \cong A$, т.е. модуль M проективен.

б) $\Rightarrow$ в). Очевидно. в) $\Rightarrow$ а). Пусть I — максимальный правый идеал кольца R. По условию простой модуль R/I является R_R-проективным. Поэтому канонический эпиморфизм $R \to R/I$ расщепляется, I_R — прямое слагаемое модуля R_R. Этого достаточно для классической полупростоты кольца R (теорема 16.4).

17.7. а) $\Rightarrow$ б). Пусть $M \oplus P = Q_R$, где Q — свободный модуль с базисом $\{x_j \,|\, j \in J\}$, и $g_j\colon x_jR \to R_R$ — такие гомоморфизмы, что $g_j(x_j) = 1$. Далее, пусть $\pi\colon Q \to M$ — проекция с ядром P и $\pi_j\colon Q \to x_jR$ — канонические проекции. Обозначим $m_j = \pi(x_j)$, $f_j = g_j\pi_j|M$. Для каждого $m \in M$ существует такое конечное подмножество $F \subseteq J$, что $m = \sum_{j\in F} x_ja_j$. Так как $\sum_{j\in F} m_jf_j(m) = \sum_{j\in F} m_jg_j(x_ja_j) = \sum_{j\in F} m_ja_j = m$, то $\{m_j \,|\, j \in J\}$ и $\{f_j \,|\, j \in J\}$ обладают требуемыми свойствами.

Так как $m = \sum_{j\in F} m_jf_j(m)$ для всех $m \in M$, то множество $\{m_j \,|\, j \in J\}$ порождает M.

б) $\Rightarrow$ а). Пусть Q_R — свободный модуль с базисом $\{x_j \,|\, j \in J\}$, $u_j\colon R_R \to x_jR$ и $\pi\colon Q \to M$ — такие гомоморфизмы, что $u_j(1) = x_j$ и $\pi(x_j) = m_j$ $(j \in J)$. Определим отображение $f\colon Q \to M$ по правилу $f(m) = \sum_{j\in F} u_j(f_j(m)) = \sum_{j\in F} x_jf_j(m)$. Несложно установить, что f — корректно определенный гомоморфизм. Тогда $\pi(f(m)) = \pi\left(\sum_{j\in F} x_jf_j(m)\right) = \sum_{j\in F} m_jf_j(m) = m$, т.е. $\pi f = 1_M$, значит, π расщепляется. Следовательно, M изоморфен прямому слагаемому свободного модуля Q. Поэтому M — проективный модуль. Аналогично доказывается импликация в) $\Rightarrow$ а). Импликация а) $\Rightarrow$ в) проверяется непосредственно.

17.8. Пусть $f\colon M_1 \to M_2$ — заданный изоморфизм. Так как P_1 — проективный модуль и h_2 является эпиморфизмом, то существует такой гомоморфизм $u\colon P_1 \to P_2$, что $h_2u = fh_1$. Откуда $u(P_1) + Q_2 = P_2$ и $u^{-1}(Q_2) = Q_1$. Пусть гомоморфизм $\varphi\colon P_1 \oplus Q_2 \to P_2$ задается правилом $\varphi(p_1 + q_2) = u(p_1) - q_2$. Так как P_2 — проективный модуль, то φ расщепляется: $P_1 \oplus Q_2 \cong P_2 \oplus \operatorname{Ker}\varphi$. Пусть $K = \{q_1 + u(q_1) \,|\, q_1 \in Q_1\} \subseteq Q_1 \oplus Q_2$. Тогда $K \cong Q_1$. Достаточно показать, что $\operatorname{Ker}\varphi = K$. Так как $\varphi(q_1 + u(q_1)) = u(q_1) - u(q_1) = 0$, то $K \subseteq \operatorname{Ker}\varphi$. Если $p_1 + q_2 \in \operatorname{Ker}\varphi$, то $q_2 = u(p_1)$ и $p_1 \in u^{-1}(Q_2) = Q_1$. Откуда $\operatorname{Ker}\varphi \subseteq K$.

17.9. 1) Так как Q — проективный модуль, то существует такой гомоморфизм $h\colon Q \to P$, что $g = fh$. Тогда $h(Q) + \operatorname{Ker} f = P$, откуда $h(Q) = P$. Поэтому h расщепляется и $Q = \operatorname{Ker} h \oplus \overline{P}$.

2) По 1) существуют такие расщепляющиеся эпиморфизмы $h_1\colon P_2 \to P_1$ и $h_2\colon P_1 \to P_2$, что $f_2 = f_1h_1$, $f_1 = f_2h_2$, $P_2 = \operatorname{Ker} h_1 \oplus \overline{P}_1$ и $P_1 = \operatorname{Ker} h_2 \oplus \overline{P}_2$. Поэтому $f_2 = f_2h_2h_1$ и $(1 - h_2h_1)(P_2) \subseteq \operatorname{Ker} f_2$. Следовательно, $(1 - h_2h_1)(P_2)$ — малый подмодуль в P_2. Кроме того, $\operatorname{Ker} h_1 = (1 - h_2h_1)(\operatorname{Ker} h_1) \subseteq (1 - h_2h_1)(P_2)$. Значит, $\operatorname{Ker} h_1$ — малое прямое слагаемое в P_2. Поэтому $\operatorname{Ker} h_1 = 0$, h_1 — изоморфизм и $h_2h_1 = 1$. Аналогично, h_2 — изоморфизм и $h_1h_2 = 1$.

17.10. 1) Пусть $n \in \mathbb{N}$ — такое, что N^n содержит свободный циклический подмодуль F. Тогда M — F-проективный модуль, а, следовательно, M проективен относительно всех конечно порожденных свободных R-модулей. Но каждый конечно порожденный модуль является гомоморфным образом конечно порожденного проективного (свободного) модуля. Поэтому M проективен и относительно этих гомоморфных образов.

Пусть M конечно порожден. Тогда существует эпиморфизм $h\colon N \to M$, где N — конечно порожденный свободный модуль. Модуль M является N-проективным. Поэтому M изоморфен прямому слагаемому модуля N и, значит, M проективен.

2) следует из 1).

17.12. 1) Пусть I — множество всех порядковых чисел, меньших α. Для каждого $\beta \leqslant \alpha$ положим $M_{(\beta)} = \bigoplus\limits_{i<\beta} M_i$. При естественном отображении модуля $M_{(\beta+1)} = M_{(\beta)} + M_\beta$ на M_β образом модуля $N \cap M_{(\beta+1)}$ является некоторый проективный подмодуль N_β модуля M_β, откуда N_β изоморфен прямому слагаемому модуля $N \cap M_{(\beta+1)}$, $N \cap M_{(\beta+1)} = (N \cap M_{(\beta)}) \oplus N'_\beta$, где $N'_\beta \cong N_\beta$. Покажем, что $N \cap M_{(i)} = \bigoplus\limits_{j<i} N'_j$ для всех $i \leqslant \alpha$. Это равенство очевидно для $i = 0$. Из его справедливости для $i = \beta$ в силу сказанного выше следует справедливость при $i = \beta + 1$. Пусть теперь β — предельное порядковое число, и пусть утверждение имеет место для всех $i < \beta$. Тогда

$$N \cap M_{(\beta)} = N \cap \Big(\bigcup_{i<\beta} M(i)\Big) = \bigcup_{i<\beta} (N \cap M(i)) = \bigcup_{i<\beta} \Big(\bigoplus_{j<i} N'_j\Big) = \bigoplus_{j<\beta} N'_j.$$

2) следует из 1).

17.16. Пусть $F \in \mathcal{E}$. Непосредственно проверяется, что M инъективен относительно любого подмодуля модуля F. Допустим, что $\pi\colon F \to \overline{F}$ является эпиморфизмом, $\overline{G} \in L\left(\overline{F}\right)$, $\overline{g} \in \operatorname{Hom}\left(\overline{G}, M\right)$. Положим $N = \pi^{-1}\left(\overline{G}\right) \in L(F)$, $\pi_1 = \pi \,|\, N$. По условию гомоморфизм $\overline{g}\pi_1\colon N \to M$ продолжается до некоторого гомоморфизма $f\colon F \to M$. Так как $\operatorname{Ker}\pi \subseteq \pi^{-1}(\overline{G}) = N$, то $\operatorname{Ker}\pi \subseteq \operatorname{Ker} f$. Значит, f продолжается до некоторого гомоморфизма $\overline{f}\colon \overline{F} \to M$. Поэтому M — $\overline{F}$-инъективный модуль.

Пусть $D = \bigoplus\limits_{j\in J} F_j$, где $F_j \in \mathcal{E}$, $D_1 \in L(D)$, $d_1 \in \operatorname{Hom}(D_1, M)$, E — множество всех пар (L, d_L), где L — подмодуль модуля D, содержащий D_1, а d_L — гомоморфизм из L в M, продолжающий d_1. Определим отношение $\leqslant$ на E следующим образом: $(L, d_L) \leqslant (Q, d_Q)$ в точности тогда, когда $L \subseteq Q$ и d_L продолжается до d_Q. По лемме Цорна в E существует максимальный элемент $\left(\overline{D}, \overline{d}\right)$. Достаточно показать, что $\overline{D} = D$ или, что равносильно, $F_j \subseteq \overline{D}$ для всех $j \in J$. Так как M — F_j-инъективный модуль, то ограничение гомоморфизма $\overline{d}$ на $F_j \cap \overline{D}$ продолжается до некоторого гомоморфизма $d_j\colon F_j \to M$. Пусть $u\colon \left(F_j + \overline{D}\right) \to M$ — такой гомоморфизм, что $u(x + y) = d_j(x) + \overline{d}(y)$ для всех $x \in F_j$ и $y \in \overline{D}$. Этот гомоморфизм определен корректно: если $x + y = 0$, то $x = -y \in F_j \cap \overline{D}$ и $u(x + y) = \overline{d}(-y) + \overline{d}(y) = 0$. По построению $F_j + \overline{D} = \overline{D}$. Поэтому $F_j \subseteq \overline{D}$.

17.19. По 17.16 M — $f(M)$-инъективный модуль и, таким образом, M — квазиинъективный модуль. Так как $f(M)$ —

N-инъективный модуль, то естественное вложение $f(M) \to N$ продолжается до гомоморфизма $g\colon N \to f(M)$. Тогда g — проекция модуля N на $f(M)$. Поэтому $f(M)$ — прямое слагаемое в N.

17.22. 1) ($\Rightarrow$). Для каждого $0 \neq m \in M$ существует изоморфная копия T_m модуля T и гомоморфизм $f_m\colon M \to T_m$ такие, что $f_m(m) \neq 0$. Прямое произведение всех гомоморфизмов f_m является мономорфизмом из M в $\prod_{m\in M} T_m$.

($\Leftarrow$). Пусть $g\colon M \to \prod_{j\in J} T_j$ — такой мономорфизм, что для любого $j \in J$ существует изоморфизм $f_j\colon T_j \to T$. Пусть $h_j\colon \prod_{j\in J} T_j \to T_j$ — естественные проекции. Тогда $(h_j g)(M) \neq 0$ для некоторого $j \in J$. Следовательно, $f_j h_j g\colon M \to T$ — ненулевой гомоморфизм.

2) а) $\Rightarrow$ б). Заметим, что любой ненулевой гомоморфизм из простого модуля является мономорфизмом.

б) $\Rightarrow$ а). Пусть M — модуль, N — его ненулевой циклический подмодуль. Модуль N обладает простым фактормодулем. Поэтому существует ненулевой гомоморфизм $f\colon N \to T$. Так как T — инъективный модуль, то f продолжается до некоторого гомоморфизма $M \to T$.

б) $\Longleftrightarrow$ в). Заметим, что сумма попарно неизоморфных простых подмодулей модуля T является прямой суммой.

17.24. 1) проверяется непосредственно. 2) Пусть Γ — множество всех существенных расширений модуля N в M. Очевидно, что $\Gamma \neq \varnothing$, удовлетворяет лемме Цорна и поэтому содержит максимальный элемент H. Ясно, что H — замыкание N в M.

3) Существует $H \in L(M)$ такой, что $N \subseteq H$, $G \cap H = 0$, M — существенное расширение модуля $G \oplus H$ и $G \cap K \neq 0$ для любого подмодуля K модуля M, строго содержащего H. Допустим, что $K \in L(M)$ и K — существенное расширение модуля H, строго содержащее H. Тогда $G \cap K \neq 0$. Так как K — существенное расширение H, то $(G \cap K) \cap H = G \cap H \neq 0$. Полученное противоречие показывает, что H — замкнутый подмодуль в M.

4) есть следствие 3).

5) По 3) существует такой замкнутый подмодуль M_2 модуля M, что $N_2 \subseteq M_2$, $N_1 \cap M_2 = 0$, M — существенное расширение модуля $N_1 \oplus M_2$ и $N_1 \cap K \neq 0$ для любого подмодуля K модуля M, строго содержащего M_2. По 2) N_1 обладает замыканием M_1 в M. Так как M_1 — существенное расширение модуля N_1 и $N_1 \cap M_2 = 0$, то $M_1 \cap M_2 = 0$. Существенность $N_1 \oplus M_2$ в M влечет существенность $M_1 \oplus M_2$.

6) Так как $N \cap H = 0$, то по 3) существует замкнутое дополнение H_1 к N, содержащее дополнение H к N. Поэтому $H = H_1$ — замкнутый подмодуль в M. Так как G — существенное расширение N и $N \cap H = 0$, то $H \cap G = 0$. Кроме того, M — существенное расширение $H \oplus G$. Непосредственно проверяется, что $H \cap T \neq 0$ для любого $T \in L(M)$, строго содержащего G. Поэтому G — дополнение к H.

7) следует из 6) и из того, что каждый замкнутый подмодуль совпадает со своим замыканием.

17.25. а) $\Rightarrow$ в). Существуют такие замкнутые подмодули M_1 и M_2 модуля M, что $N_1 \subseteq M_1$, $N_2 \subseteq M_2$, $M_1 \cap M_2 = 0$, M — существенное расширение модуля $M_1 \oplus M_2$ и $M_1 \cap K \neq 0$ для любого $K \in L(M)$, строго содержащего M_2. Пусть $\overline{M} = M_1 \oplus M_2$, $\overline{f}\colon \overline{M} \to M_1$ — проекция с ядром M_2. По условию существует $f \in \operatorname{End} M$, совпадающий с $\overline{f}$ на $\overline{M}$. Поэтому $M_1 \subseteq f(M)$, $M_2 \subseteq \operatorname{Ker} f$. Кроме того, $M_2 \subseteq f^{-1}(M_2)$. Поэтому $M_2 = f^{-1}(M_2)$, поскольку в противном случае $M_1 \cap f^{-1}(M_2) \neq 0$. Допустим, что $f(M)$ строго содержит M_1. Тогда существует ненулевой элемент $f(m) \in M_2 \cap f(M)$. Поэтому $m \in f^{-1}(M_2) = M_2$ и $f(m) = 0$, противоречие. Следовательно, $f(M) = M$ и $M_2 = \operatorname{Ker} f$, $f = f^2$. Поэтому $M = M_1 \oplus M_2$.

в) $\Rightarrow$ г). Существуют такие замкнутые подмодули $\overline{M}_1$ и $\overline{M}_2$ модуля M, что $Q_1 \subseteq \overline{M}_1$, $Q_2 \subseteq \overline{M}_2$, $\overline{M}_1 \cap \overline{M}_2 = 0$, M — существенное расширение модуля $\overline{M}_1 \oplus \overline{M}_2$ и $\overline{M}_1 \cap K \neq 0$ для любого $K \in L(M)$, строго содержащего $\overline{M}_2$. По б) существует такое прямое разложение $M = M_1 \oplus M_2$, что $\overline{M}_1 \subseteq M_1$ и $\overline{M}_2 \subseteq M_2$. Допустим, что M_2 строго содержит $\overline{M}_2$. Тогда $0 \neq \overline{M}_1 \cap M_2 \subseteq M_1 \cap M_2$, противоречие. Следовательно, $M_2 = \overline{M}_2$. Докажем, что $M_1 = \overline{M}_1$. Достаточно показать, что M_1 — существенное расширение модуля $\overline{M}_1$. Допустим противное. Тогда существует такой $0 \neq T \in L(M_1)$, что $T \cap \overline{M}_1 = 0$. Так как M — существенное расширение модуля $\overline{M}_1 \oplus M_2$, то существует такой ненулевой элемент $t = \overline{m}_1 + m_2$, что $\overline{m}_1 \in \overline{M}_1$, $m_2 \in M_2$. Откуда $m_2 = t - \overline{m}_1 \in M_1 \cap M_2 = 0$ и, значит, $t = \overline{m}_1 \in T \cap M_1 = 0$, противоречие.

г) $\Rightarrow$ б). Пусть f — идемпотентный эндоморфизм модуля $N \in L(M)$, $N_1 = f(N)$, $N_2 = (1_N - f)(N)$. Тогда $N_1 \cap N_2 = 0$. Существуют такие замкнутые подмодули Q_1 и Q_2 модуля M, что $N_1 \subseteq Q_1$, $N_2 \subseteq Q_2$, $Q_1 \cap Q_2 = 0$, и M — существенное расширение модуля $Q_1 \oplus Q_2$. По условию $M = Q_1 \oplus Q_2$. Пусть $g\colon M \to Q_1$ — проекция с ядром Q_2, g — требуемое продолжение f.

17.35. Импликации б) $\Rightarrow$ в) и в) $\Rightarrow$ г) очевидны.

г) $\Rightarrow$ в). Пусть M_R — счетная прямая сумма инъективных модулей, Q — инъективная оболочка R_R. Тогда по условию $Q \oplus M$ — π-инъективный модуль и, значит, M — Q-инъективный модуль (убедитесь в этом). Поэтому, если I — правый идеал в R, то всякий гомоморфизм $I \to M$ продолжается до гомоморфизма $Q \to M$, в частности, до $R_R \to M_R$. По критерию Бэра M — инъективный модуль.

в) $\Rightarrow$ а). Пусть $B_1 \subseteq B_2 \subseteq \ldots$ — цепь правых идеалов кольца R, E_i — инъективная оболочка для R_R/B_i, $B = \bigcup_{i=1}^{\infty} B_i$, $M = \oplus_{i=1}^{\infty} E_i$, $f_i\colon B \to E_i$ — такие гомоморфизмы, что $f_i(x) = x + B_i$, $i = 1, 2, \ldots$. Пусть f — прямая сумма гомоморфизмов f_i, $f\colon B \to M$. Так как по условию M — инъективный модуль, то по критерию Бэра существует такое $m \in M$, что $f(b) = mb$ для всех $b \in B$. Поэтому существует такое n, что $mR \subseteq \sum_{i=1}^{n} E_i$, откуда $B_i = B_n$ для всех $i > n$.

а) $\Rightarrow$ б). Пусть M — прямая сумма инъективных правых R-модулей M_j ($j \in J$), B — правый идеал кольца R, $f \in \operatorname{Hom}(B_R, M)$. Так как $f(B)$ — конечно порожденный модуль, то $f(B)$ содержится в $N = \oplus_{k\in K} M_k$ для некоторого конечного подмножества $K \subseteq J$. Тогда N — инъективный модуль, поэтому f продолжается до гомоморфизма $g\colon R_R \to M$. По критерию Бэра M — инъективный модуль.

17.39. Пусть $h\colon M \to \overline{M}$ — эпиморфизм, B — конечно порожденный правый идеал кольца R, $\overline{f}\colon B_R \to \overline{M}$ — гомоморфизм. По условию B_R — проективный модуль. Поэтому существует такой гомоморфизм $f\colon B_R \to M$, что $\overline{f} = hf$. Так как M —

конечно инъективный модуль, то f продолжается до гомоморфизма $g\colon R_R \to M$. Пусть $\overline{g} = hg \in \operatorname{Hom}\left(R_R, \overline{M}\right)$. Так как $\overline{g}$ — продолжение $\overline{f}$, то $\overline{M}$ — конечно инъективный модуль.

17.40. б) $\Rightarrow$ в). Допустим, что R содержит бесконечную цепь $B_1 \subset B_2 \subset \ldots$ правых M-аннуляторов. Если $N_i = \{m \in M \,|\, mB_i = 0\}$, то $N_1 \supset N_2 \supset \ldots$ — бесконечная цепь подмодулей модуля M. Пусть $x_i \in N_i \backslash N_{i+1}$, $B = \bigcup_{i=1}^{\infty} B_i$. Для каждого $b \in B$ существует такое n, что $x_{n+j}b = 0$ для всех $j \geqslant 1$. Поэтому правилом $f(b) = (x_1 b, x_2 b, \ldots)$ задается гомоморфизм $f\colon B_R \to \oplus_{\aleph_0} M$ в инъективный модуль $\oplus_{\aleph_0} M$. По критерию Бэра существует $y = (y_1, \ldots, y_n, 0, \ldots) \in \oplus_{\aleph_0} M$ такой, что $(x_1 b, x_2 b, \ldots) = f(b) = yb = (y_1 b, \ldots, y_n b, 0, \ldots)$. Получено противоречие, поскольку $x_{n+1} \notin N_{n+2}$.

в) $\Rightarrow$ а). Пусть B — правый идеал кольца R, $f \in \operatorname{Hom}(B_R, \oplus_{|I|} M)$. Так как $\oplus_{|I|} M$ — подмодуль инъективного модуля M^I, то по критерию Бэра существует $x = (x_i)_{i\in I} \in M^I$ такой, что $f(b) = xb$ для всех $b \in B$. Для любого подмножества $J \subseteq I$ через x_J обозначим такое $(y_i)_{i\in I} \in M^I$, что $y_i = x_i$ при $i \in J$ и $y_i = 0$ при $i \in I\backslash J$. Рассмотрим множество $\mathcal{E} = \{r\left(x_{I\backslash F}\right) \,|\, F$ — конечное подмножество в $I\}$. Из условия следует, что $\mathcal{E}$ содержит максимальный элемент $r\left(x_{I\backslash G}\right)$. Если F — конечное подмножество в I, содержащее G, то $r\left(x_{I\backslash G}\right) = r\left(x_{I\backslash F}\right)$. Пусть $b \in B$, $f(b) = (z_i)_{i\in I} \in M^I$. Так как $f(b) \in \oplus_{|I|} M$, то существует такое конечное подмножество $F(b)$ множества I, что $G \subseteq F(b)$ и $z_i = 0$ при $i \in I\backslash F(b)$. Поэтому $b \in r\left(x_{I\backslash F(b)}\right) = r\left(x_{I\backslash G}\right)$. Следовательно, $f(b) = xb - x_{I\backslash G}b = x_G b$. Так как b — произвольный элемент из B и $x_G \in \oplus_{|I|} M$, то по критерию Бэра $\oplus_{|I|} M$ — инъективный модуль.

17.43. а) $\Rightarrow$ б). Пусть $0 \neq U \subseteq Q$ и $Q(U) \subseteq Q$ — инъективная оболочка модуля U. Тогда $Q(U)$ — прямое слагаемое в Q. Откуда $Q(U) = Q$.

б) $\Rightarrow$ в). Пусть $M \subseteq Q$ и $0 \neq A, B \subseteq M$. Так как Q — инъективная оболочка для A, то A — существенный подмодуль в Q. Значит, $A \cap B \neq 0$.

в) $\Rightarrow$ г). В качестве равномерного подмодуля можно взять сам Q.

г) $\Rightarrow$ а). Пусть Q — инъективная оболочка своего равномерного подмодуля M. Допустим, что $Q = A \oplus B$, где $A, B \neq 0$. Так как M — существенный подмодуль в Q, то $0 \neq M \cap A, M \cap B$. Из однородности M следует, что $0 \neq (M \cap A) \cap (M \cap B) \subseteq A \cap B = 0$, противоречие.

17.46. а) $\Rightarrow$ б). Артиновость справа кольца R влечет его нетеровость. Поэтому по 17.42 в) Q_R является прямой суммой неразложимых модулей, каждый из которых по 17.44 есть инъективная оболочка простого модуля.

б) $\Rightarrow$ а). Достаточно показать, что каждый фактормодуль $M = R/A$ модуля R_R удовлетворяет условию 17.45. Пусть $Q(R/A)$ — инъективная оболочка R/A, $Q(R/A) = \oplus_{i\in I} Q_i$, где Q_i — инъективные оболочки простых модулей. Цикличность модуля R/A влечет, что он содержится в некоторой конечной сумме $\oplus_{i\in I_0} Q_i$, откуда $I = I_0$.

17.47. 1) Из 15.80 вытекает, что малость подмодуля $S\alpha$ в ${}_S S$ равносильна включению $\alpha \in J(S)$. Здесь инъективность Q не потребовалась.

Докажем, что $\operatorname{Ker}\alpha$ — существенный подмодуль в Q для любого $\alpha \in J(S)$. Пусть $U \subseteq Q_R$ и $\operatorname{Ker}\alpha \cap U = 0$. Тогда $\alpha_0 = \alpha \,|\, U$ — мономорфизм. Существует $\beta \in \operatorname{End} Q_R$ со свойством $\beta\alpha_0 = \rho$, где $\rho\colon U \to Q$ — вложение. Тогда $U \subseteq \operatorname{Ker}(1 - \beta\alpha)$. Так как $\beta\alpha \in J(S)$, то $1 - \beta\alpha$ обратим. Значит, $\operatorname{Ker}(1 - \beta\alpha) = 0$, поэтому $U = 0$.

Докажем, что $S\alpha$ — малый подмодуль в ${}_S S$, если $\operatorname{Ker}\alpha$ — существенный подмодуль в Q. Пусть $S\alpha + \Gamma = S$, где $\Gamma \subseteq {}_S S$. Существуют такие $\sigma \in S$, $\gamma \in \Gamma$, что $\sigma\alpha + \gamma = 1$. Тогда $\operatorname{Ker}\alpha \cap \operatorname{Ker}\gamma = 0$. Поэтому $\operatorname{Ker}\gamma = 0$, откуда $1_Q = \delta\gamma$ для некоторого $\delta \in \operatorname{End} Q_R$ и, значит, $\Gamma = S$.

2) Опять первая эквивалентность следует из 15.80.

Допустим, что $\alpha \in J(S)$. Пусть $U \subseteq P_R$, $\operatorname{Im}\alpha + U = P$ и $\nu\colon P \to P/U$ — канонический эпиморфизм. Тогда $\nu\alpha$ — эпиморфизм. Поэтому $\nu = \nu\alpha\beta$ для некоторого $\beta \in \operatorname{End} P_R$. Тогда $\nu(1 - \alpha\beta) = 0$, т.е. $\operatorname{Im}(1 - \alpha\beta) \subseteq U$. Так как $\alpha \in J(S)$, то $\alpha\beta \in J(S)$. Следовательно, $1 - \alpha\beta$ обратим. Откуда $P = \operatorname{Im}(1 - \alpha\beta) \subseteq U$, т.е. $U = P$. Поэтому $\operatorname{Im}\alpha$ мал в P.

Допустим, что $\operatorname{Im}\alpha$ мал. Пусть $\alpha S + \Gamma = S_S$. Тогда $\alpha\sigma + \gamma = 1$ для некоторых $\sigma \in S$, $\gamma \in \Gamma$. Поэтому $\operatorname{Im}\alpha + \operatorname{Im}\gamma = P$ и, значит, $\operatorname{Im}\gamma = P$, т.е. γ — эпиморфизм. Следовательно, $1_P = \gamma\delta$ для некоторого $\beta \in \operatorname{End} P_R$. Откуда $\Gamma = S$. Поэтому αS мал в S_S.

17.49. Согласно 17.7 для $u \in J(P)$ существуют такие $y_i \in P$ и $\varphi_i \in \operatorname{Hom}_R(P, R)$, что $u = \sum y_i \varphi_i(u)$. Так как $\varphi_i(u) \in J(R)$, то $u \in PJ(R)$.

18. Тензорное произведение, плоские и регулярные модули

18.4. а) Если $a \in I$ и $\overline{r} \in R/I$, то $(\rho \otimes 1_{R/I})(a \otimes \overline{r}) = a \otimes \overline{r} = 1 \cdot a \otimes \overline{r} = 1 \otimes \overline{ar} = 1 \otimes \overline{0} = 0$.

б) Пусть $a \in I$, обозначим $\overline{a} = a + I^2$. Так как отображение $I \times R/I \ni (a, \overline{r}) \mapsto \overline{ar} \in I/I^2$ R-сбалансировано и сюръективно, то существует эпиморфизм $\lambda\colon I \otimes_R R/I \to I/I^2$ со свойством $\lambda(a \otimes r) = \overline{ar}$. Пусть

$$\sum\nolimits_{i=1}^{n} a_i \otimes \overline{r}_i = \sum\nolimits_{i=1}^{n} a_i r_i \otimes \overline{1} = \left(\sum\nolimits_{i=1}^{n} a_i r_i\right) \otimes \overline{1} \in \operatorname{Ker}\lambda,$$

следовательно, $\sum_{i=1}^{n} a_i r_i \in I^2$, т.е. $\sum_{i=1}^{n} a_i r_i = \sum_{j=1}^{k} a'_j a''_j$, $a'_j, a''_j \in I$. Тогда

$$\left(\sum\nolimits_{i=1}^{n} a_i r_i\right) \otimes \overline{1} = \sum\nolimits_{j=1}^{k} a'_j \otimes a''_j = \sum\nolimits_{j=1}^{k} a'_j \otimes \overline{0} = 0.$$

18.5. б) Достаточно проверить, что $(\bigoplus_i A_i) \otimes B \cong \bigoplus_i (A_i \otimes B)$. Если π_i — проекции, связанные с заданным прямым разложением группы $A = \bigoplus_i A_i$, то функция $g(a, b) = \sum_i (\pi_i a \otimes b)$ является билинейной $g\colon A \times B \to G = \bigoplus_i (A_i \otimes B)$, причем $\pi_i a \otimes b \in A_i \otimes B$.

Поэтому существует однозначно определенный эпиморфизм $\varphi\colon A\otimes B\to G$, для которого $g(a,\,b)=\varphi e(a,\,b)$, где e — тензорное отображение $A\times B\to A\otimes B$. Функция $e(\pi_i a,\,b)$, определенная на $A_i\times B$, является билинейной, поэтому для каждого i существует гомоморфизм $\psi_i\colon A_i\otimes B\to A\otimes B$, для которого $\psi_i(\pi_i a\otimes b)=e(\pi_i a,\,b)$. Гомоморфизмы ψ_i дают гомоморфизм $\psi\colon G\to A\otimes B$, для которого

$$\psi g\,(a,\,b)=\psi\sum_i(\pi_i a\otimes b)=\sum_i\psi_i(\pi_i a\otimes b)=\sum_i e(\pi_i a\otimes b)=e(a,\,b).$$

Следовательно, отображение ψ обратно отображению φ, т.е. φ — изоморфизм.

18.7. Пусть $\alpha\colon A_R\to B_R$ — мономорфизм и $\sum a_i\otimes m_i\in\operatorname{Ker}(\alpha\otimes 1_M)$. Тогда согласно 18.6 существует конечно порожденный подмодуль $M_0\subseteq M$, для которого $\sum a_i\otimes m_i\in\operatorname{Ker}(\alpha\otimes 1_{M_0})$. Пусть $M_0\subseteq M_1\subseteq M$ и M_1 плосок. Согласно 18.6 б) $\sum a_i\otimes m_i\in\operatorname{Ker}(\alpha\otimes 1_{M_1})$. Тогда $\sum a_i\otimes m_i=0\ \in A\otimes_R M_1$, откуда $\sum a_i\otimes m_i=0\ \in A\otimes_R M$.

18.12. Очевидно, $\widehat{f}$ сопоставляет элементу $a\in A$ отображение $\widehat{f}(a)\colon B\to C$, которое переводит элемент $b\in B$ в элемент $f(a\otimes b)\in C$. Проверьте, что $\widehat{f}(a)$, $\widehat{f}$ и $\Phi\colon f\mapsto\widehat{f}$ — гомоморфизмы. Осталось проверить, что Φ — изоморфизм. Пусть $\chi\colon A_R\to\operatorname{Hom}_S(B,\,C)$ — гомоморфизм. Тогда $(a,\,b)\mapsto(\chi a)(b)$ есть билинейная функция. Поэтому существует однозначно определенный гомоморфизм $f\colon A\otimes B\to C$ со свойством $f(a\otimes b)\mapsto(\chi a)(b)$. Отображение $\Psi\colon\chi\mapsto f$ является обратным к Φ.

18.21. а) $\Rightarrow$ б). Если $u=\sum a_i m_i\in U\cap IM$, то для $t=\sum a_i\otimes\overline{m}_i\in I\otimes_R(M/U)$ имеем $\left(\rho\otimes 1_{M/U}\right)t=\sum a_i\otimes\overline{m}_i=1\otimes\overline{u}=0\in R\otimes_R(M/U)$. Поэтому $t=0$. Соответствие $I\times(M/U)\ni(a,\overline{m})\mapsto\overline{am}=am+IU\in IM/IU$ задает R-сбалансированное отображение, которое индуцирует гомоморфизм $\lambda\colon I\otimes_R(M/U)\to IM/IU$. Поскольку $t=0$, то $0=\lambda(0)=\lambda(t)=\sum\overline{a_i m_i}=\overline{u}$, откуда $u\in IU$.

б) $\Rightarrow$ а). Пусть для $t=\sum a_i\otimes\overline{m}_i\in I\otimes_R(M/U)$ имеем $\left(\rho\otimes 1_{M/U}\right)t=\sum a_i\otimes\overline{m}_i=1\otimes\sum\overline{a_i m_i}=0$, т.е. $\sum a_i m_i\in U$. Значит, $\sum a_i m_i=\sum a'_j u_j\in IU$, где $u_j\in U$. Тогда $\sum a_i\otimes m_i-\sum a'_j\otimes u_j\in\operatorname{Ker}(\rho\otimes 1_M)$. Так как M плосок, то $\sum a_i\otimes m_i=\sum a'_j\otimes u_j$. Следовательно, для $\gamma\colon M\to M/U$ имеем $t=(1_I\otimes\gamma)\left(\sum a_i\otimes m_i\right)=\sum a_i\otimes\overline{m}_i=(1_I\otimes\gamma)\left(\sum a'_j\otimes u_j\right)=\sum a'_j\otimes u_j=0$. Следовательно, $\rho\otimes 1_{\overline{M}}$ — мономорфизм.

18.23. Докажем этот результат сначала для свободного модуля ${}_RF$. Пусть $\{x_i\,|\,i\in I\}$ — базис F. Если $u=\sum a_i x_i\in U$, $a_i\in R$, то обозначим через $I=\sum a_i R$ правый идеал, порожденный коэффициентами a_i в представлении элемента u. Так как идеал I конечно порожден, то по 18.22 $U\cap IF=IU$. Откуда $u=\sum b_j u_j$, где $b_j\in I$, $u_j\in U$. Так как $u\in J(F)=J(R)F$ (17.49), то $u_j=\sum c_{jk}x_k$, где $c_{jk}\in J(R)$. Тогда $u=\sum_i a_i x_i=\sum_j\sum_k b_j c_{jk}x_k$. Откуда $a_i=\sum_j b_j c_{ji}\in IJ(R)$, т.е. $I\subseteq IJ(R)$. Следовательно, $I=IJ(R)$. Так как идеал I конечно порожден, то $I=0$ (15.82). Значит, $U=0$.

Пусть теперь P — прямое слагаемое свободного модуля F, $F=P\oplus P_1$. Если $\nu\colon F\to F/U$ — канонический эпиморфизм, то $F/U=\nu(F)=\nu(P)\oplus\nu(P_1)$, $F/U\cong P/U\oplus P_1$. Так как P/U и P_1 — плоские модули, то F/U также плосок. Как было показано, $U=0$.

18.27. ($\Rightarrow$). Индукцией по числу n образующих подмодуля. Допустим, что любой подмодуль с числом образующих $<n$ является прямым слагаемым в M. Пусть $F=G+L$ — n-порожденный подмодуль модуля M, где G — $(n-1)$-порожденный, а L — циклический подмодуль в M. Тогда $M=G\oplus H$. Следовательно, $F=F\cap(G\oplus H)=G\oplus T$, где $T=F\cap H$. Так как $T\cong F/G\cong L/(G\cap L)$, то T — циклический модуль. Поэтому существует прямое разложение $M=T\oplus U$. Поскольку $T\subseteq H$, то $H=T\oplus W$, где $W=H\cap U$. Откуда $M=G\oplus H=G\oplus T\oplus W=F\oplus W$.

18.28. Импликации а) $\Rightarrow$ б) $\Rightarrow$ в) $\Rightarrow$ а) и эквивалентность в) $\Longleftrightarrow$ г) проверяются непосредственно.

б) $\Rightarrow$ д). $f(M)=e_1(M)$ и $\operatorname{Ker}f=(1-e_2)(M)$.

д) $\Rightarrow$ а). Допустим, что $M=\operatorname{Ker}f\oplus N=f(M)\oplus L$. Пусть $t=f|N$. Тогда $t(N)=f(M)$. Следовательно, t — мономорфизм. Возьмем такое $g\in S$, что $g(x+y)=t^{-1}(x)$ для всех $x\in f(M)$ и $y\in L$. Тогда $f=fgf$.

18.29. б) $\Rightarrow$ в). Условие $f=gf^2$ влечет $\operatorname{Im}f\cap\operatorname{Ker}f=0$. Так как $a-fg(a)\in\operatorname{Ker}f$, то $a\in\operatorname{Im}f+\operatorname{Ker}f$ для любого $a\in M$, т. е. $M=\operatorname{Im}f\oplus\operatorname{Ker}f$.

в) $\Rightarrow$ а). Если $M=\operatorname{Im}f\oplus\operatorname{Ker}f$, то f индуцирует на $\operatorname{Im}f$ мономорфизм, который должен быть автоморфизмом, так как $f(M)=f(f(M))$. Пусть $g\in S$ обратен к $f\,|\,f(M)$ на $f(M)$ и аннулирует $\operatorname{Ker}f$. Тогда если $M\ni a=x+y$, где $x\in\operatorname{Im}f$, $y\in\operatorname{Ker}f$, то $f(a)=f(x)=fgf(x)=fgf(a)$ и $fg(a)=fg(x)=x=gf(x)=gf(a)$, т. е. $f=fgf$ и $fg=gf$.

18.31. Эквивалентность а) $\Longleftrightarrow$ б) следует из 18.28.

в) $\Rightarrow$ г) следует из того, что $fS\cap vS$ — прямое слагаемое модуля vS.

г) $\Rightarrow$ а). Пусть $f\in S$, $v=1_M-f$. Так как $fS+vS=S$, то fS — прямое слагаемое модуля S_S. По 18.28 S — регулярное кольцо.

а) $\Rightarrow$ в). По 18.28 S_S — регулярный модуль. Поэтому конечно порожденный правый идеал $X+Y$ кольца S является циклическим прямым слагаемым модуля S_S. Поскольку отображение $f(x,y)=x-y$ задает эпиморфизм $f\colon X\oplus Y\to X+Y$ с ядром $X\cap Y$, то $X\cap Y$ изоморфен прямому слагаемому модуля $X+Y$. Следовательно, $X\cap Y$ — циклический подмодуль модуля S_S.

18.34. Пусть $\alpha\in S$ и U — д.п. для $\operatorname{Ker}\alpha$ в Q. Тогда $\operatorname{Ker}\alpha+U$ — существенный подмодуль в Q и $\alpha_0=\alpha\,|\,U$ — мономорфизм. Если $\rho\colon U\to Q$ — вложение, то существует такой $\gamma\in S$, что $\rho=\gamma\alpha_0$. Откуда $\operatorname{Ker}\alpha+U\subseteq\operatorname{Ker}(\alpha\gamma\alpha-\alpha)$. Осталось заметить, что $\alpha\gamma\alpha-\alpha\in J(S)$ (17.47).

18.37. а) Если $a=aca$, то в качестве b можно взять cac.

б) Пусть $a\in Z(R)$ и $a=a^2b$, $b=b^2a$ (см. а)). Так как идемпотент ba является центральным, то $bx=b^2ax=bxba=baxb=xbab=xb$ для любого $x\in R$.

в) $b \in bRb$ для любого $b \in I$.

18.38. 3) ($\Rightarrow$). Пусть $a = aba$ и $c = cdc$. Имеем $ac = a(bacd)c = a(bacd)u(bacd)c$ для некоторого $u \in R$. Откуда $ac = ac(dub)ac$.

($\Leftarrow$). Очевидно, поскольку каждый идемпотент является регулярным элементом.

18.39. 1) ($\Rightarrow$). Так как S — строго регулярное кольцо, то $f = eu$, где e — центральный идемпотент кольца S, u — автоморфизм модуля M. Тогда $f(M) = e(M)$ и $\operatorname{Ker} f = \operatorname{Ker} e = (1-e)(M)$. Поэтому $M = f(M) \oplus \operatorname{Ker} f$.

($\Leftarrow$). Если $f \in S$, $g = f \,|\, f(M)$, то g — автоморфизм модуля $f(M)$. Для $m \in M$ по условию существуют такие $x \in M$ и $y \in \operatorname{Ker} f$, что $m = f(x) + y$. Тогда $f(m) = f^2(x)$ и $f(M) = f^2(M)$. Пусть $h \in \operatorname{End} M$ — такой, что $h(w+z) = g^{-1}(w)$ для $w \in f(M)$, $z \in \operatorname{Ker} f$. Тогда $f = f^2h$. Поэтому S — строго регулярное кольцо.

2) следует из 1).

3) Пусть $M = B \oplus G = N \oplus F$ и $e_1 \colon M \to B$, $e_2 \colon M \to N$ — соответствующие проекции. Тогда $G + N = G \oplus (B \cap (G+N))$. Поэтому справедливость данного утверждения вытекает из равенств $B \cap (G+N) = \operatorname{Im}(e_1e_2)$ и $(G \cap N) \oplus F = \operatorname{Ker}(e_1e_2)$. Докажем, например, первое равенство. Пусть $b = g + n$, где $b \in B$, $g \in G$, $n \in N$. Тогда $n = b - g$ и $b = e_1(n) \in e_1(\operatorname{Im} e_2) = \operatorname{Im}(e_1e_2)$, т.е. $B \cap (G+N) \subseteq \operatorname{Im}(e_1e_2)$. Пусть теперь $x \in \operatorname{Im}(e_1e_2) = e_1(N)$, $x = e_1(n)$, $n \in N$. Если $n = b + g$, где $b \in B$, $g \in G$, то $e_1(n) = b$ и $x = b = n - g \in (G+N) \cap B$, значит, $\operatorname{Im}(e_1e_2) \subseteq (G+N) \cap B$.

4) вытекает из 3) и 18.38 3).

5) Вытекает из того факта, что согласно 15.93 в этом случае все идемпотенты кольца S центральны.

($\Leftarrow$). Пусть $M = B \oplus C = N \oplus F$ и $\alpha \colon M \to B$, $\beta \colon M \to N$ — проекции. Если $M \ni a = n + f$, $n = b + c$, где $n \in N$, $f \in F$, $b \in B$, $c \in C$, то из условия следует, что $b \in N$. Имеем $(\alpha\beta)^2(a) = \alpha\beta\alpha(n) = \alpha\beta(b) = \alpha(b) = \alpha(n) = \alpha\beta(a)$. Итак, $(\alpha\beta)^2 = \alpha\beta$.

18.41. а) Проверяется непосредственно. б) Пусть H — циклический подмодуль модуля P. Тогда H — прямое слагаемое в M. Поэтому $f(H) = g(H) \subseteq P$ для некоторого $g \in \operatorname{End} M$. Откуда $f(P) \subseteq P$. в) вытекает из б).

г) По а) существует такой подмодуль E модуля M, что $H + C = H \oplus E$. Так как $(H+C)/H \cong C/(H \cap C)$, то E является циклическим. д) Индукция по числу образующих.

е) K является объединением счетной возрастающей цепи конечно порожденный модулей H_n, где $H_{n+1} = H_n + C_n$, а C_n — циклический модуль. По д) $H_n + C_n = H_n \oplus E_n$, где E_n — циклические модули. Пусть $E_0 = H_1$. Тогда $K = \oplus_{n=0}^{\infty} E_n$.

ж) По а) все подмодули модуля M являются регулярными. По теореме Капланского (теорема 17.2) $M = \oplus_{i \in I} M_i$, где M_i — счетно порожденные модули. Теперь можно применить е).

з) По теореме Капланского M — прямая сумма счетно порожденных модулей. По ж) M — прямая сумма циклических регулярных модулей M_i. Каждый циклический проективный модуль M_i изоморфен прямому слагаемому модуля R_R. По д) K — прямая сумма циклических прямых слагаемых проективного модуля M. Следовательно, K — проективный модуль.

18.42. 1) M — проективный модуль, поэтому по 18.41 з) достаточно показать регулярность M, т.е. что каждый его циклический подмодуль H — прямое слагаемое в M. Существует $n \in \mathbb{N}$ такое, что $H \subseteq F = \oplus_{j=1}^{n} M_j$. Осталось показать регулярность F. Индукцией по n. Пусть $n > 1$ и $G = \oplus_{j=1}^{n-1} M_j$, G — регулярный модуль. Пусть $f \colon F \to M_n$ — проекция. Тогда $f(H)$ — циклический подмодуль регулярного модуля M_n, значит, $M_n = f(H) \oplus N$. Проективность M_n влечет проективность $f(H)$. Следовательно, $G \cap H$ — прямое слагаемое в H: $H = (G \cap H) \oplus E$. Тогда $f(E) = f(H)$ и $G \cap E = 0$. Откуда $G \oplus E = G \oplus f(H)$. Так как $G \cap H$ — циклический подмодуль регулярного модуля G, то $G = (G \cap H) \oplus L$. Поэтому $G \oplus f(H) = (G \cap H) \oplus L \oplus E = H \oplus L$. Тогда $F = H \oplus L \oplus N$.

2) следует из 1) и 18.41 з).

18.43. Импликация б) $\Rightarrow$ а) проверяется непосредственно.

а) $\Rightarrow$ б). По 18.42 2) M — регулярный модуль. Поэтому для каждого $f \in S$ конечно порожденный подмодуль $f(M)$ — прямое слагаемое в M. Согласно 18.33 б) S — регулярное кольцо.

а) $\Rightarrow$ в). Пусть $f = \sum_{i=1}^{n} m_i b_i \in N \cap MI$, где $m_i \in M$ и $b_i \in I$. Конечно порожденный левый идеал $\sum_{i=1}^{n} Rb_i$ порождается некоторым идемпотентом $e \in R$. Поэтому $b_i = a_i e$ для всех $i = 1, \ldots, n$, где $a_i \in R$. Тогда если $m = \sum_{i=1}^{n} m_i a_i$, то $f = me \in N$ и $f = fe \in NI$. Поэтому $N \cap MI \subseteq NI \subseteq N \cap MI$.

в) $\Rightarrow$ а). Пусть $a \in R$, $M = R_R$, $N = aR$, $I = Ra$. Так как $a \in N \cap MI$, то $a \in NI = aRa$. Следовательно, $a = aba$ для некоторого $b \in R$.

18.45. $B \times A \to B \otimes_R A$, $(b,a) \to b \otimes_R a$ — S-сбалансированное отображение. Значит, эпиморфизм t существует.

19. Основные понятия теории абелевых групп

19.13. 1) Дополнением подгруппы B служит объединение смежных классов $a + B$, эти смежные классы — открытые множества, и тем же свойством обладает их объединение.

19.14. Так как p-адическая топология группы A хаусдорфова, если и только если $\bigcap_k p^k A = 0$, то эквивалентность условий

а) и б) очевидна. Из б) следует, что $h_p(a) = \infty$ в том и только в том случае, когда $a = 0$. Учитывая также неравенство $h_p(a+b) \geqslant \min(h_p(a), h_p(b))$, получаем, что: 1) $||a|| \geqslant 0$ для любого $a \in A$, 2) $||a|| = 0$, если и только если $a = 0$, 3) $||a+b|| \leqslant \max(||a||, ||b||)$ для всех $a, b \in A$.

Таким образом, $||a||$ — норма на группе A. Чтобы доказать импликацию в) $\Rightarrow$ г), заметим, что из свойств нормы следует, что $\delta(a,b) = ||a-b||$ — метрика на A, при которой база открытых множеств состоит из множеств $\{b \in A \,|\, \delta(a,b) < e^{(-k+1)}\} = a + p^k A$. Таким образом, в) $\Rightarrow$ г), а импликация г) $\Rightarrow$ а) очевидна.

19.22. Предположим, что выполнены условия а) и $a_3 \in \operatorname{Ker} \gamma_3$. Тогда $\gamma_4\alpha_3a_3 = \beta_3\gamma_3a_3 = 0$. Следовательно, $\alpha_3a_3 = 0$. В силу

того, что верхняя строка точна, существует элемент $a_2 \in A_2$ со свойством $\alpha_2 a_2 = a_3$. Откуда $\beta_2\gamma_2 a_2 = \gamma_3\alpha_2 a_2 = \gamma_3 a_3 = 0$. Нижняя строка точна, поэтому $\beta_1 b_1 = \gamma_2 a_2$ для некоторого $b_1 \in B_1$, а так как γ_1 — эпиморфизм, то $\gamma_1 a_1 = b_1$ для некоторого $a_1 \in A_1$. Таким образом, $\gamma_2\alpha_1 a_1 = \beta_1\gamma_1 a_1 = \beta_1 b_1 = \gamma_2 a_2$, откуда $\alpha_1 a_1 = a_2$. Это означает, что $a_3 = \alpha_2 a_2 = \alpha_2\alpha_1 a_1 = 0$, т.е. γ_3 — мономорфизм.

К б) применимы похожие рассуждения (они известны под названием «диаграмный поиск»). Условия а) и б) влекут в).

19.24. а) Если нужный φ существует, то из равенства $\eta = \alpha\varphi$ следует, что $\beta\eta = \beta\alpha\varphi = 0$ и поэтому условие утверждения необходимо. Обратно, если $\beta\eta = 0$, то $\operatorname{Im}\eta \subseteq \operatorname{Ker}\beta$. Так как $\operatorname{Im}\alpha = \operatorname{Ker}\beta$ и α — мономорфизм, то определено отображение $\varphi = \alpha^{-1}\eta$ группы G в A. Гомоморфизм φ является искомым. Если $\varphi'\colon G \to A$ — другое отображение с теми же свойствами, то $\alpha\varphi' = \eta = \alpha\varphi$. Так как α — мономорфизм, то $\varphi' = \varphi$.

б) Доказательство в определенном смысле двойственно а).

19.30. Пусть A_p состоит из всех элементов $a \in A$, порядок которых равен степени простого числа p. Тогда A_p — подгруппа. В группе $A_{p_1}+\ldots+A_{p_k}$ всякий элемент аннулируется произведением степеней чисел $p_1, \ldots, p_k$, значит, $A_p \cap (A_{p_1}+\ldots+A_{p_k}) = 0$ при $p \neq p_1, \ldots, p_k$, поэтому подгруппы A_p порождают в A прямую сумму $\bigoplus\limits_p A_p$. Покажем, что всякий элемент $a \in A$ лежит в $\bigoplus\limits_p A_p$. Пусть $o(a) = m = p_1^{r_1}\ldots p_n^{r_n}$, где p_i — различные простые числа. Числа $m_i = mp_i^{-r_i}$ $(i = 1, \ldots, n)$ взаимно просты, поэтому существуют такие целые числа $s_1, \ldots, s_n$, что $s_1 m_1 + \ldots + s_n m_n = 1$. Имеем $a = s_1 m_1 a + \ldots + s_n m_n a$, где $m_i a \in A_p$, следовательно, $a \in A_{p_1} + \ldots + A_{p_n} \subseteq \oplus A_p$.

19.34. Пусть $\beta\colon B \to C$ — эпиморфизм, F — свободная группа, $\varphi\colon F \to C$. Для всякого x_i из системы свободных образующих $\{x_i\}_{i\in I}$ группы F выберем такой элемент $b_i \in B$, что $\beta b_i = \varphi x_i$. Соответствие $x_i \mapsto b_i$ $(i \in I)$ можно продолжить до гомоморфизма $\psi\colon F \to B$. Для него выполнено равенство $\beta\psi = \varphi$, следовательно, группа F проективна.

Пусть G — проективная группа и $\beta\colon F \to G$ — эпиморфизм свободной группы F на G. Тогда существует такой гомоморфизм $\psi\colon G \to F$, что $\beta\psi = 1_G$. В частности, ψ — инъективное отображение на прямое слагаемое группы F, т.е. группа G изоморфна прямому слагаемому группы F, но подгруппы свободных групп свободны.

19.37. Если $A = B \oplus C$ и $a = b' + c'$ $(b' \in B,\ c' \in C)$, то $pa = pb' + pc' = b + c$ дает $pb' = b$. Обратно, если из $pa = b + c$ следует, что $pb' = b$ для некоторого $b' \in B$, то $a - b' \in B \oplus C$, $a \in B \oplus C$, значит, $A/(B \oplus C)$ является группой без кручения. С другой стороны, поскольку C есть B-высокая подгруппа, факторгруппа $A/(B \oplus C)$ обязана быть периодической, следовательно, $A = B \oplus C$.

19.46. Проверки требует только достаточность. Пусть $\{a_1, a_2, \ldots\}$ — система образующих группы A; A является объединением возрастающей последовательности своих конечных подгрупп $A_n = \{a_1, \ldots, a_n\}$, $n = 1, 2, \ldots$. Остается применить теорему 19.2.

19.47. Предположим, что $A = \bigoplus\limits_n A_n$, где A_n — прямая сумма циклических групп одного и того же порядка p^n. Цоколи $S_n = \bigoplus\limits_{i=n}^{\infty} A_i[p]$ с возрастанием n образуют убывающую цепочку, причем S_n состоит в точности из тех элементов подгруппы $S_1 = A[p]$, которые имеют высоту $\geqslant n-1$. Элемент $a = (b_1, b_2, \ldots) \in \prod\limits_n \mathbb{Z}_{p^n}$, где $b_n \in \mathbb{Z}_{p^n}$, имеет высоту $\geqslant n-1$ только при $b_1 = \ldots = b_{n-1} = 0$, поэтому каждая факторгруппа S_n/S_{n+1} имеет порядок p. Из $A_n[p] \cong S_n/S_{n+1}$ следует, что группы A_n конечны, поэтому группа A счетна. Полученное противоречие показывает, что A не является прямой суммой циклических групп.

19.48. Пусть S_n — подгруппа в $S = A[p]$, состоящая из элементов высоты $\geqslant n-1$. Если A — прямая сумма циклических p-групп, то S_n — прямая сумма цоколей всех прямых слагаемых порядка $\geqslant p^n$, поэтому факторгруппа S_n/S_{n+1} изоморфна прямой сумме цоколей прямых слагаемых порядка p^n в разложении группы A. Следовательно, число прямых слагаемых порядка p^n в разложении группы A в прямую сумму циклических групп равно рангу группы S_n/S_{n+1}. Подгруппы S_n определяются независимо от прямых разложений, значит, мощность m_{p^n} множества прямых слагаемых порядка p^n в любом разложении группы A в прямую сумму циклических p-групп одинакова. Так как число m_0 прямых слагаемых вида $\mathbb{Z}$ в разложении A в прямую сумму циклических групп равно рангу без кручения $r_0(A)$, то m_0 также однозначно определяется группой A.

Из предыдущего доказательства следует, что для прямых сумм циклических групп мощности m_0 и m_{p^n} для всевозможных $n \in \mathbb{N}$ составляют полную и независимую систему инвариантов.

19.51. Пусть сначала A — прямая сумма циклических p-групп, и пусть $B \subseteq A$; A является объединением возрастающей цепи $A_1 \subseteq A_2 \subseteq \ldots$ своих подгрупп, где в подгруппе A_n высоты элементов ограничены, например, числом k_n. Подгруппа B является объединением возрастающей цепи $B_1 \subseteq B_2 \subseteq \ldots$, где $B_n = B \cap A_n$. По теореме 19.2 группа B — прямая сумма циклических групп. Пусть A — произвольная прямая сумма циклических групп. Если $T = t(A)$, то $B \cap T = t(B)$. Теперь $B/(B \cap T) \cong (B+T)/T \subseteq A/T$, где A/T — свободная группа. Поэтому группа $B/(B \cap T)$ также свободна. Следовательно, $B = (B \cap T) \oplus C$ для некоторой свободной подгруппы C группы B. По доказанному, $B \cap T$ — прямая сумма циклических p-групп. Значит, B также — прямая сумма циклических групп.

19.52. Предположим, что $A = \langle a_1, a_2, \ldots\rangle$ — счетная группа без кручения, каждая подгруппа которой, имеющая конечный ранг, свободна. Обозначим через A_n множество, состоящее из всех элементов $a \in A$, зависящих от $\{a_1, \ldots, a_n\}$, и нуля. Ранг подгруппы A_n будет $\leqslant n$. Так как $r(A_{n+1}) \leqslant r(A_n) + 1$, то или группа A имеет конечный ранг (в этом случае утверждение тривиально), или существует такая подпоследовательность B_n последовательности групп A_n, что $r(B_n) = n$ и A — объединение возрастающей цепи $0 = B_0 \subset B_1 \subset B_2 \subset \ldots$. Теперь B_{n+1}/B_n — группа без кручения ранга 1 с конечным числом образующих. Следовательно, $B_{n+1}/B_n \cong \mathbb{Z}$. Откуда $B_{n+1} = B_n \oplus \langle b_{n+1}\rangle$ для некоторого b_{n+1}. Элементы $b_1, b_2, \ldots$ порождают прямую сумму $\bigoplus\limits_n \langle b_n\rangle = A$.

19.53. Пусть N — пересечение ядер всех гомоморфизмов $\eta\colon A\to\mathbb{Z}$. Тогда группа A/N изоморфна счетной подгруппе прямого произведения бесконечных циклических групп. По теореме 19.3 она свободна, значит, N служит для A прямым слагаемым. Единственность подгруппы N вытекает из того, что если M — какое-то прямое слагаемое группы A, не имеющее свободных факторгрупп, то его проекция на F должна быть нулевой. Поэтому $M\subseteq N$.

19.56. Пусть D — делимая группа, $A\subseteq B$ и $\xi\colon A\to D$. Рассмотрим все подгруппы G, $A\subseteq G\subseteq B$, для которых существует продолжение $\theta\colon G\to D$ гомоморфизма ξ. Частично упорядочим множество пар $(G,\ \theta)$, полагая $(G,\ \theta)\leqslant(G',\ \theta')$, если $G\subseteq G'$ и θ — ограничение гомоморфизма $\theta'\colon G'\to D$ на G. Множество этих пар не пусто и индуктивно. По лемме Цорна в рассматриваемом множестве существует максимальная пара $(G_0,\,\theta_0)$. Если $G_0\subset B$ и для элемента $b\in B\setminus G_0$ имеет место включение $nb=g\in G_0$ при некотором минимальном $n>0$, то $nx=\theta_0 g$ для некоторого $x\in D$ в силу делимости группы D. Отображение $\varphi_b\colon c+rb\mapsto\theta_0 c+rx$ $(c\in G_0, 0\leqslant r<n)$ является гомоморфизмом группы $\langle G_0,\,b\rangle$ в группу D. Если $nb\notin G_0$ при $n\neq 0$, то φ_b является гомоморфизмом группы $\langle G_0,\ b\rangle$ в группу D при произвольном $x\in D$ (на r тогда ограничений не накладывается). Значит, предположение $G_0\subset B$ противоречит максимальности пары $(G_0,\,\theta_0)$, т.е. $G_0=B$ и $\theta_0=\xi$.

19.57. По 19.56 для естественного вложения $\alpha\colon D\to A$ и тождественного отображения $1_D\colon D\to D$ существует такой гомоморфизм $\eta\colon A\to D$, что $\eta\alpha=1_D$. Откуда $A=D\oplus\operatorname{Ker}\eta$. Если для подгруппы $B\subseteq A$ имеет место равенство $D\cap B=0$, то $D+B=D\oplus B$ и существует гомоморфизм $\xi\colon D\oplus B\to D$, совпадающий с тождественным на D и нулевой на B. Если в предыдущих рассуждениях заменить 1_D на ξ, то $A=D\oplus\operatorname{Ker}\eta$, где $B\subseteq\operatorname{Ker}\eta$.

19.58. Если D — максимальная делимая подгруппа группы A и $A=D'\oplus C'$, где D' — делимая, а C' — редуцированная подгруппы, то $D=(D\cap D')\oplus(D\cap C')$. Здесь $D\cap C'=0$, откуда $D=D'$.

19.59. Периодическая часть T группы D — делимая группа; значит, $D=T\oplus E$, где E — делимая группа без кручения. Нужно показать, что каждая p-компонента T_p группы T есть прямая сумма групп $\mathbb{Z}_{p^\infty}$, а E — прямая сумма групп $\mathbb{Q}$.

Выберем в цоколе группы T_p максимальную независимую систему элементов $\{a_i\}_{i\in I}$. В силу делимости в группе T_p для каждого i существует такая бесконечная последовательность элементов a_{i_1}, a_{i_2}, …, что $a_{i_1}=a_i$, $pa_{i,\,n+1}=a_{in}$, $n=1,\,2,\,\ldots$; каждый элемент a_i может быть вложен в подгруппу $A_i=\langle a_{i_1},\,a_{i_2},\,\ldots\rangle\cong\mathbb{Z}_{p^\infty}$ группы T_p. Так как $\langle a_i\rangle$ — цоколь группы A_i и элементы a_i $(i\in I)$ независимы, то подгруппы A_i порождают в группе T_p подгруппу A, являющуюся их прямой суммой: $A=\bigoplus\limits_{i\in I}A_i$. Группа A является делимой подгруппой, и поэтому — прямым слагаемым группы T_p. Но A содержит цоколь группы T_p, значит, $A=T_p$.

Выберем максимальную независимую систему элементов $\{b_j\}_{j\in J}$ в группе E. Так как E — делимая группа без кручения, то при любом натуральном n существует ровно один элемент $x\in E$, для которого $nx=b_j$; значит, каждый b_j может быть вложен в подгруппу $B_j\cong\mathbb{Q}$ группы E. Поскольку $\{b_j\}$ — независимая система элементов, то подгруппы B_j порождают в E подгруппу B, являющуюся их прямой суммой: $B=\bigoplus\limits_{j\in J}B_j$. А поскольку система $\{b_j\}$ — максимальная, то $B=E$.

Число прямых слагаемых, изоморфных $\mathbb{Z}_{p^\infty}$ или $\mathbb{Q}$, в разложении группы D равно, соответственно, рангу $r(D_p)$ или рангу $r_0(D)$, это замечание заканчивает доказательство утверждения.

20. Чистота и чистая инъективность

20.11. Пусть B есть p^nA-высокая подгруппа группы A. Тогда $p^nB\subseteq B\cap p^nA=0$. Подгруппа B чиста в A. Для этого достаточно показать, что $B\cap p^kA\subseteq p^kB$ при любом целом $k\geqslant 0$. Примените индукцию по k. Если $b=p^{k+1}a\neq 0$, то проверьте, что $p^ka\in p^nA\oplus B$, т.е. $p^ka=p^nc+d$ для некоторых $c\in A$, $d\in B$, где $k\leqslant n-1$. Откуда $d=p^ka-p^nc\in B\cap p^kA=p^kB$ (подгруппы совпадают в силу индуктивного предположения). Значит, $b=pd\in p^{k+1}B$. Поэтому B как ограниченная чистая подгруппа является прямым слагаемым.

20.16. Необходимость. Пусть $a^*\in A/B$. Если $o(a^*)=\infty$, то любой представитель смежного класса a^* имеет бесконечный порядок. Если $o(a^*)=n$, то для любого $g\in a^*$ имеем $ng\in B$, значит, $nb=ng$ для некоторого $b\in B$. Поэтому элемент $a=g-b\in a^*$ имеет порядок n. Достаточность. Пусть $ng=b\in B$ для некоторого $g\in A$. Выберем в смежном классе $g+B$ представитель a со свойством $o(a)=o(g+B)$. Тогда $na=0$ и $n(g-a)=b$ для $g-a\in B$.

20.19. 2) Пусть A — слабо чистая подгруппа группы C, где C — прямое произведение элементарных p-групп. Из $\Phi(C)=0$ и $\Phi(A)=\Phi(C)\cap A$ получаем $\Phi(A)=0$.

Предположим теперь, что $\Phi(A)=0$. Тогда $\cap pA=0$, где p пробегает все простые числа с $pA\neq A$ (19.25 2)). Обозначим через e_p канонический гомоморфизм $A\to A/pA$, а через C_p факторгруппу A/pA. Определим гомоморфизм $f\colon A\to\prod C_p$, полагая $f(a)=(e_p(a))$, $a\in A$. Тогда f — мономорфизм и его образ — слабо чистая подгруппа.

20.23. Пусть $\{a_i\}_{i\in I}$ — множество всех элементов группы A, и пусть $A_i=\langle a_i\rangle$. Для каждого a_i возьмем группу $\langle x_i\rangle$, изоморфную группе A_i, и положим $X=\bigoplus\limits_{i\in I}\langle x_i\rangle$. Вложения $\eta_i\colon\langle x_i\rangle\to A$, где $\eta_i x_i=a_i$, порождают эпиморфизм $\eta=\nabla\left[\bigoplus\limits_{i\in I}\eta_i\right]\colon X\to A$, где $\nabla\colon(\ldots,\,\eta_i,\,\ldots)\mapsto\sum\limits_i\eta_i$ — *кодиагональное отображение*. Нужно проверить, что $K=\operatorname{Ker}\eta$ — чистая подгруппа группы X. Пусть $nx=b\in K$ для некоторого $x\in X$. Если $\eta x=a_i\in A$, то $x-x_i\in K$. Так как $na_i=\eta(nx)=\eta b=0$ и $o(x_i)=o(a_i)$, то $n(x-x_i)=b$.

20.33. Нужно проверить только достаточность условия. Предположим, что A обладает указанным свойством. Тогда A является прямым слагаемым во всякой группе G, в которой она — чистая подгруппа и G/A — делимая группа. Рассмотрим случай, когда A — чистая подгруппа группы G и G/A — периодическая группа. Если B/A — базисная подгруппа в G/A, то $B=A\oplus B'$. Так как $G/B\cong(G/A)/(B/A)$ — делимая группа, то G/B' содержит $B/B'\cong A$ в качестве чистой подгруппы, факторгруппа по которой делима, значит, $G/B'=B/B'\oplus G'/B'$. Имеем $G=B+G'=A+B'+G'=A+G'$ и $A\cap G'=A\cap B'=0$, т.е. $G=A\oplus G'$.

Если G/A — группа без кручения, то существует такая группа H, что $G \subseteq H$ и H/A — делимая группа без кручения. Группа A служит прямым слагаемым для группы H, а тогда и для G. Наконец, если G/A — произвольная группа и $T/A = t(G/A)$, то $T = A \oplus T'$, а так как $T/T' \cong A$ — прямое слагаемое группы G/T', то $G = A \oplus G'$ для некоторой подгруппы $G' \subseteq G$.

20.36. Предположим, что A — редуцированная алгебраически компактная группа. Тогда A служит прямым слагаемым для прямого произведения циклических групп $\mathbb{Z}_{p^k}$. Каждая группа $\mathbb{Z}_{p^k}$ полна в своей $\mathbb{Z}$-адической топологии. Откуда следует, что группа A полна в своей $\mathbb{Z}$-адической топологии.

Предположим теперь, что A полна в своей $\mathbb{Z}$-адической топологии. Тогда A хаусдорфова и, следовательно, редуцированная. Пусть группа G содержит A в качестве чистой подгруппы, причем G/A — делимая группа. Если G хаусдорфова в своей $\mathbb{Z}$-адической топологии, то в силу плотности подгруппы A в G каждый элемент $g \in G$ является пределом некоторой последовательности элементов из A. Так как относительная топология в A совпадает с $\mathbb{Z}$-адической топологией группы A, то $g \in A$ и $A = G$. Если G не хаусдорфова, то хаусдорфова группа G/G^1, где $A \cap G^1 = 0$, и G/G^1 содержит $(A+G^1)/G^1 \cong A$ в качестве чистой подгруппы. Как уже показано, из этого вытекает, что $A \oplus G^1 = G$.

20.37. Если это не так, то существует строго возрастающая последовательность натуральных чисел $n_1, n_2, \ldots$, где $n_j \mid n_{j+1}$, и существуют такие группы B_j, каждая из которых есть прямая сумма конечного числа групп C_i, что эти B_j порождают в $\oplus C_i$ подгруппу, являющуюся их прямой суммой, и $n_j A \cap \bigoplus_{k=1}^{j-1} B_k \subset n_j A \cap \bigoplus_{k=1}^{j} B_k$ $(j = 1, 2, \ldots)$. Пусть a_j — элемент, входящий в правую часть, но не лежащий в левой части. Тогда a_{j-1} имеет нулевую компоненту в B_j, а элемент a_j — ненулевую. Поэтому последовательность Коши $a_1, a_2, \ldots$ $(a_i \in A)$ не имеет предела в $\oplus C_i$.

20.42. Пусть группа A алгебраически компактна, и $A \oplus B = C$ — прямое произведение циклических p-групп. Соберем слагаемые $\mathbb{Z}_{p^k}$, относящиеся к одному и тому же простому числу p, и образуем их прямое произведение C_p. Очевидно, $C = \prod_p C_p$. Подгруппы C_p вполне инвариантны, поэтому $C_p = A_p \oplus B_p$, где $A_p = A \cap C$, $B_p = B \cap C_p$. И далее $C = \prod_p A_p \oplus \prod_p B_p$. Подгруппы A_p все вместе порождают в A подгруппу $A_0 = \bigoplus_p A_p$. Если рассмотреть группу C как топологическую с $\mathbb{Z}$-адической топологией, то замыкание в C подгруппы A_0 содержит $\prod_p A_p$, так как $\prod_p A_p/A_0$ — делимая группа. Поскольку $B^1 = 0$, то подгруппа A замкнута в C. Следовательно, $\prod_p A_p \subseteq A$. Аналогично, $\prod_p B_p \subseteq B$, значит, $A = \prod_p A_p$ и $B = \prod_p B_p$. Как прямое слагаемое полной группы, группа A_p полна в своей $\mathbb{Z}$-адической топологии, которая здесь совпадает с p-адической топологией.

Обратно, пусть A_p — группа, полная в своей p-адической топологии. Группу A_p можно следующим естественным образом превратить в модуль над кольцом $\widehat{\mathbb{Z}}_p$ целых p-адических чисел. Пусть $a \in A_p$ и $\xi = s_0 + s_1 p + s_2 p^2 + \ldots \in \widehat{\mathbb{Z}}_p$. Последовательность $s_0 a, (s_0 + s_1 p)a, \ldots, (s_0 + s_1 p + \ldots + s_n p^n)a, \ldots$ является последовательностью Коши в группе A_p; она сходится в A_p к пределу, который определим как ξa. Поэтому $qA_p = A_p$ для всех простых $q \neq p$. В частности, $\mathbb{Z}$-адическая топология группы A_p совпадает с p-адической топологией, A_p алгебраически компактна. Поэтому A, как прямое произведение групп A_p, алгебраически компактна.

Наконец, единственность компонент A_p следует из соотношения $A_p = \bigcap_{q \neq p} q^k A$ $(k = 1, 2, \ldots)$.

21. Группы гомоморфизмов

21.17. а) Ограничение гомоморфизма $\alpha\colon \oplus A_i \to C$ на A_i — это гомоморфизм $\alpha_i\colon A_i \to C$. Таким образом, получается гомоморфизм $\varphi\colon \alpha \mapsto (\ldots, \alpha_i, \ldots)$ группы $\operatorname{Hom}(\oplus A_i, C)$ в группу $\prod \operatorname{Hom}(A_i, C)$. Легко проверить, что φ — изоморфизм.

б) Если через π_i обозначить i-ю координатную проекцию $\prod C_i \to C_i$, то каждый гомоморфизм $\alpha \in \operatorname{Hom}(A, \prod C_i)$ будет определять гомоморфизмы $\pi_i \alpha \in \operatorname{Hom}(A, C_i)$. Отображение $\alpha \mapsto (\ldots, \pi_i \alpha, \ldots)$ есть искомый изоморфизм.

21.24. 1) Чтобы проверить, что $\operatorname{Im}\beta^*$ есть p-чистая подгруппа в $\operatorname{Hom}(B, G)$, возьмем $\eta \in \operatorname{Hom}(B, G)$ и $\chi \in \operatorname{Hom}(C, G)$, для которых $p^n\eta = \chi\beta$. Из $\operatorname{Im}\alpha \subseteq \operatorname{Ker}\chi\beta = \operatorname{Ker} p^n\eta$ следует, что $\operatorname{Im} p^n\alpha \subseteq \operatorname{Ker}\eta$. Существует прямое разложение $B/p^n(\alpha A) = \alpha A/p^n(\alpha A) \oplus B'/p^n(\alpha A)$, где B' — некоторая подгруппа в B. Обозначив через π проекцию на второе слагаемое, положим $\varphi b = \eta'\pi(b + p^n\alpha A)$, где $\eta'(b + p^n\alpha A) = \eta b$. Это дает гомоморфизм $\varphi\colon B \to G$, для которого $p^n\varphi = p^n\eta$. Так как $\alpha A \subseteq \operatorname{Ker}\varphi$, то существует такое $\theta\colon C \to G$, что $\varphi = \theta\beta$. Из $p^n(\theta\beta) = p^n\varphi = p^n\eta = \chi\beta$ вытекает, что последовательность (2) p-чисто точна.

Перейдем к последовательности (3). Пусть $p^n\eta = \alpha\chi$, где $\eta \in \operatorname{Hom}(G, B)$, $\chi \in \operatorname{Hom}(G, A)$. Тогда $p^n\eta$ отображает группу G в αA, а η отображает G в $p^{-n}\alpha A$. Подгруппа αA служит прямым слагаемым в $p^{-n}\alpha A$, т.е. $p^{-n}\alpha A = \alpha A \oplus B'$. Если π — проекция на первое слагаемое, то для $\varphi = \alpha^{-1}\pi\eta \in \operatorname{Hom}(G, A)$ выполнено $p^n\alpha\varphi = \alpha\chi$, т.е. (3) p-чисто точна.

21.26. Можно ограничиться случаем p-групп. Поэтому покажем, что если A есть p-группа, то группа $H = \operatorname{Hom}(A, G)$ полна в своей p-адической топологии. Предположим, что элемент $\eta \in H$ делится на любую степень числа p. Если $a \in A$ имеет порядок p^k и $p^k\chi = \eta$, то $\eta a = p^k\chi a = 0$, откуда $\eta = 0$, т.е. группа H хаусдорфова. Пусть, далее, $\eta_1, \eta_2, \ldots$ — последовательность Коши в группе H. Можно считать, что она чистая: $\eta_{n+1} - \eta_n = p^n\chi_n \in p^n H$ для любого n. Положим $\eta = \eta_1 + (\eta_2 - \eta_1) + \ldots + (\eta_{n+1} - \eta_n) + \ldots$. Это гомоморфизм $A \to G$. Кроме того, $\eta - \eta_n = (\eta_{n+1} - \eta_n) + (\eta_{n+2} - \eta_{n+1}) + \ldots = p^n(\chi_n + p\chi_{n+1} + \ldots)$, где $\chi_n + p\chi_{n+1} + \ldots$ снова принадлежит H, т.е. η — предел данной последовательности. Следовательно, H — полная группа.

21.27. Точная последовательность $0 \to B \xrightarrow{\alpha} A \to A/B \to 0$ индуцирует точную последовательность

$$0 = \operatorname{Hom}(A/B, C) \to \operatorname{Hom}(A, C) \xrightarrow{\alpha^*} \operatorname{Hom}(B, C).$$

Значит, $\mathrm{Hom}\,(A,\,C)$ можно рассматривать как подгруппу группы $\mathrm{Hom}\,(B,\,C)$. Осталось показать, что соответствующая факторгруппа есть группа без кручения. Если $p^n\eta = \chi\alpha$, где $\chi \in \mathrm{Hom}\,(A,\,C)$, $\eta \in \mathrm{Hom}\,(B,\,C)$, то можно определить $\theta\colon A \to C$ как $\theta\, a = \chi g + \eta b$, если $a \in A$ и $a = p^n g + \alpha b$ ($g \in A$, $b \in B$). Нетрудно проверить, что θ является гомоморфизмом со свойством $\theta\alpha = \eta$. Это и требовалось.

22. Группы расширений. Тензорные и периодические произведения

22.7. Если $\alpha_1, \ldots, \alpha_n$ — эндоморфизмы группы A, то $(\alpha_1 + \ldots + \alpha_n)_* = (\alpha_1)_* + \ldots + (\alpha_n)_*$. Так как, очевидно, 1_A индуцирует $1_{\mathrm{Ext}(C,\,A)}$, выбрав $\alpha_1 = \ldots = \alpha_n = 1_A$, получим требуемое. Доказательство для случая группы C аналогично.

Умножение на целое p-адическое число ξ в группе A индуцирует эндоморфизм ξ_* группы $\mathrm{Ext}(C,\,A)$. Число ξ является пределом последовательности $n_i \in \mathbb{Z}$ $(i = 1, 2, \ldots)$ в p-адической топологии, $p^i \mid \xi - n_i$ для каждого i, по доказанному, ξ_* — предел умножений на n_i. Значит, ξ_* можно отождествить с умножением на ξ.

22.9. Возьмем точные последовательности $0 \to G_i \to F_i \to C_i \to 0$, где F_i — свободные группы. Эти последовательности индуцируют точную последовательность $0 \to \oplus G_i \to \oplus F_i \to \oplus C_i \to 0$. Имеем

$$\mathrm{Hom}(F_i,\,A) \to \mathrm{Hom}(G_i,\,A) \to \mathrm{Ext}(C_i,\,A) \to \mathrm{Ext}(F_i,\,A) = 0.$$

Это дает коммутативную диаграмму с точными строками

$$\begin{array}{ccccc} \prod \mathrm{Hom}(F_i,\,A) \to & & \prod \mathrm{Hom}(G_i,\,A) \to & & \prod \mathrm{Ext}(C_i,\,A) \to 0 \\ \updownarrow & & \updownarrow & & \\ \mathrm{Hom}(\oplus F_i,\,A) \to & & \mathrm{Hom}(\oplus G_i,\,A) \to & & \mathrm{Ext}(\oplus C_i,\,A) \to 0\,, \end{array}$$

где вертикальные изоморфизмы естественные. Следовательно, существует естественный изоморфизм $\prod \mathrm{Ext}(C_i,\,A) \cong \mathrm{Ext}(\oplus C_i,\,A)$. Доказательство второго изоморфизма проводится двойственным образом.

22.10. а) Последовательность $0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \to 0$ (где m — умножение на число m) точна. Поэтому последовательность

$$\mathrm{Hom}\,(\mathbb{Z},\,A) \xrightarrow{m} \mathrm{Hom}\,(\mathbb{Z},\,A) \to \mathrm{Ext}\,(\mathbb{Z}_m,\,A) \to 0$$

также точна (m^* также действует как умножение на m). Так как существует естественный изоморфизм $\mathrm{Hom}\,(\mathbb{Z},\,A) \cong A$, то группа $\mathrm{Ext}\,(\mathbb{Z}_m,\,A)$ изоморфна группе A/mA, причем это опять естественный изоморфизм.

б) Так как последовательность $0 \to A\,[m] \to A \xrightarrow{m} mA \to 0$ точна, получаем индуцированную точную последовательность

$$\mathrm{Ext}(mA,\,\mathbb{Z}_m) \xrightarrow{m} \mathrm{Ext}(A,\,\mathbb{Z}_m) \to \mathrm{Ext}(A\,[m],\,\mathbb{Z}_m) \to 0.$$

Образ первого отображения здесь нулевой, откуда получается требуемый изоморфизм.

22.13. 1) Последовательность $0 \to C \xrightarrow{m} C$ точна. Поэтому точна последовательность $\mathrm{Ext}\,(C,\,A) \xrightarrow{m} \mathrm{Ext}\,(C,\,A) \to 0$.

2) Пусть D — делимая оболочка группы A. Тогда D/A — периодическая группа с нулевой p-компонентой, откуда $\mathrm{Hom}\,(C,\,D/A) = 0$. Теперь утверждение вытекает из точности последовательности

$$\mathrm{Hom}(C,\,D/A) \to \mathrm{Ext}(C,\,A) \to \mathrm{Ext}(C,\,D) = 0.$$

22.14. Из точной последовательности $0 \to A \to D \to D/A \to 0$ (так как D — группа без кручения) получаем точную последовательность

$$0 = \mathrm{Hom}(C,\,D) \to \mathrm{Hom}(C,\,D/A) \to \mathrm{Ext}(C,\,A) \to \mathrm{Ext}(C,\,D) = 0,$$

откуда следует справедливость требуемого утверждения.

22.15. Пусть B — p-базисная подгруппа группы A. В точной последовательности $0 \to B \to A \to A/B \to 0$ факторгруппа A/B p-делима и имеет нулевую p-компоненту. Поэтому $\mathrm{Hom}\,(\mathbb{Z}_{p^\infty},\,A/B) = 0$ и $\mathrm{Ext}\,(\mathbb{Z}_{p^\infty},\,A/B) = 0$. Следовательно, точна последовательность $0 \to \mathrm{Ext}(\mathbb{Z}_{p^\infty},\,B) \to \mathrm{Ext}(\mathbb{Z}_{p^\infty},\,A) \to 0$, т.е. $\mathrm{Ext}\,(\mathbb{Z}_{p^\infty},\,A) \cong \mathrm{Ext}\,(\mathbb{Z}_{p^\infty},\,B)$. Здесь B — свободная группа ранга m, ее делимой оболочкой является группа $\underset{m}{\oplus}\,\mathbb{Q}$. Факторгруппа делимой оболочки по подгруппе B — это группа $\underset{m}{\oplus}\,\mathbb{Q}/\mathbb{Z}$. Это и свойства группы гомоморфизмов дают требуемый изоморфизм.

22.16. 1) Имеем точную последовательность $0 \to T \to C \to C/T \to 0$, где T — периодическая группа, C/T — группа без кручения. Поэтому индуцированная последовательность

$$0 = \mathrm{Hom}(T,\,A) \to \mathrm{Ext}(C/T,\,A) \to \mathrm{Ext}(C,\,A) \to \mathrm{Ext}(T,\,A) \to 0$$

точна. Группа $\mathrm{Ext}\,(C/T,\,A)$ делима. Значит, эта последовательность расщепляется: $\mathrm{Ext}\,(C,\,A) \cong \mathrm{Ext}\,(C/T,\,A) \oplus \mathrm{Ext}\,(T,\,A)$. Второе слагаемое алгебраически компактно, что доказывает данное утверждение.

2) Без ограничения общности можно предполагать, что группа A редуцированная. Значит, A служит прямым слагаемым для прямого произведения циклических p-групп. При умножении на p^n группа $\mathrm{Ext}\,(C,\,\mathbb{Z}_{p^n})$ обращается в нуль, поэтому она является ограниченной группой. Согласно 22.9 группа $\mathrm{Ext}\,(C,\,A)$ — прямое слагаемое прямого произведения таких групп, поэтому она алгебраически компактна.

22.22. Из чисто точной последовательности $0 \to A \to \widehat{A} \to \widehat{A}/A \to 0$ получите точную последовательность

$$0 = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\, \widehat{A}) \to \mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\, \widehat{A}/A) \to \mathrm{Pext}(\mathbb{Q}/\mathbb{Z},\, A) \to \mathrm{Pext}(\mathbb{Q}/\mathbb{Z},\, \widehat{A}) = 0.$$

22.30. 1) Если G — копериодическая группа и $G \to H \to 0$ — точная последовательность, то точна последовательность $0 = \mathrm{Ext}\,(\mathbb{Q},\, G) \to \mathrm{Ext}\,(\mathbb{Q},\, H) \to 0$. Откуда $\mathrm{Ext}\,(\mathbb{Q},\, H) = 0$.

2) Точная последовательность $0 \to H \to G \to G/H \to 0$ дает точную последовательность

$$0 = \mathrm{Hom}\,(\mathbb{Q},\, G) \to \mathrm{Hom}\,(\mathbb{Q},\, G/H) \to \mathrm{Ext}\,(\mathbb{Q},\, H) \to \mathrm{Ext}\,(\mathbb{Q},\, G) = 0.$$

Откуда $\mathrm{Ext}\,(\mathbb{Q},\, H) \cong \mathrm{Hom}\,(\mathbb{Q},\, G/H)$. Вторая из этих групп равна нулю, если и только если G/H — редуцированная группа.

4) Получите точную последовательность

$$0 = \mathrm{Ext}\,(\mathbb{Q},\, H) \to \mathrm{Ext}\,(\mathbb{Q},\, G) \to \mathrm{Ext}\,(\mathbb{Q},\, G/H) = 0.$$

22.31. 2) Получите точную последовательность

$$0 = \mathrm{Hom}\,(\mathbb{Q},\, G) \to \mathrm{Hom}\,(\mathbb{Z},\, G) \cong G \to \mathrm{Ext}\,(\mathbb{Q}/\mathbb{Z},\, G) \to \mathrm{Ext}\,(\mathbb{Q},\, G) = 0.$$

22.33. Пусть G — редуцированная копериодическая группа. Точная последовательность $0 \to G \to D \to D/G \to 0$, где D — делимая группа, дает точную последовательность

$$\mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\, D/G) \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, G) \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, D) = 0.$$

Здесь $\mathrm{Hom}\,(\mathbb{Q}/\mathbb{Z},\, D/G)$ — алгебраически компактная группа, тогда как средняя группа изоморфна группе G.

22.35. 1) Пусть G — периодическая копериодическая группа. Тогда G/G^1 — редуцированная периодическая алгебраически компактная группа, поэтому она является ограниченной группой. Значит, $mG \subseteq G^1$ для некоторого натурального числа m. Откуда $mG \subseteq nmG$ для любого n, т.е. $mG = G^1$ — делимая группа, что доказывает необходимость. Достаточность очевидна.

2) В группе без кручения G подгруппа G^1 делима. Поэтому $G = R \oplus G^1$, где подгруппа $R \cong G/G^1$ является алгебраически компактной.

3) Точная последовательность $0 \to A \to D \to D/A \to 0$, где D — делимая группа, дает точную последовательность

$$\mathrm{Hom}(C,\, D/A) \to \mathrm{Ext}(C,\, A) \to \mathrm{Ext}(C,\, D) = 0.$$

Здесь первая группа алгебраически компактна, а группа $\mathrm{Ext}\,(C,\, A)$ является ее эпиморфным образом.

22.38. Получите точную последовательность $0 = \mathrm{Hom}(\mathbb{Q},\, T) \to \mathrm{Hom}(\mathbb{Z},\, T) \cong T \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, T) \to \mathrm{Ext}(\mathbb{Q},\, T) \to \mathrm{Ext}(\mathbb{Z},\, T) = 0$. Теперь утверждение вытекает из того, что $\mathrm{Ext}(\mathbb{Q},\, T)$ — делимая группа без кручения.

22.39. Точная последовательность $0 \to T \to A \to J \to 0$ дает точную последовательность $0 = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\, J) \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, T) \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, A) \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, J) \to 0$. Здесь последняя группа изоморфна группе $\mathrm{Hom}(\mathbb{Q}/\mathbb{Z},\, D/J)$, где D — делимая оболочка группы J. Поэтому группа $\mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, J)$ является прямым произведением групп $\mathrm{Hom}(\mathbb{Z}_{p^\infty},\, D/J)$, где p пробегает все простые числа, эти группы являются группами без кручения. Так как $\mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, T)$ есть копериодическая группа, то последняя точная последовательность расщепляется. Отсюда получается требуемый изоморфизм.

22.40. Существует чисто точная последовательность $0 \to H \to F \to T \to 0$, где F и, значит, H — прямые суммы конечных циклических групп. Так как $\mathrm{Pext}(F,\, A) = 0$, то точна последовательность

$$0 \to \mathrm{Hom}(T,\, A) \to \mathrm{Hom}(F,\, A) \to \mathrm{Hom}(H,\, A) \to \mathrm{Pext}(T,\, A) \to 0.$$

Алгебраически компактная группа $\mathrm{Hom}(T,\, A)$ служит прямым слагаемым для группы $\mathrm{Hom}\,(F,\, A)$. Отсюда получается точная последовательность

$$0 \to G \to \mathrm{Hom}(H,\, A) \to \mathrm{Pext}(T,\, A) \to 0,$$

где G и $\mathrm{Hom}(H,\, A)$ — редуцированные алгебраически компактные группы. Получаем точную последовательность

$$0 = \mathrm{Hom}(\mathbb{Q},\, \mathrm{Hom}(H,\, A)) \to \mathrm{Hom}(\mathbb{Q},\, \mathrm{Pext}(T,\, A)) \to \mathrm{Ext}(\mathbb{Q},\, G) = 0.$$

Это показывает, что $\mathrm{Pext}\,(T,\, A)$ и, значит, $\mathrm{Ext}\,(T,\, A)$ — редуцированные группы.

22.46. Достаточно рассмотреть случай, когда группа A редуцированная. Получите точную последовательность $0 \to A \to \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, A) \to \mathrm{Ext}(\mathbb{Q},\, A) \to 0$, где $\mathrm{Ext}(\mathbb{Q},\, A)$ — делимая группа без кручения. Достаточно взять $G = \mathrm{Ext}(\mathbb{Q}/\mathbb{Z},\, A)$.

22.51. 2) Элементы группы $\mathbb{Z} \otimes C$ могут быть приведены к виду

$$\sum (n_i \otimes c_i) = \sum (1 \otimes n_i c_i) = 1 \otimes \sum n_i c_i = 1 \otimes c$$

для некоторого $c \in C$. Отображение $\varphi\colon c \mapsto 1 \otimes c$ является эпиморфизмом группы C на $\mathbb{Z} \otimes C$. Отображение $(m,\, c) \mapsto mc$ является билинейным. Поэтому существует такой гомоморфизм $\psi\colon \mathbb{Z} \otimes C \to C$, что $\psi\colon 1 \otimes c \mapsto c$. Отображения φ и ψ взаимно обратные.

Отображение $\varphi\colon c \mapsto 1 \otimes c$ является эпиморфизмом группы C на группу $\mathbb{Z}_m \otimes C$, $mC \subseteq \mathrm{Ker}\,\varphi$. Билинейное отображение $(n,\, c) \mapsto nc + mC$ индуцирует такой эпиморфизм $\psi\colon \mathbb{Z}_m \otimes C \to C/mC$, что $\psi\varphi$ является каноническим отображением $C \to C/mC$. Откуда $\mathrm{Ker}\,\varphi = mC$.

22.53. Возьмите $A = \mathbb{Q}$, а в качестве C_i можно взять неограниченные периодические группы.

22.62. Поскольку C есть p-группа, то p-чисто точная последовательность $0 \to B \to A \to A/B \to 0$ дает точную последовательность $0 \to B \otimes C \to A \otimes C \to (A/B) \otimes C = 0$.

22.64. Пусть A, C — периодические группы и B, D — их базисные подгруппы соответственно. Тогда $A \otimes C \cong B \otimes D$. Здесь B и D — прямые суммы циклических групп, то же должно иметь место для $B \otimes D$.

22.65. Точная последовательность $0 \to B \to A \to A/B \to 0$ индуцирует точную последовательность

$$0 \to B \otimes C \to A \otimes C \to (A/B) \otimes C \to 0.$$

Здесь $(A/B) \otimes C$ есть p-делимая группа без кручения, т.е. p-базисные подгруппы группы $B \otimes C$ одновременно являются p-базисными подгруппами группы $A \otimes C$. Повторяя эти рассуждения, получаем, что $B \otimes D$ есть p-базисная подгруппа группы $A \otimes C$.

22.66. Проверьте сначала, что ядро естественного эпиморфизма $A \otimes C \to A/t(A) \otimes C/t(C)$ является подгруппой, порожденной подгруппами $A \otimes t(C)$ и $t(A) \otimes C$ (покажите, что последние группы можно отождествить с подгруппами группы $A \otimes C$). Далее, обоснуйте, почему

$$A \otimes t(C) \cong [t(A) \otimes t(C)] \oplus [A/t(A) \otimes t(C)],$$
$$t(A) \otimes C \cong [t(A) \otimes t(C)] \oplus [t(A) \otimes C/t(C)].$$

Доказательство вытекает из того, что пересечение последних групп совпадает с $t(A) \otimes t(C)$.

22.68. 5) Если $(a_{i_1} + \ldots + a_{i_k},\, m,\, c)$ $(a_i \in A_i)$ — образующий элемент группы $\mathrm{Tor}(A,\, C)$, то $m(a_{i_1} + \ldots + a_{i_k}) = 0 = m\,c$. Значит, $ma_{i_1} = \ldots = ma_{i_k} = m\,c = 0$. Поэтому в группе $\mathrm{Tor}(A,\, C)$ выполнено равенство

$$(a_{i_1} + \ldots + a_{i_k},\, m,\, c) = (a_{i_1},\, m,\, c) + \ldots + (a_{i_k},\, m,\, c).$$

Тройки вида $(a_i,\, m,\, c)$ при фиксированном i порождают подгруппу группы $\mathrm{Tor}\,(A,\, C)$, изоморфную группе $\mathrm{Tor}\,(A_i,\, C)$. Эти подгруппы порождают подгруппу, являющуюся их прямой суммой и совпадающую с группой $\mathrm{Tor}\,(A,\, C)$.

23. p-группы

23.3. В сепарабельной p-группе A все подгруппы $A\,[p^n]$ замкнуты. Если G — замкнутая подгруппа, то $G\,[p^n] = G \cap A\,[p^n]$ — также замкнутая подгруппа. Пусть теперь G — чистая подгруппа и подгруппа $G\,[p^n]$ замкнута в $A\,[p^n]$ при некотором n. Тогда подгруппа $G\,[p]$ замкнута в $A\,[p]$. Предположим, что G не замкнута, т.е. $(A/G)^1 \neq 0$. Значит, в A/G существует смежный класс $a + G$ порядка p и бесконечной высоты. Так как G чиста, то в качестве a можно выбрать элемент порядка p. Для любого k существуют такие элементы $x \in A$ и $g \in G$, что $p^k x = a + g$. Откуда $p^{k+1}x = pg \in G$. Тогда $p^{k+1}h = pg$ для некоторого $h \in G$. Имеем $p^k(x - h) = a + (g - p^k h)$, где $g - p^k h \in G\,[p]$, т.е. a лежит в замыкании подгруппы $G\,[p]$ и $a \in G\,[p] \subseteq G$. Противоречие.

23.4. Очевидно, $G \cap C = 0$ и $G + C$ содержит цоколь группы A. Запишем элемент $a \in A\,[p]$ в виде $a = b + c$ $(b \in B\,[p] = G\,[p],$ $c \in C\,[p])$. Тогда высота элемента a в $G + C$ больше или равна $\min(h(b),\, h(c))$, а последнее число равно высоте элемента a в группе A. Следовательно, подгруппа $G + C$ чиста в A и, значит, $G + C = A$.

23.5. Существование подгруппы C следует из леммы Цорна.

Докажем по индукции, что $C \cap p^n A \subseteq p^n C$. Пусть $n = 1$ и $pa = c \in C$, где $a \in A$. Если $a \notin C$, то в силу максимальности подгруппы C существует элемент $b \in \langle C,\, a\rangle$ порядка p, не лежащий в S. Пусть $b = -c' + ka$ для некоторого $c' \in C$ и некоторого целого числа k $(1 \leqslant k \leqslant p-1)$, которое без ограничения общности можно считать равным 1. Откуда $pc' = p(a - b) = pa = c$. Предположим теперь, что $C \cap p^n A \subseteq p^n C$ при некотором $n \geqslant 1$, и пусть для $a \in A$ имеет место включение $p^{n+1}a \in C$. По доказанному $p^{n+1}a = pc$ при некотором $c \in C$. Из плотности S в $A\,[p]$ и включения $p^n a - c \in A\,[p]$ следует существование такого $d \in S$, что $p^n a - c - d \in p^n A$. По предположению индукции для некоторого $c_1 \in C$ имеем $p^n c_1 = c + d$. Откуда $p^{n+1}c_1 = pc = p^{n+1}a$. Чистота подгруппы C доказана.

Так как C чиста, то в смежных классах порядка p группы A/C могут быть выбраны в качестве представителей элементы порядка p группы A. Из плотности S следует, что элементы порядка p группы A/C имеют бесконечную высоту в A/C. Значит, A/C — делимая группа и подгруппа C плотна в A.

23.17. Редуцированные периодически полные p-группы A могут быть охарактеризованы как группы, удовлетворяющие условию $\mathrm{Pext}(X,\, A) = 0$ для любой p-группы X. В частности, $\mathrm{Pext}\,(\mathbb{Z}_{p^\infty},\, A) = 0$. Для любой p-группы X существует чисто точная последовательность $0 \to C \to X \to \oplus\mathbb{Z}_{p^\infty} \to 0$, где C — прямая сумма циклических групп. Тогда точная последовательность

$$\mathrm{Pext}\,(\oplus\mathbb{Z}_{p^\infty},\, A) \cong \prod \mathrm{Pext}\,(\mathbb{Z}_{p^\infty},\, A) \to \mathrm{Pext}\,(X,\, A) \to \mathrm{Pext}\,(C,\, A) = 0$$

доказывает утверждение.

23.26. Пусть A/G есть прямая сумма делимой и периодически полной группы. Делимая подгруппа G^-/G чиста в A/G, поэтому подгруппа G^- чиста в A.

Для доказательства необходимости предположим, что A — квазиполная группа, и H — замыкание неограниченной чистой подгруппы G группы A, причем замыкание взято в группе $\overline{B}$, где B — базисная подгруппа группы A. Тогда H служит для $\overline{B}$ прямым слагаемым. Откуда $A + H = \overline{B}$. В силу квазиполноты $(A \cap H)/G = (A/G)^1$ — делимая группа. Поэтому группа A/G изоморфна прямой сумме делимой группы и группы $A/(A \cap H) \cong (A + H)/H = \overline{B}/H$, которая изоморфна прямому слагаемому группы $\overline{B}$.

24. Группы без кручения

24.7. Рассмотрите ранги подгрупп $A(t)$.

Чтобы построить пример группы с данным свойством, в группе $\mathbb{Q}a \oplus \mathbb{Q}b$ выберите такую подгруппу A, что для каждого простого числа p_n выполняется равенство $\chi_A(a + p_n b) = (0, \dots, 0, \infty, \dots)$, где ∞ стоит на n-месте.

24.14. Пусть A — p-чистая подгруппа группы $\widehat{\mathbb{Z}}_p$ и $\xi \in A$. Если $\xi = s_k p^k + s_{k+1}p^{k+1} + \dots$ — канонический вид числа ξ, то $s_k + s_{k+1}p + \dots \in A$. Значит, группа A содержит p-адическую единицу. Поэтому $A + p\widehat{\mathbb{Z}}_p = \widehat{\mathbb{Z}}_p$. Так как $pA = A \cap p\widehat{\mathbb{Z}}_p$, то

$$A/pA = A/(A \cap p\widehat{\mathbb{Z}}_p) \cong (A + p\widehat{\mathbb{Z}}_p)/p\widehat{\mathbb{Z}}_p = \widehat{\mathbb{Z}}_p/p\widehat{\mathbb{Z}}_p \cong \mathbb{Z}_p.$$

Пусть $A = B \oplus C$, где $B \neq 0$, $C \neq 0$. Тогда $A/pA \cong B/pB \oplus C/pC \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, противоречие.

24.15. б) Если $pA \neq A$, то существует мономорфизм $A \to \widehat{\mathbb{Z}}_p$, p-базисные подгруппы группы A должны быть циклическими.

24.31. 4) Достаточно показать, что ни для какого простого числа p группа $\mathbb{Z}_p$ не является W-группой. Последнее очевидно, так как $\operatorname{Ext}(\mathbb{Z}_p, \mathbb{Z}) \cong \mathbb{Z}_p$.

5) В противном случае она не является конечно порожденной (19.19). Тогда для некоторой существенной свободной подгруппы F этой группы G периодическая группа G/F бесконечна. Точная последовательность $0 \to F \to G \to G/F \to 0$ индуцирует точную последовательность

$$\operatorname{Hom}(F, \mathbb{Z}) \to \operatorname{Ext}(G/F, \mathbb{Z}) \to \operatorname{Ext}(G, \mathbb{Z}) = 0.$$

Здесь группа $\operatorname{Hom}(F, \mathbb{Z})$ — счетная, а группа $\operatorname{Ext}(G/F, \mathbb{Z})$ имеет мощность континуума.

24.36. 2) Необходимость очевидна, поскольку изоморфизм сохраняет p-типы элементов. Пусть теперь B, G — связные группы из R_p и $\tau_p^B(b) = \tau_p^G(g)$ для некоторых $b \in B \setminus pB$, $g \in G \setminus pG$. Существуют натуральные числа n, m со свойствами

$$H_p^B(b) \subseteq H_p^G(ng),\ H_p^G(g) \subseteq H_p^B(mb).$$

Элементы b и g являются p-образующими групп B и G соответственно. Поэтому существуют гомоморфизмы $\varphi\colon B \to G$, $\psi\colon G \to B$ со свойствами $\varphi b = ng$, $\psi g = mb$. Так как ненулевые гомоморфизмы связных групп в редуцированные группы являются мономорфизмами, то $\psi\varphi = (nm)\,1_B$ и $\varphi\psi = nm\,1_G$. Откуда

$$nmB = (\psi\varphi)B \subseteq \psi G \subseteq B \text{ и } nmG = \varphi\psi G \subseteq \varphi B \subseteq G.$$

Значит, группы B и G квазиизоморфны, но квазиизоморфизм связных групп влечет изоморфизм.

25. Смешанные группы

25.1. 5) Достаточно доказать для случая, когда $n = p$ — простое число. Пусть $pA = T' \oplus G'$, где T' — периодическая часть группы pA. Очевидно, что $T' = pT$, где $T = t(A)$. Пусть G есть T-высокая подгруппа группы A, содержащая G', т.е. G — максимальная подгруппа в A со свойствами: $G \cap T = 0$ и $G' \subseteq G$. Если $a \in A$ и $pa = b + c$ ($b \in T$, $c \in G$), то $b \in T' = pT$ и, значит, $A = T \oplus G$.

25.4. в) Допустим, что $A_1 = T_1 \oplus G$. Тогда из равенства $b_i = h_i + g_i$ ($h_i \in T_1$, $g_i \in G$) следует, что $p_i h_i + p_i g_i = p_i b_i = b_0 - a_i = (h_0 - a_i) + g_0$. Приравнивая слагаемые, лежащие в T_1, получаем $p_i h_i = h_0 - a_i$ при $i = 1, 2, \dots$. Для одного из наших простых чисел, пусть это будет p_j, справедливо равенство $p_j h = h_0$ при некотором $h \in T_1$. Откуда $p_j(h - h_j) = a_j$, противоречие.

25.5. Если $A_2 = T_2 \oplus G$, то в силу $pb_{i+1} - b_i \in T_2$ группа G была бы p-делимой. Это противоречит тому, что группа $\prod \langle a_i \rangle$ не содержит ненулевых p-делимых подгрупп.

25.9. Используйте группу из 25.3 или в группе из 25.4 возьмите такую подгруппу C, что $A_1 \subseteq C \subset \prod \langle a_i \rangle$ и $C/T_1 \cong \mathbb{Q}$. Допустив существование эпиморфизма $C \to T_1$, рассмотрите образ элемента b_0 при этом отображении.

25.11. $A = \operatorname{Ext}(\mathbb{Q}/\mathbb{Z}, T) \oplus D$, где D — делимая часть группы T.

25.13. Если бы группа A расщеплялась, то существовал бы такой гомоморфизм $\xi\colon G \to T$, что $\eta g = \xi g + pT$ при любом $g \in G$. Так как группа G алгебраически компактна, то группа ξG должна быть ограниченной, а тогда образ ξG в T/pT был бы конечным. Противоречие.

25.14. Ввиду определения подгруппы $p^\sigma G$ для предельных порядковых чисел σ, достаточно показать, что если это равенство выполняется для σ, то оно выполняется и для $\sigma + 1$. Пусть $a \in A \cap p^{\sigma+1}G$ и $a = pg$ для некоторого $g \in p^\sigma G$. Тогда $g \in A$, так как G/A — группа без кручения. Откуда $g \in A \cap p^\sigma G = p^\sigma A$ и, значит, $a \in p^{\sigma+1}A$.

25.15. Пусть A — редуцированная группа и $\mathbb{H}(a) \leqslant \mathbb{H}(b)$ для a, $b \in A$. Нужно показать, что $o(b) \mid o(a)$. Если $o(a) = \infty$, то всегда $o(b) \mid o(a)$. Заметим, что если $0 \neq c \in A$, то $h_p^*(c) = \infty$ тогда и только тогда, когда существует порядковое число τ со свойством $c \in p^\tau A = p^{\tau+1}A$. Если элемент c лежит в p-компоненте A_p группы A, то A_p, значит, и A — нередуцированные группы. Поэтому рассмотрим случай: $o(a) = k$, $o(b) = s$, где k, $s < \infty$. Пусть $k = p_1^{k_1} \dots p_n^{k_n}$, $s = p_1^{r_1} \dots p_n^{r_n}$, $\mathbb{H}(a) = [\sigma_{ij}]$ и $\mathbb{H}(b) = [\delta_{ij}]$ (где $\sigma_{ij} = \infty$ при $i \geqslant n$ или $j \geqslant k_1, \dots, k_n$, $\delta_{ij} = \infty$ при $i \geqslant n$ или $j \geqslant r_1, \dots, r_n$). Так как $sb = 0$, то $\mathbb{H}(sb)$ состоит из одних ∞. Если $\mathbb{H}(sa) = \mathbb{H}(sb)$, то это влечет $o(b) \mid o(a)$. Поскольку $\sigma_{ij} \leqslant \delta_{ij}$, то неравенство $\sigma_{ij} < \infty$ ($i = 1, \dots, n$) влечет $0 \leqslant j \leqslant k_i - r_i$. Откуда $k_i \geqslant r_i$ и, значит, $o(b) \mid o(a)$.

25.18. Пусть a, $b \in A$, $\mathbb{H}(a) \leqslant \mathbb{H}(b)$, $a = (\dots, a_i, \dots)$, $b = (\dots, b_i, \dots)$. Так как $\mathbb{H}(a) \leqslant \mathbb{H}(b_i)$ и $\pi(A_i) \cap \pi(A_j) = \varnothing$ при $i \neq j$, то $\mathbb{H}(a_i) \leqslant \mathbb{H}(b_i)$. Поэтому существуют $\varphi_i \in \operatorname{End} A_i$, $\varphi_i a_i = b_i$, а тогда существует $\varphi \in \operatorname{End} A$ со свойством $\varphi a = b$ ($\pi_i\varphi a = \varphi_i\pi_i a$, где $\pi_i\colon A \to A_i$ — проекция).

26. Кольца эндоморфизмов

26.7. 1) Если α, β удовлетворяют равенствам $\alpha\beta = \varepsilon$ и $\beta\alpha = \varepsilon'$, то из $\beta\alpha\beta = \beta\varepsilon = \varepsilon'\beta$ и $\alpha\beta\alpha = \varepsilon\alpha = \alpha\varepsilon'$ следует, что $\beta^* = \beta\alpha\beta\,|\,B$ и $\alpha^* = \alpha\beta\alpha\,|\,B'$ — это гомоморфизмы $\beta^*\colon B \to B'$ и $\alpha^*\colon B' \to B$. Теперь равенства $(\alpha\beta\alpha)(\beta\alpha\beta) = \varepsilon$ и $(\beta\alpha\beta)(\alpha\beta\alpha) = \varepsilon'$ показывают, что β^* и α^* — взаимно обратные отображения, откуда $B \cong B'$. Обратно, если $\beta^*\colon B \to B'$ и $\alpha^*\colon B' \to B$ — взаимно обратные изоморфизмы, то для $\beta = \beta^*\varepsilon$ и $\alpha = \alpha^*\varepsilon'$ выполнены равенства $\alpha\beta = \varepsilon$ и $\beta\alpha = \varepsilon'$.

2) а)$\Rightarrow$ б). Так как f — проекция, а u — автоморфизм, то $(1-f)M = \ker f = u^{-1}(\ker e) = u^{-1}(1-e)M \cong (1-e)M$ и $fM = u^{-1}(eM) \cong eM$. б) $\Rightarrow$ а). Если $v\colon fM \to eM$, $w\colon (1-f)M \to (1-e)M$ — изоморфизмы, то пусть u — такой автоморфизм, что $u(x+y) = v(x) + w(y)$, где $x \in fM$, $y \in (1-f)M$. Тогда $u^{-1}(v(x)+w(y)) = x+y$ для всех $v(x) \in eM$, $w(y) \in (1-e)M$. Поэтому $u^{-1}(e(u(x+y))) = u^{-1}(e(v(x))) = u^{-1}(v(x)) = x$ и, значит, $u^{-1}eu = f$.

26.15. Пусть $\alpha,\ \beta \in \operatorname{End} A$ и $\alpha\beta + U_x$ — окрестность элемента $\alpha\beta$. Так как U_x — левый идеал и $U_{\beta x}\beta \subseteq U_x$, то непрерывность умножения получается из включений $(\alpha + U_{\beta x})(\beta + U_x) \subseteq \alpha\beta + U_{\beta x}\beta + U_x \subseteq \alpha\beta + U_x$. Таким образом, $\operatorname{End} A$ — топологическое кольцо. Предположим, что $\{\alpha_i\}_{i\in I}$ — сеть Коши. В рассматриваемом случае множество индексов I частично упорядочено с помощью порядка, обратного к порядку на конечных подмножествах группы A. Сеть Коши удовлетворяет следующему условию: если дано $x \in A$, то $\alpha_i - \alpha_j \in U_x$ при всех $i,\ j$, больших некоторого $i_0 \in I$, т.е. при больших индексах $\alpha_i x$ — это один и тот же элемент из A. Поэтому если определить $\alpha\, x$ как общее значение всех таких $\alpha_i x$, то $\alpha \in \operatorname{End} A$ и $\alpha - \alpha_i \in U_x$ при всех таких i.

26.17. Пусть $\sigma \in \operatorname{End} A$ и $a_1,\ \ldots\ ,\ a_n$ — конечное подмножество группы A. Это подмножество можно вложить в конечное слагаемое G группы A. Достаточно установить плотность E_0 в $\operatorname{End} A$, а для этого нужно показать, что $V = E_0 \cap (\sigma + U_G) \neq \varnothing$. Если $\pi\colon A \to G$ — проекция, то $1 - \pi \in U_G$. Так как U_G — левый идеал, то $\sigma(1-\pi) \in U_G$ и, значит, $\sigma\pi = \sigma - \sigma(1-\pi) \in V$.

26.27. 1) Если A — эндоартинова группа, то среди ее вполне инвариантных подгрупп вида nA найдется минимальная mA. Тогда mA — делимая группа и $A = B \oplus mA$, где $B \cong A/mA$ и, значит, B — ограниченная группа. p-компоненты являются вполне инвариантными подгруппами, поэтому их должно быть конечное число. Обратно, пусть группа A имеет указанный вид. Достаточно проверить эндоартиновость групп B и D. Для этого используйте известное строение этих групп.

2) Предположим, что A — эндонетерова группа. Семейство вполне инвариантных подгрупп вида $A\,[n]$ имеет максимальный элемент $A\,[m]$; $A\,[m]$ — наибольшая периодическая подгруппа группы A и, значит, $A = A\,[m] \oplus C$, где C — группа без кручения. Подгруппа $A\,[m]$ вполне инвариантна в A и $C \cong A/A\,[m]$. Прообраз любой вполне инвариантной подгруппы из $A/A\,[m]$ в A будет вполне инвариантной подгруппой группы A. Группы $A\,[m]$ и C эндонетеровы, а тогда группа A также эндонетерова.

26.34. Если $\operatorname{End} A$ — тело, то всякий $0 \neq \alpha \in \operatorname{End} A$ есть автоморфизм. Поэтому $pA = 0$ или $pA = A$ для всякого простого p. Если $pA = 0$ для некоторого p, то A — элементарная p-группа. Так как A неразложима, то $A \cong \mathbb{Z}_p$. Во втором случае A — неразложимая делимая группа; так как умножение на p является эндоморфизмом с нулевым ядром, то A — группа без кручения. Таким образом, $A \cong \mathbb{Q}$.

Обратно, кольца эндоморфизмов групп $\mathbb{Q}$ и $\mathbb{Z}_p$ являются простыми полями характеристики 0 и p соответственно.

26.35. Если $E = \operatorname{End} A$ — простое кольцо, то для любого простого числа p или $pE = 0$, или $pE = E$. В первом случае легко следует, что A — элементарная p-группа. Если $pE = E$ для любого простого p, то E, а значит, и A делимы. Цоколь в E служит идеалом, поэтому E — кольцо без кручения. Умножение на p^{-1} — эндоморфизм группы A, значит, A — группа без кручения. Таким образом, $A = \oplus\mathbb{Z}_p$ или $A = \oplus\mathbb{Q}$. Эндоморфизмы группы A, отображающие ее на подгруппы конечного ранга, образуют ненулевой идеал в E. Следовательно, A — конечная прямая сумма.

Достаточность очевидна.

27. Аддитивные группы колец

27.3. а) Для каждого $\eta \in \operatorname{End} A$ отображения $a \to \eta(\varphi a)$ и $a \to (\varphi a)\eta$ являются гомоморфизмами $A \to \operatorname{End} A$. Поэтому среди образующих группы $I(A)$ имеются $\eta(\varphi a)$ и $(\varphi a)\eta$ при всех $a \in A$, т.е. $I(A)$ — идеал кольца $\operatorname{End} A$.

б) Пусть R — кольцо на A. С каждым элементом $a \in A$ можно связать левое умножение $\lambda_a\colon x \to ax$. Соответствие $\varphi\colon a \mapsto \lambda_a$ является гомоморфизмом A в $(\operatorname{End} A)^+$ и, значит, в группу $I(A)$. Подгруппа C является левым идеалом в R тогда и только тогда, когда каждый гомоморфизм λ_a переводит C в себя; то же рассуждение применимо к правому умножению. Поэтому если $I(A)C \subseteq C$, то C — идеал в каждом кольце R на A. Обратно, всякий гомоморфизм $\varphi \in \operatorname{Hom}(A, (\operatorname{End} A)^+)$ дает некоторое кольцевое умножение, если произведение элементов $a,\ c \in A$ положить равным $ac = (\varphi a)c$. Значит, если C — идеал в каждом кольце на A, то $(\varphi a)c \in C$ при $c \in C$, т.е. $I(A)C \subseteq C$.

в) Либо редуцированная p-группа A обладает циклическими слагаемыми порядка $\geqslant p^k$ для сколь угодно больших k, либо в A найдется циклическое слагаемое максимального порядка и A — ограниченная группа. В обоих случаях образы ее циклических слагаемых в группе $(\operatorname{End} A)^+$ порождают периодическую часть этой группы и поэтому последняя совпадает с $I(A)$.

27.8. Рассмотрите $\mathbb{Z}_n \oplus \mathbb{Z}_n$.

27.12. Из чисто точной последовательности $0 \to C \to A \to A/C \to 0$ получим точные последовательности

$$0 \to C \otimes C \to A \otimes C \to (A/C) \otimes C \to 0,$$
$$0 \to A \otimes C \to A \otimes A \to A \otimes (A/C) \to 0.$$

Группы $(A/C) \otimes C$ и $A \otimes (A/C)$ делимы, что дает точную последовательность

$$0 \to C \otimes C \to A \otimes A \to [(A/C) \otimes C] \oplus [A \otimes (A/C)] \to 0.$$

Последовательность $0 \to \mathrm{Hom}(A\otimes A,\, A) \to \mathrm{Hom}(C\otimes C,\, A)$ также точна. Это означает, что любое $\nu\colon C\times C \to A$ может иметь не более одного продолжения $\mu\colon A\times A\to A$.

27.22. Пусть $pR \not\subseteq M$ ни для какого простого числа p. Тогда $pR+M=R$, т.е. группа $(R/M)^+$ делима, она обязана не иметь кручения, так как иначе для некоторого простого числа p имело бы место строгое включение $M\subset p^{-1}M$.

28. Простейшие свойства полей

28.1. а) Если $\sqrt{n}\notin\mathbb{Q}$; б) если $n<0$; в) нет; г) если $n=2$ при $p=3$; $n=2,\,3$ при $p=5$; $n=3,\,5,\,6$ при $p=7$.

28.12. Если $e(x)=1+a_1x+a_2x^2+\ldots=1+p(x)\in K\,[[x]]$, то проверьте, что $\bigl(\sum\limits_{j=0}^{\infty}(-1)^j(p(x))^j\bigr)e(x)=1$. Если $0\ne c_0\in K$ и $f(x)=c_0+c_1x+c_2x^2+\ldots$, то $f(x)=c_0e(x)$, где c_0 и $e(x)$ — обратимые элементы кольца $K\,[[x]]$, значит, $f(x)$ обратим в $K\,[[x]]$. Таким образом, каждый элемент $g(x)\in K\,[[x]]$ представим в виде $g(x)=x^mf(x)$, где $f(x)$ — обратимый элемент в $K\,[[x]]$. Тогда $g(x)/u(x)=x^{m-n}f(x)/\varphi(x)$, здесь $f(x)/\varphi(x)=h(x)\in K\,[[x]]$ и $s=n-m$.

28.15. Действительно, $\sqrt{2}=-\dfrac{9}{2}\theta+\dfrac{1}{2}\theta^3$, $\sqrt{3}=\dfrac{11}{2}\theta-\dfrac{1}{2}\theta^3$, $\sqrt{6}=-\dfrac{5}{2}+\dfrac{1}{2}\theta^2$.

28.20. Указанные числа образуют подкольцо в соответствующих полях. Покажите, что только они являются целыми алгебраическими. Число $r+s\sqrt{d}\in\mathbb{Q}(\sqrt{d})$ удовлетворяет уравнению $x^2-2rx+(r^2-ds^2)=0$. Поэтому число $\alpha=r+s\sqrt{d}$ является целым алгебраическим в точности тогда, когда его след $s(\alpha)=2r$ и норма $n(\alpha)=r^2-ds^2\in\mathbb{Z}$.

Пусть $d\equiv 2,\,3 \pmod 4$. Так как $2r\in\mathbb{Z}$, то $r\in\mathbb{Z}$, либо $r=u+\dfrac{1}{2}$, где $u\in\mathbb{Z}$. Если $r\in\mathbb{Z}$, то $ds^2\in\mathbb{Z}$ и, значит, $s\in\mathbb{Z}$. Второе же предположение невозможно. Действительно, из $r=u+\dfrac{1}{2}$ следует, что $s=t+\dfrac{1}{2}$, где $t\in\mathbb{Z}$. Поэтому $4(r^2-ds^2)=1-d+4(u^2+u-dt^2-dt)$, $d\equiv 1 \pmod 4$, что противоречит условию на d.

Пусть $d\equiv 1 \pmod 4$. Если $r=a/2$ и $s=b/2$, то $2r=a$, $r^2-ds^2=(1/4)(a^2-db^2)$. Откуда условие $2r,\,r^2-ds^2\in\mathbb{Z}$ влечет $a,b\in\mathbb{Z}$, причем a и b обязаны иметь одинаковую четность. Необходимость установлена. Если a и b — четные, то $2r=a$, $r^2-ds^2=(1/4)(a^2-db^2)\in\mathbb{Z}$. Если же $a=2u+1$, $b=2t+1$, где $u,\,t\in\mathbb{Z}$, то $(1/4)(a^2-db^2)=(1/4)(1-d)+u^2+u-dt^2-dt\in\mathbb{Z}$.

28.22. Если $\alpha\alpha^{-1}=1$, то $n(\alpha)n(\alpha^{-1})=1$. Откуда $n(\alpha)=\pm1$. Так как $n(\alpha)=r^2-ds^2=\alpha(r-s\sqrt{d})$, то из $n(\alpha)=\pm1$ следует обратимость α.

28.23. Если $d\equiv 2,\,3 \pmod 4$, то целые алгебраические числа можно записать в виде $\alpha=x+y\sqrt{d}$, где $x,\,y\in\mathbb{Z}$, $n(\alpha)=x^2-dy^2=1$, а при $d\equiv 1 \pmod 4$ в виде $\alpha=x/2+y/2\sqrt{d}$, где x и y — целые числа одинаковой четности, $n(\alpha)=(x^2-dy^2)/4=1$. Рассмотрите четыре случая.

1) При $d=-1$ получается кольцо целых гауссовых чисел $\mathbb{Z}[i]$. Уравнение $x^2-dy^2=1$ примет вид $x^2+y^2=1$ и имеет четыре решения: $x=\pm1$, $y=0$; $x=0$, $y=\pm1$. Им соответствуют обратимые числа ±1, $\pm i$, которые и составляют группу обратимых элементов $U(\mathbb{Z}[i])$ кольца $\mathbb{Z}[i]$.

2) Если $d=-2$, то уравнение $x^2+2y^2=1$ имеет только два решения: $x=\pm1$, $y=0$, которым соответствуют числа ±1.

3) Если $d=-3$, то уравнение $x^2+3y^2=4$ имеет шесть решений: $x=\pm2$, $y=0$; $x=\pm1$, $y=1$; $x=\pm1$, $y=-1$. Им соответствуют числа ±1, $\pm1/2+(1/2)i\sqrt{3}$, $\pm1/2-(1/2)i\sqrt{3}$.

4) В случае $d\leqslant -5$ уравнения $x^2-dy^2=1$ (при $d\equiv 2,\,3 \pmod 4$) имеют только два решения: $x=\pm1$, $y=0$; уравнения $x^2-dy^2=4$ (при $d\equiv 1 \pmod 4$) также имеют только два решения: $x=\pm2$, $y=0$.

28.27. $\mathbb{Z}_p$.

28.28. $x=a$.

28.29. в) Для каждого элемента x в поле существует его p-я степень x^p. Различные элементы имеют различные степени, так как $x^p-y^p=(x-y)^p$. Следовательно, в поле существует столько же p-х степеней, сколько самих элементов.

28.32. $\varphi(1)=1$ для каждого автоморфизма φ. Откуда $\varphi(n)=\varphi(1)+\ldots+\varphi(1)=n\cdot1=n$ при $n\in\mathbb{N}$. Поэтому равенства $\varphi(-a)=-\varphi(a)$ и $\varphi\left(ab^{-1}\right)=\varphi(a)\,(\varphi(b))^{-1}$ показывают, что φ действует тождественно на $\mathbb{Q}$. Если же $\varphi\in\mathrm{Aut}\,\mathbb{R}$, то ограничение $\varphi\,|\,\mathbb{Q}=1_{\mathbb{Q}}$. Так как для каждого $x\in\mathbb{R}$, $x>0$, найдется $y\in\mathbb{R}$ со свойством $x=y^2$, то $\varphi(x)=(\varphi(y))^2>0$. Поэтому из $x<z$ следует $\varphi(x)<\varphi(z)$. Далее воспользуйтесь тем, что $\mathbb{Q}$ плотно в $\mathbb{R}$.

28.33. $x+iy\mapsto x-iy$ — единственный нетождественный такой автоморфизм ($x,\,y\in\mathbb{R}$).

28.34. $x+\sqrt{2}y\mapsto x-\sqrt{2}y$ — единственный такой автоморфизм ($x,\,y\in\mathbb{Q}$).

28.35. При $m/n=r^2\in\mathbb{Q}\backslash\{0\}$ (поля совпадают).

28.36. а) $\{-3-2\sqrt{2},\,-1\}$; б) $\varnothing$; в) $\{2-\sqrt{2},\,1+\sqrt{2}\}$; г) $\{\sqrt{2},\,-2-\sqrt{2}\}$; д) $\{-2,\,3-\sqrt{2}\}$; е) $\{\sqrt{2},\,6-3\sqrt{2}\}$.

28.38. $f(x)=x^3+3x^2+x+3$.

28.40. б) и в) не имеют.

28.41. а) $\varnothing$; б) $\{7,\,10\}$; в) $\{2,\,7\}$; г) $\{2\}$; д) $\varnothing$; е) $\varnothing$.

28.44. Если $b\ne0$ и $a^2+ab+b^2=0$, то $a^3-b^3=0$, откуда $\left(ab^{-1}\right)^3=1$. Тогда $a=b$ (это влечет $ab=0$ и, значит, $a=b=0$), либо $3\,|\,2^n-1$, что неверно.

28.45. а) Заметить, что $k\mapsto k^{-1}$ — биекция и $\sum\limits_{k=1}^{p-1}k^{-1}=\sum\limits_{k=1}^{p-1}k$. б) Используйте формулу $1+2^2+\ldots+n^2=\dfrac{n\,(n+1)\,(2n+1)}{6}$.

28.47. а) $x+2$ (над $\mathbb{Z}_3$), 1 (над $\mathbb{Z}_5$); б) x^2+x+2 (над $\mathbb{Z}_3$), 1 (над $\mathbb{Z}_5$).

28.48. Пусть $f(x) = a(x)d(x)$, $g(x) = b(x)d(x)$, где $a(x), b(x), d(x) \in \mathbb{Q}[x]$, $\deg d(x) > 0$. Вынося общие знаменатели и общие наибольшие делители числителей коэффициентов этих многочленов и применяя лемму Гаусса (лемма 14.2), получим $f(x) = a_1(x)d_1(x)$, $g(x) = b_1(x)d_1(x)$, где $a_1(x), b_1(x), d_1(x) \in \mathbb{Z}[x]$ и старший коэффициент $d_1(x)$ не делится на p. Переходя к полю вычетов по модулю p, получим общий делитель для $f(x)$ и $g(x)$ над этим полем, что невозможно.

Многочлены $f(x) = x$, $g(x) = x + p$ взаимно просты над $\mathbb{Q}$ и равны x над полем $\mathbb{Z}_p$.

28.49. Если $f(x)$ и $g(x)$ взаимно просты, то $f(x)u(x) + g(x)v(x) = c$, где $u(x), v(x) \in \mathbb{Z}[x]$ и $c \in \mathbb{Z}$; $f(x)$ и $g(x)$ взаимно просты над полем $\mathbb{Z}_p$ для любого p, не делящего c. Для доказательства обратного утверждения использовать предыдущее упражнение.

28.50. а) $(x+1)^3\left(x^2+x+1\right)$; б) $(x+3)\left(x^2+4x+2\right)$;
в) $\left(x^2+x+1\right)\left(x^2+2x+4\right)$.

28.51. $f_1 = x^2$, $f_2 = x^2+1 = (x+1)^2$, $f_3 = x^2+x = x(x+1)$, $f_4 = x^2+x+1$ неприводим.

$f_1 = x^3$, $f_2 = x^3+1 = (x+1)\left(x^2+x+1\right)$, $f_3 = x^3+x = x(x+1)^2$, $f_4 = x^3+x^2 = x^2(x+1)$, $f_5 = x^3+x+1$ неприводим, $f_6 = x^3+x^2+1$ неприводим, $f_7 = x^3+x^2+x = x\left(x^2+x+1\right)$, $f_8 = x^3+x^2+x+1 = (x+1)^3$.

28.52. $f_1 = x^2+1$, $f_2 = x^2+x+2$, $f_3 = x^2+2x+2$. $f_1 = x^3+2x+1$, $f_2 = x^3+2x+2$, $f_3 = x^3+x^2+2$, $f_4 = x^3+2x^2+1$, $f_5 = x^3+x^2+x+2$, $f_6 = x^3+x^2+2x+1$, $f_7 = x^3+2x^2+x+1$, $f_8 = x^3+2x^2+2x+2$.

28.53. Применив лемму Гаусса (лемма 14.2), из разложения на многочлены с рациональными коэффициентами получить разложение на многочлены с целыми коэффициентами. Многочлен $f = px^2 + (p+1)x + 1 = (px+1)(x+1)$ по модулю p равен $x+1$.

28.54. Используйте тот факт, что если элементы a и b циклической группы G не являются квадратами, то ab — квадрат в G. Действительно, множество H элементов из G, являющихся квадратами, есть подгруппа. Факторгруппы циклической группы — циклические. Если $C = cH$ — образующий факторгруппы G/H, то из $c^2 \in H$ следует $C^2 = c^2H = H$. Значит, $H = G$ или G/H — группа второго порядка и $ab \in aH \cdot bH = H$.

Отсюда следует, что по любому простому модулю p одно из чисел 2, 3, 6 сравнимо с квадратом ($2 \equiv 0^2$ при $p = 2$; $3 \equiv 0^2$ при $p = 3$; и по вышедоказанному $6 = 2 \cdot 3$ — квадрат в поле $\mathbb{Z}_p$ при $p > 3$, если 2 и 3 — не квадраты).

Многочлен

$$f(x) = \left(x - \sqrt{2} - \sqrt{3}\right)\left(x - \sqrt{2} + \sqrt{3}\right)\left(x + \sqrt{2} - \sqrt{3}\right) \cdot \\ \cdot \left(x + \sqrt{2} + \sqrt{3}\right) = x^4 - 10x^2 + 1$$

неприводим над полем $\mathbb{Q}$.

По доказанному существует $a \in \mathbb{Z}_p$, для которого $a^2 = 2$, или $a^2 = 3$, или $a^2 = 6$. Если $a^2 = 2$, то $x^4 - 10x^2 + 1 = \left(x^2 + 2ax - 1\right)\left(x^2 - 2ax - 1\right)$; если $a^2 = 3$, то $x^4 - 10x^2 + 1 = \left(x^2 + 2ax + 1\right)\left(x^2 - 2ax + 1\right)$; если $a^2 = 6$, то $x^4 - 10x^2 + 1 = \left(x^2 - 5 + 2a\right)\left(x^2 - 5 - 2a\right)$.

28.58. Индукцией по i ($0 \leqslant i \leqslant m$) доказать, что при надлежащей нумерации элементов $b_1, \ldots, b_n$ система $a_1, \ldots, a_i, b_{i+1}, \ldots, b_n$ является максимальной системой алгебраически независимых над K элементов в P.

28.59. 1) Покажите, что число максимальных идеалов не превосходит $[A : K]$. Далее покажите, что если элемент $a \in A$ не является нильпотентным, то идеал, максимальный во множестве идеалов, не пересекающихся с $\{a, a^2, \ldots\}$, является максимальным идеалом в A.

2) Используйте 1). Для получения единственности в 5) покажите, что во всяком представлении $A^{red} = \prod_{j=1}^{t} L_j$ поля L_j изоморфны факторалгебрам по всевозможным максимальным идеалам в A.

29. Поля разложения

29.5. б) Пример $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{Q}\left(\sqrt[4]{3}\right)$; в) пример $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}, i\right)$.

29.6. Пусть σ — вложение PF над F (в $\overline{L}$). Тогда σ тождественно на F (следовательно, и на K) и по предположению его ограничение на P отображает P в себя. Откуда $\sigma(PF) = \sigma(P)\sigma(F) = PF$, т.е. PF нормально над F.

Если P и F нормальны над K, то для любого вложения σ поля PF над K имеем $\sigma(PF) = \sigma(P)\sigma(F) = PF$. Аналогично доказывается нормальность $P \cap F$ над K.

29.8. $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{1}\right)$ — поле разложения (под $\sqrt[3]{2}$ понимается вещественный корень).

29.15. Достаточно показать, что $\Phi_p(x)$ неприводим над $\mathbb{Q}$. Неприводимость $\Phi_p(x)$ эквивалентна неприводимости

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1},$$

к которому применим критерий Эйзенштейна.

29.17. а) 1; б) 2; в) 2; г) 6, $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{1}\right)$ — поле разложения (под $\sqrt[3]{2}$ понимается вещественный корень); д) 8, $\mathbb{Q}\left(i, \sqrt[4]{2}\right)$ — поле разложения; е) $p-1$; ж) $\varphi(n)$; з) $p(p-1)$.

29.18. Конечность K влечет конечность P. Тогда $P^* = \langle\theta\rangle$, и θ будет примитивным элементом. Считаем K бесконечным.

Допустим, что число промежуточных полей конечно. Пусть $\alpha, \beta \in P$. Тогда найдутся $c_1, c_2 \in K$, $c_1 \neq c_2$, такие, что $E = K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Откуда $\alpha, \beta \in E$, т.е. $K(\alpha, \beta) = E$. По индукции получаем, что если $P = K(\alpha_1, \ldots, \alpha_n)$, то существуют $c_2, \ldots, c_n \in K$, для которых $P = K(\theta)$ и $\theta = \alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$.

Обратно, пусть $P = K(\theta)$ для некоторого θ, и $f = f_\theta(x)$ — минимальный многочлен для θ. Если $K \subset E \subset P$ и g — минимальный многочлен для θ над E, то g делит f. Но $P[x]$ — факториальное кольцо, поэтому g равен произведению некоторого числа множителей $x - \alpha_i$, где $\alpha_1, \ldots, \alpha_n$ — корни f. Следовательно, имеется лишь конечное число таких многочленов. Получаем отображение $E \mapsto g_E$ из множества промежуточных полей в конечное множество многочленов.

Пусть E_0 — подполе в E, порожденное над K коэффициентами многочлена g_E. Тогда g_E имеет коэффициенты в E_0 и является неприводимым над E_0, поскольку он неприводим над E. Стало быть, степень элемента θ над E_0 совпадает со степенью θ над E, а это дает равенство $E = E_0$. Таким образом, поле E однозначно определяется ассоциированным с ним многочленом g_E. Поэтому отображение $E \mapsto g_E$ инъективно.

29.20. Пусть $\alpha_1, \ldots, \alpha_r$ — различные корни f в алгебраическом замыкании $\overline{P}$ поля P, и m — кратность корня $\alpha = \alpha_1$ в f. Для всякого $1 \leqslant i \leqslant r$ существует изоморфизм $\sigma\colon P(\alpha) \to P(\alpha_i)$ над P, для которого $\sigma\alpha = \alpha_i$. Продолжим σ до автоморфизма $\overline{\sigma}$ поля $\overline{P}$. Так как коэффициенты f лежат в P, то $f^\sigma = f$. Заметим, что $f(x) = \prod_{i=1}^{r} (x - \sigma\alpha_i)^{m_i}$, где m_i — кратность α_i в f.

В силу однозначности разложения на множители заключаем, что $m_i = m_1$ и, следовательно, все m_i равны одному и тому же числу m. Если $f' \neq 0$, то f и f' имеют общий корень. Это невозможно, так как f неприводим. Откуда $f' = 0$. Значит, $\operatorname{char} P = p$ и $f(x) = g(x^p)$ для некоторого $g(x) \in P[x]$. Продолжая, получим наименьшее целое число $\mu \geqslant 0$ такое, что α^{p^μ} является корнем сепарабельного многочлена $h(x) \in P[x]$, для которого $f(x) = h(x^{p^\mu})$.

29.25. б) $\Rightarrow$ в). Соответствие $x \mapsto a \otimes 1$ продолжается до гомоморфизма $L[x] \to F \otimes_K L$ с ядром $f_a(x)L[x]$. Поэтому каждый элемент $y \in F \otimes_K L$ можно представить в виде $g(a \otimes 1)$ для некоторого $g(x) \in L[x]$. Если $y^t = 0$ для $t \in \mathbb{N}$, то $g(x)^t \in f_a(x)L[x]$. Так как $f_a(x)$ сепарабелен, то он не делится на квадрат никакого неприводимого многочлена над L. Поэтому $f_a(x)$ делит $g(x)$ и $y = g(a \otimes 1) = 0$.

в) $\Rightarrow$ а). Предположим, что а) не верно. Если $b \in F$ не является сепарабельным, то K имеет характеристику p и $f_b(x) = g(x^p)$ для некоторого $g(x) \in K[x]$. Если L — произвольное расширение поля K, содержащее корни p-й степени из коэффициентов многочлена $g(x)$, то $f_b(x) = (h(x))^p$ для $h(x) \in L[x]$. Так как $\deg h(x) < \deg f_b(x)$, то $0 \neq h(b \otimes 1) \in F \otimes_K L$ и $0 = f_b(b) \mapsto f(b \otimes 1) = h(b \otimes 1)^p = 0$.

в) $\Longleftrightarrow$ г). Так как F — конечномерная алгебра над K, то алгебра $A = F \otimes_K L$ конечномерна над L. Поэтому применима теорема Веддерберна-Артина. Следовательно, A является прямым произведением конечного числа полей тогда и только тогда, когда A не имеет ненулевых нильпотентных элементов.

29.26. а) $\Rightarrow$ б). Пусть $f_\alpha(x, K) = \prod_{i=1}^{r} (x - \alpha_i)^{m_i}$, где $\alpha = \alpha_1$ и α_i — различные корни многочлена $f_\alpha(x, K)$. Каждый корень α_i имеет одинаковую кратность p^μ и элемент $\alpha_i^{p^\mu}$ сепарабелен над K. Поэтому $a = \alpha^{p^\mu} \in K$. Тогда α есть корень многочлена $x^{p^\mu} - a$, делящегося на $f_\alpha(x, K)$. Следовательно, $f_\alpha(x, K) = x^{p^\mu} - a$.

г) $\Rightarrow$ а). Если $\alpha \in L \backslash K$ — сепарабельный элемент и $\sigma\colon K \to \overline{K}$ — вложение, то σ имеет продолжения до $K(\alpha) \to \overline{K}$, число которых равно числу различных корней $f_\alpha(x, K)$, каждое из которых продолжается до вложения $L \to \overline{K}$. Однако, поскольку $a_i = \alpha_i^{p^{n_i}} \in K$, то $f_{\alpha_i}(x, K)$ делит $x^{p^{n_i}} - a_i \in K[x]$, поэтому $f_{\alpha_i}(x, K)$ имеет только один (кратный) корень. Отсюда следует, что любое вложение поля L над K тождественно на каждом α_i и поэтому тождественно на L. Это означает, что в $L \backslash K$ нет сепарабельных элементов.

29.29. Пусть σ — вложение E_0 в $\overline{E}$ над K, σ продолжается до автоморфизма поля E. Поле σE_0 сепарабельно над K, следовательно, оно содержится в E_0, поскольку E_0 — максимальное сепарабельное подполе. Значит, $\sigma E_0 = E_0$.

29.31. Пусть E_0 — максимальное сепарабельное подполе в E. Допустим, что $E^p K = E$. Положим $E = K(\alpha_1, \ldots, \alpha_n)$. Так как E чисто несепарабельно над E_0, то существует такое m, что $\alpha_i^{p^m} \in E_0$ для всех $i = 1, \ldots, n$. Следовательно, $E^{p^m} \subset E_0$. Но $E^{p^m} K = E$, так что $E = E_0$ сепарабельно над K. Обратно, пусть E сепарабельно над K. Но E чисто несепарабельно над $E^p K$. Так как E в то же время сепарабельно над $E^p K$, то $E = E^p K$. Отсюда $E = E^{p^n} K$ для всех $n \geqslant 1$.

29.32. Пусть $\alpha \in F^G$ и σ — произвольное вложение поля $K(\alpha)$ над K в $\overline{F}$. Продолжим σ до вложения поля F. Тогда σ — автоморфизм поля F. Так как $\sigma\alpha = \alpha$, то действие σ тождественно на $K(\alpha)$ и, следовательно, α чисто несепарабелен над K. Пересечение $F_0 \cap F^G$ одновременно и сепарабельно, и чисто несепарабельно над K, поэтому равно K.

Покажем, что F сепарабельно над F^G. Предположим, что F конечно над K, тогда группа G также конечна. Пусть $\alpha \in F$ и $\sigma_1, \ldots, \sigma_r$ — максимальное подмножество элементов из G таких, что $\sigma_1\alpha, \ldots, \sigma_r\alpha$ различны. Тогда некоторое σ_i тождественно на α и α есть корень многочлена $f(x) = \prod_{i=1}^{r} (x - \sigma_i\alpha)$, причем $f^\tau = f$ для любого $\tau \in G$, поскольку τ переставляет корни.

Итак, f сепарабелен и его коэффициенты лежат в неподвижном поле F^G. Поэтому α сепарабелен над F^G. Бесконечный случай сводится к конечному, поскольку всякий элемент $\alpha \in F$ содержится в некотором конечном нормальном подрасширении в F.

Поле F чисто несепарабельно над F_0 и, следовательно, чисто несепарабельно над $F_0 F^G$. С другой стороны, F сепарабельно над F^G и, следовательно, сепарабельно над $F_0 F^G$. Таким образом, $F = F_0 F^G$.

30. Конечные поля

30.2. б) Пусть $F_q \subset K$ — расширение степени m. Группа K^* — циклическая, $K^* = \langle\theta\rangle$, $K = F_q(\theta)$. Если $h(x)$ — минимальный многочлен примитивного элемента θ, то $\deg h(x) = [F_q(\theta) : F_q] = [K : F_q] = m$ и $h(x)$ неприводим над F_q по определению.

30.3. Многочлен $f(x) = x^q - x$ ввиду того, что его производная $qx^{q-1} - 1 = -1 \neq 0$, имеет ровно q различных корней. Равенства $x^q = x$, $(x - y)^q = x^q - y^q$ и $(x/y)^q = x^q/y^q$ (при $y \neq 0$) показывают, что корни многочлена $f(x)$ образуют над F_p поле из q элементов. Оно является полем разложения над F_p многочлена $f(x)$. Отсюда следует единственность (с точностью до изоморфизма) поля F_q.

30.4. Это вытекает из того, что $x^{q-1}-1=\prod\limits_{i=1}^{q-1}(x-a_i)$, где a_i — все ненулевые элементы поля F_q.

30.6. Если β — корень многочлена $x^p-x-\alpha$, то его корнями будут и $\beta+1,\ldots,\beta+(p-1)$. Откуда и следует утверждение об этом многочлене. Для доказательства последнего заметьте, что из $\beta^p=\beta+\alpha$ следует $\beta^{p^2}=\beta^p+\alpha^p=\beta+\alpha+\alpha^p$ и т. д. Таким образом, $\beta^{p^n}=\beta+\operatorname{tr}(\alpha)$, а потому $\beta\in F_q$ тогда и только тогда, когда $\operatorname{tr}(\alpha)=0$.

30.8. Неприводимые: x, $x+1$; x^2+x+1; x^3+x+1, x^3+x^2+1.

30.9. Проверьте, что каждый из перечисленных многочленов не равен $\left(x^2+x+1\right)^2$.

$x^{16}-x=x^{16}+x=x\left(x+1\right)\left(x^2+x+1\right)\left(x^4+x^3+1\right)\left(x^4+x+1\right)\left(x^4+x^3+x^2+x+1\right)$.

30.12. $\psi_4(2)=\dfrac{1}{4}\left(2^4-2^2\right)=3$, $\psi_5(2)=\dfrac{1}{5}\left(2^5-2\right)=6$, $\psi_6(2)=\dfrac{1}{6}\left(2^6-2^3-2^2+2\right)=9$.

30.14. а) Проверьте, что $x^3+1=(x+1)\left(x^2+x+1\right)$, $x^7+1=(x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right)$. б) $x^3-1=(x-1)(x+5)(x+3)$.

30.18. Если $m=o(f)$, $k=o(g)$, то $m\,|\,k$. С другой стороны, $g\,|\,(x^m-1)^n$ и $p^t\geqslant n$. Поэтому $g\,|\,(x^m-1)^{p^t}$. А так как $(x^m-1)^{p^t}=x^{mp^t}-1$, то $k\,|\,mp^t$. Откуда и вытекают данные утверждения.

30.19. 1) Пусть $\alpha=o(f)$, $\beta=o(\theta)$. Так как $f\,|\,x^\alpha-1$, то $\theta^\alpha=1$, откуда $\beta\leqslant\alpha$. С другой стороны, $\theta^\beta=1$. Тогда f и $x^\beta-1$ имеют общий корень. Поэтому $f\,|\,x^\beta-1$, значит, $\alpha\leqslant\beta$.

2) Пусть θ — корень многочлена f в его поле разложения F. Тогда θ — элемент группы F^* порядка p^n-1. Теперь утверждение вытекает из предыдущего и из того, что $o(\theta)\,|\,p^n-1$.

30.21. а) $a^{q-1}=1$, поэтому $\left(a^{(q-1)/2}+1\right)\left(a^{(q-1)/2}-1\right)=0$. Отсюда $a^{(q-1)/2}=\pm1$ в F.

б) Пусть $x^2=a$, $F^*=\langle g\rangle$ и $a=g^b$, $x=g^y$. Равенство $x^2=a$ равносильно равенству $g^{2y}=g^b$, что эквивалентно сравнению $2y\equiv b\pmod{q-1}$. Последнее сравнение разрешимо в точности тогда, когда $2\,|\,b$.

Если $2\,|\,b$, то $a^{(q-1)/2}=g^{b(q-1)/2}=1$. Обратно, если $a^{(q-1)/2}=1$, то $g^{b(q-1)/2}=1$, значит, $q-1$ делит $b(q-1)/2$, или $2\,|\,b$.

г) В циклической группе F^* порядка $q-1$ ровно $(q-1)/2$ элементов удовлетворяют уравнению $x^{(q-1)/2}=1$.

е) Проверьте, что $(ab/F)=(a/F)(b/F)$: $(ab/F)=(ab)^{(q-1)/2}=a^{(q-1)/2}b^{(q-1)/2}=(a/F)(b/F)$.

30.22. Пусть $p_1,\ldots,p_m$ — простые числа вида $4k+1$ и $b=(2p_1\ldots p_m)^2+1$. Предположим, что простое число $p\,|\,b$. Тогда -1 будет квадратичным вычетом в F_p. Поэтому p имеет вид $4k+1$. Но p не находится среди чисел p_i.

30.24. Пусть $\pm m_l$ — наименьший вычет для la, где $m_l>0$. Когда l пробегает значения между 1 и $(p-1)/2$, μ будет числом получившихся при этом знаков минус. Заметим, что $m_l\neq m_k$ для $l\neq k$ и $1\leqslant l,k\leqslant(p-1)/2$. Действительно, если $m_l=m_k$, то $la\equiv\pm ka\pmod p$, из $p\nmid a$ следует $l\pm k\equiv0\pmod p$. Это невозможно, так как $|l\pm k|\leqslant l+k\leqslant p-1$. Таким образом, множества $\{1,\ldots,(p-1)/2\}$ и $\{m_1,\ldots,m_{(p-1)/2}\}$ совпадают. Перемножая сравнения $1\cdot a\equiv\pm m_1\pmod p$, $\ldots$, $((p-1)/2)\,a\equiv\pm m_{(p-1)/2}\pmod p$, получаем $((p-1)/2)!\,a^{(p-1)/2}\equiv(-1)^\mu((p-1)/2)!\pmod p$. Значит, $(a/p)\equiv a^{(p-1)/2}\equiv(-1)^\mu\pmod p$. Откуда $(a/p)=(-1)^\mu$.

30.25. Число μ из леммы Гаусса равно числу элементов множества $2\cdot1,\ldots,2\cdot(p-1)/2$, которые превосходят $(p-1)/2$. Пусть m определяется условиями: $2m\leqslant(p-1)/2$ и $2(m+1)>(p-1)/2$. Тогда $\mu=(p-1)/2-m$.

Если $p=8k+1$, то $(p-1)/2=4k$, $m=2k$, $\mu=2k$ и $(2/p)=1$. Если $p=8k+7$, то $(p-1)/2=4k+3$, $m=2k+1$, $\mu=2k+2$ и $(2/p)=1$. Легко проверяется, что в оставшихся случаях μ будет нечетным.

30.26. Предварительно заметим, что если $r_1,\ldots,r_m$ — нечетные целые числа, то $\sum_{i=1}^m(r_i-1)/2\equiv(r_1\ldots r_m-1)/2\pmod2$ и $\sum_{i=1}^m\left(r_i^2-1\right)/8\equiv\left(r_1^2\ldots r_m^2-1\right)/8\pmod2$. Действительно, $(r_1-1)(r_2-1)\equiv0\pmod4$. Тогда $r_1r_2-1\equiv(r_1-1)+(r_2-1)\pmod4$. Откуда $(r_1r_2-1)/2\equiv(r_1-1)/2+(r_2-1)/2\pmod2$. Первое сравнение теперь доказывается индукцией по m. Далее, $\left(r_1^2-1\right)\left(r_2^2-1\right)\equiv0\pmod{16}$, это влечет $r_1^2r_2^2-1\equiv\left(r_1^2-1\right)+\left(r_2^2-1\right)\pmod{16}$. Откуда $\left(r_1^2r_2^2-1\right)/8\equiv\left(r_1^2-1\right)/8+\left(r_2^2-1\right)/8\pmod2$. Опять можно применить индукцию по m.

Пусть $b=p_1\ldots p_m$, где p_i — простые числа (не обязательно различные). Тогда

$(-1/b)=(-1/p_1)\ldots(-1/p_m)=(-1)^{(p_1-1)/2}\ldots(-1)^{(p_m-1)/2}=(-1)^{\sum(p_i-1)/2}$.

Так как $\sum(p_i-1)/2\equiv(p_1\ldots p_m-1)/2\equiv(b-1)/2\pmod2$, то это доказывает а). б) доказывается аналогично.

30.27. Если $a=q_1\ldots q_l$, $b=p_1\ldots p_m$, то $(a/b)(b/a)=\prod\limits_{i=1}^{l}\prod\limits_{j=1}^{m}(q_i/p_j)(p_j/q_i)=(-1)^{\sum\limits_{i=1}^{l}\sum\limits_{j=1}^{m}((q_i-1)/2)((p_j-1)/2)}$. Далее, $\sum\limits_{i=1}^{l}\sum\limits_{j=1}^{m}((q_i-1)/2)((p_j-1)/2)\equiv((a-1)/2)\sum\limits_{i=1}^{l}(p_i-1)/2\equiv((a-1)/2)((b-1)/2)\pmod2$, что завершает доказательство.

30.32. Пусть b — образующий группы F^*. Положим $\alpha=b^a$ и $x=b^y$. Равенство $x^n=\alpha$ эквивалентно сравнению $ny\equiv a\pmod{q-1}$, которое разрешимо в точности тогда, когда $\delta\,|\,a$, причем, если $\delta\,|\,a$, то имеется ровно δ решений. Так как порядок b в F^* равен $q-1$, то $\delta\,|\,a$ в точности тогда, когда $\alpha^{(q-1)/\delta}=b^{(q-1)a/\delta}=1$.

30.35. $q^n-1=(q-1)\left(q^{n-1}+\ldots+q+1\right)$. Так как $q\equiv1\pmod n$, то $q^{n-1}+\ldots+q+1\equiv n\equiv0\pmod n$. Таким образом, $n(q-1)\,|\,q^n-1$. Воспользуйтесь тем, что $a^{q-1}=1$.

31. Начала теории Галуа

31.4. а) Группа $\operatorname{Gal}\mathbb{C}/\mathbb{R}$ состоит из тождественного автоморфизма и комплексного сопряжения, $\operatorname{Gal}\mathbb{C}/\mathbb{R}\cong\mathbb{Z}_2$; б), в) $\mathbb{Z}_2$; г) $\mathbb{Z}_2\oplus\mathbb{Z}_2$.

31.5. Всякий элемент $a\in L$ является корнем сепарабельного многочлена над K степени $\leqslant|G|$, а именно $f(x)=\prod\limits_{\sigma\in G}(x-\sigma(a))$.

Используя существование примитивного элемента у всякого конечного сепарабельного расширения, докажите, что $(L:K)=|G|$.

31.6. $\Phi_1(x)=x-1$, $\Phi_2(x)=x+1$, $\Phi_3(x)=x^2+x+1$, $\Phi_4(x)=x^2+1$, $\Phi_6(x)=x^2-x+1$, $\Phi_8(x)=x^4+1$, $\Phi_9(x)=x^6+x^3+1$, $\Phi_{10}(x)=x^4-x^3+x^2-x+1$, $\Phi_{12}(x)=x^4-x^2+1$; $\Phi_p(x)=x^{p-1}+x^{p-2}+\ldots+1$ при простом p.

31.8. Пусть $H=\operatorname{Gal}KF/F$. Тогда $H\cong\operatorname{Gal}(K/(K\cap F))$, $|H|=[KF:F]$ и $L\subseteq K\cap F\subseteq K$. Из соответствия Галуа следует, что $|H|$ делит порядок группы $G=\operatorname{Gal}K/L$.

31.10. а) Всякий элемент из $H\cap N$ оставляет FL неподвижным, и всякий элемент из G, оставляющий FL неподвижным, оставляет неподвижными также F и L и, следовательно, лежит в $H\cap N$.

б) Рассуждения, аналогичные а).

31.14. а) Любое разложение на множители должно содержать множитель степени 1.

в) Если $f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ — разложение на множители в поле L, и $G=\operatorname{Gal}L/K$, то элементы из G переставляют корни $f(x)$. Таким образом, получается инъективный гомоморфизм $G\to S_3$.

д) Пусть $\delta=(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)$, где α_i — различные корни $f(x)$. Если $\sigma\in G$, то $\sigma(\delta)=\pm\delta$. Множество тех σ в G, которые оставляют δ неподвижным, совпадает с множеством четных перестановок. Таким образом, $G\cong S_3$ в точности тогда, когда $\Delta=\delta^2$ не является квадратом в K.

31.15. а) Если θ — корень уравнения, то $\zeta\theta,\ldots,\zeta^{n-1}\theta$ (где ζ — примитивный корень n-й степени из 1) — остальные корни этого уравнения. Поэтому θ порождает поле корней и любая перестановка из группы Галуа имеет вид $\theta\mapsto\zeta^\nu\theta$. Следовательно, каждой перестановке соответствует вполне определенный корень из единицы ζ^ν. Это соответствие является инъективным гомоморфизмом. Поэтому группа Галуа изоморфна подгруппе циклической группы корней n-й степени из 1. Если уравнение $x^n-a=0$ неразложимо (a не является степенью с показателем $d>1$ ни для какого делителя d числа n), то группа Галуа изоморфна полной группе корней n-й степени из 1, т.е. $\mathbb{Z}_n$.

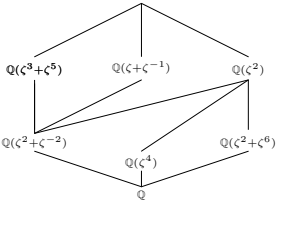
б) Пусть $\zeta\in K$ — примитивный корень n-й степени из 1, σ — порождающая перестановка из группы Галуа. Все автоморфизмы $1,\sigma,\ldots,\sigma^{n-1}$ различны, поэтому линейно независимы, следовательно, найдется $\alpha\in P$ такой, что $\beta=(\zeta,\alpha)=\alpha+\zeta\sigma\alpha+\ldots+\zeta^{n-1}\sigma^{n-1}\alpha\neq0$. Так как $\sigma(\zeta,\alpha)=\zeta^{-1}(\zeta,\alpha)$, то $\beta^n=(\zeta,\alpha)^n$ остается неизменным под действием σ, т.е. $a=\beta^n\in K$. Далее, $\sigma^\nu(\zeta,\alpha)=\zeta^{-\nu}(\zeta,\alpha)$. Откуда $[K(\beta):K]=n$, т.е. $K(\beta)=P$.

31.16. а) Учесть, что группа Галуа является подгруппой группы порядка p.

б) В своем поле разложения x^p-a разлагается следующим образом: $x^p-a=\prod\limits_{i=0}^{p-1}(x-\zeta^i\theta)$, где $\theta^p=a$, ζ — примитивный корень p-й степени из 1. Поэтому если $x^p-a=\varphi(x)\psi(x)$, то $\varphi(x)$ должен быть произведением множителей $x-\zeta^i\theta$, а свободный член $\pm b$ многочлена $\varphi(x)$ должен иметь вид $\pm\zeta'\theta^m$, где ζ' — корень p-й степени из единицы: $b=\zeta'\theta^m$, $b^p=\theta^{pm}=a^m$. Так как $0<m<p$, то $(m,p)=1$ и, значит, $km+sp=1$, $a=a^{km}a^{sp}=b^{kp}a^{sp}$, т.е. a является p-й степенью.

31.17. а), б) A_3; в), г) S_3; д) $\mathbb{Z}_4$; е) $\mathbb{Z}_2$: учесть, что $x^4+x^2+1=(x^2+x+1)(x^2-x+1)$; ж) A_3.

31.22. Пусть $\zeta=\sqrt[8]{-1}$ — один из корней уравнения $x^8+1=0$. Тогда все корни имеют вид ζ, ζ^3, ζ^5, ζ^7, ζ^9, ζ^{11}, ζ^{13}, ζ^{15} и автоморфизмы поля разложения $K=\mathbb{Q}(\zeta)$ однозначно определяются отображениями $\zeta\mapsto\zeta^k$ ($k=1,3,\ldots,15$), т.е. $G=\operatorname{Gal}(K/\mathbb{Q})\cong U(\mathbb{Z}_{16})$. Группа G имеет 6 нетривиальных подгрупп, которым соответствуют подполя поля K, образующие решетку:



Литература

[1] Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987.

[2] Артамонов В.А. Введение в высшую алгебру и аналитическую геометрию. М.: Факториал Пресс, 2007.

[3] Артамонов В.А., Латышев В.Н. Линейная алгебра и выпуклая геометрия. М.: Факториал Пресс, 2004.

[4] Атья М., Макдональд И. Введение в коммутативную алгебру. М.: Мир, 1972.

[5] Белоногов В.А. Задачник по теории групп. М.: Наука, 2000.

[6] Белоногов В.А., Фомин А.Н. Матричные представления в теории конечных групп. М.: Наука, 1976.

[7] Биркгоф Г. Теория решеток. М.: Наука, 1984.

[8] Богопольский О.В. Введение в теорию групп. Москва-Ижевск: Инст. компьют. иссл., 2002.

[9] Ван-дер-Варден Б.Л. Алгебра. М.: Наука, 1976.

[10] Винберг Э.Б. Курс алгебры. М.: Факториал Пресс, 2002.

[11] Гаген Т.М. Некоторые вопросы теории конечных групп. В сб.: К теории конечных групп. Математика. Новое в зарубежной науке. М.: Мир, 1979.

[12] Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Т. 1, 2. М.: Гелиос АРВ, 2003.

[13] Горенстейн Д. Конечные простые группы. Введение в их классификацию. М.: Мир, 1985.

[14] Гретцер Г. Общая теория решеток. М.: Мир, 1982.

[15] Калужнин Л.А. Введение в общую алгебру. М.: Наука, 1973.

[16] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.: Наука, 1977.

[17] Каш Ф. Модули и кольца. М.: Мир, 1981.

[18] Клиффорд А., Престон Г. Алгебраическая теория полугрупп. Т. 1. М.: Мир, 1972.

[19] Кокорин А.И., Копытов В.М. Линейно упорядоченные группы. М.: Наука, 1972.

[20] Кон П. Свободные кольца и их связи. М.: Мир, 1975.

[21] Кострикин А.И. Вокруг Бернсайда. М.: Наука, 1986.

[22] Кострикин А.И. Введение в алгебру. Ч.1–3. М.: Физматлит, 2000.

[23] Крылов П.А., Михалев А.В., Туганбаев А.А. Абелевы группы и их кольца эндоморфизмов. М: Факториал Пресс, 2006.

[24] Крылов П.А., Туганбаев А.А. Модули над областями дискретного нормирования. М.: Факториал Пресс, 2007.

[25] Крылов П.А., Туганбаев А.А., Чехлов А.Р. Задачи по теории колец, модулей и полей. М.: Факториал Пресс, 2007.

[26] Куликов Л.Я., Москаленко А.И., Фомин А.А. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.

[27] Курош А.Г. Лекции по общей алгебре. М.: Наука, 1973.

[28] Курош А.Г. Теория групп. М.: Наука, 1967.

[29] Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. М.: Наука, 1969.

[30] Ламбек И. Кольца и модули. М.: Мир, 1971.

[31] Ленг С. Алгебра. М.: Мир, 1968.

[32] Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988.

[33] Ляпин Е.С., Айзенштат А.Я., Лесохин М.М. Упражнения по теории групп. М.: Наука, 1967.

[34] Ляпин Е.С. Полугруппы. М.: Физматгиз, 1960.

[35] Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука, 1974.

[36] Михалев А.А., Михалев А.В. Начала алгебры. Ч. 1. М.: ИНТУИТ.РУ, 2005.

[37] Мишина А.П., Скорняков Л.А. Абелевы группы и модули. М.: Наука, 1969.

[38] Нечаев В.И. Элементы криптографии. М.: Высш. шк., 1999.

[39] Пирс Р. Ассоциативные алгебры. М.: Мир, 1986.

[40] Попов А.М., Созутов А.И., Шунков В.П. Группы с системами фробениусовых подгрупп. Красноярск: ИПЦ КГТУ, 2004.

[41] Постников М.М. Теория Галуа. М.: Физматгиз, 1963.

[42] Проскуряков И.В. Сборник задач по линейной алгебре. М.: Наука, 1970.

[43] Пунинский Г.Е., Туганбаев А.А. Кольца и модули. М.: Союз, 1998.

[44] Сборник задач по алгебре. Под ред. Кострикина А.И. М.: Физматлит, 2001.

[45] Скорняков Л.А. Элементы теории структур. М.: Наука, 1970.

[46] Скорняков Л.А. Элементы общей алгебры. М.: Наука, 1983.

[47] Судзуки М. Строение группы и строение структуры ее подгрупп. М.: ИЛ, 1960.

[48] Супруненко Д.А. Группы матриц. М.: Наука, 1972.

[49] Фаддеев Д.К. Лекции по алгебре. М.: Наука, 1984.
[50] Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. М.: Наука, 1977.
[51] Фейс К. Алгебра: кольца, модули и категории. Т. 1, 2. М.: Мир, 1977, 1979.
[52] Фукс Л. Бесконечные абелевы группы. Т. 1, 2. М.: Мир, 1974, 1977.
[53] Холл М. Теория групп. М.: ИЛ, 1963.
[54] Черников С.Н. Группы с заданными свойствами системы подгрупп. М.: Наука, 1980.
[55] Чехлов А.Р. Упражнения по основам теории групп. Томск: Томский госуниверситет, 2004.
[56] Шафаревич И.Р. Основные понятия алгебры. Ижевск: Ижевская республ. типография, 1999.
[57] Шеврин Л.Н., Овсянников А.Я. Полугруппы и их полугрупповые решетки. Свердловск, 1990. Ч. 1; 1991. Ч. 2.
[58] Шеметков Л.А. Формации конечных групп. М.: Наука, 1978.
[59] Arnold D. Finite rank torsion-free Abelian groups and rings. Lecture Notes Math., 1982, 931, p. 1-191.
[60] Gorenstein D. Finite groups. Harper and Row, New York, 1968.
[61] Huppert B. Endliche Gruppen. I. Springer, Berlin, 1967.
[62] Kaplansky I. Infinite Abelian groups. The University of Michigan Press, Ann Arbor, Mich., 1969.
[63] Mader A. Almost completely decomposable groups. Gordon and Breach, Amsterdam, 2000.
[64] Valkan D., Pelea C., Modoi C., Breaz S., Calugareanu G. Exercises in Abelian Group Theory. Springer, 2003.

Предметный указатель

Учебное издание

Петр Андреевич **Крылов**, Аскар Аканович **Туганбаев**,
Андрей Ростиславович **Чехлов**

Задачи и упражнения по основам общей алгебры

Учебное пособие

Подписано в печать 01.10.2012.

Электронное издание для распространения через Интернет.

ООО «ФЛИНТА», 117342, Москва, ул. Бутлерова, д. 17-Б, комн. 324
Тел./факс: 334-82-65; тел. 336-03-11.
E-mail: flinta@mail.ru;
WebSite: www.flinta.ru