Предисловие

Настоящее пособие составлено на основе спецкурсов, читавшихся автором на механико-математическом факультете в течение более 10 лет. Выбор материала в значительной мере определялся пристрастиями автора. Наряду с классическими результатами компьютерной алгебры в этих спецкурсах (и в настоящем пособии) нашли отражение исследования нашего коллектива. Прежде всего, это относится к теории дифференциальной размерности. Теорией дифференциальной размерности мы начали заниматься по инициативе, под руководством и при активном участии А.В. Михалева в конце 70-х — начале 80-х годов прошлого века [**13**]. Наряду с теоретическими исследованиями, нами был разработан комплекс программ на алгоритмическом языке REFAL для вычислений в дифференциальных и разностных модулях [**11**]. Результаты многолетних исследований, связанных с конструктивными методами в кольцах дифференциальных и разностных многочленов и теорией дифференциально-разностной размерности, опубликованы в монографии [**20**]. Частично эти результаты отражены в настоящем курсе. Пользуюсь случаем выразить глубокую признательность Александру Васильевичу Михалеву, в значительной мере благодаря которому появился этот курс. Я также очень благодарен Марине Владимировне Кондратьевой, Александру Борисовичу Левину, Андрею Витальевичу Астрелину, Олегу Дмитриевичу Голубицкому, Алексею Игоревичу Зобнину и другим коллегам, работавшим вместе с нами в области компьютерной алгебры. Исследования выполнялись в лаборатории вычислительных методов и на кафедре высшей алгебры механико-математического факультета МГУ, и я признателен коллективу лаборатории и кафедры за очень доброжелательное отношение к нашей группе.

Преподавание компьютерной алгебры я начинал с двух полугодовых спецкурсов, по материалам которых были опубликованы учебные пособия [**15**] и [**14**]. В дальнейшем конспекты курса компьютерной алгебры были выложены на сайт и активно использовались

студентами и аспирантами при подготовке к экзамену по компьютерной алгебре. Размещение конспектов на сайте позволило оперативно исправлять опечатки, замеченные студентами в процессе подготовки к экзамену, и вносить изменения в изложение материала. Всем внимательным читателям данного курса я выражаю глубокую благодарность.

Компьютерная алгебра активно развивается, пополняется новыми результатами. Данное пособие охватывает только малую ее часть. Надеюсь, что в ближайшем будущем появятся новые, более полные учебники по компьютерной алгебре, в создании которых мне хотелось бы принять посильное участие.

Об авторе

Панкратьев Евгений Васильевич — кандидат физико-математических наук, ведущий научный сотрудник лаборатории вычислительных методов механико-математического факультета МГУ. Читает специальные курсы по компьютерной алгебре, дифференциальной алгебре и сложности алгебраических алгоритмов, руководитель и тренер студенческих команд МГУ по программированию, неоднократно становившихся чемпионами России и призерами чемпионатов мира.

Оглавление

Введение

Что такое компьютерная алгебра. Компьютерная алгебра — область математики, лежащая на стыке алгебры и вычислительных методов. Для нее, как и для любой области, лежащей на стыке различных наук, трудно определить четкие границы. Часто говорят, что к компьютерной алгебре относятся вопросы слишком алгебраические, чтобы содержаться в учебниках по вычислительной математике, и слишком вычислительные, чтобы содержаться в учебниках по алгебре. При этом ответ на вопрос о том, относится ли конкретная задача к компьютерной алгебре, часто зависит от склонностей специалиста.

Термин "компьютерная алгебра" возник как синоним терминов "символьные вычисления", "аналитические вычисления", "аналитические преобразования" и т. д. Даже в настоящее время этот термин на французском языке дословно означает "формальные вычисления".

В чем основные отличия символьных вычислений от численных и почему возник термин "компьютерная алгебра"?

Когда мы говорим о вычислительных методах, то считаем, что все вычисления выполняются в поле вещественных или комплексных чисел. В действительности же всякая программа для ЭВМ имеет дело только с конечным набором рациональных чисел, поскольку только такие числа представляются в компьютере. Для записи целого числа отводится обычно 16 или 32 двоичных символа (бита), для вещественного — 32 или 64 бита. Это множество не замкнуто относительно арифметических операций, что может выражаться в различных переполнениях, например, при умножении достаточно больших чисел или при делении на маленькое число. Еще более существенной особенностью вычислительной математики является то, что арифметические операции над этими числами, выполняемые компьютером, отличаются от арифметических операций в поле рациональных чисел, — более того, для компьютерных операций не выполняются основные аксиомы поля (ассоциативности, дистрибутивности). Эти особенности компьютерных вычислений оцениваются в

терминах погрешности или точности вычислений. Оценка погрешности представляет одну из основных проблем вычислительной математики. Каждую задачу требуется решить с использованием имеющихся ресурсов ЭВМ, за обозримое время, с заданной точностью.

Набор объектов, применяемых в символьных вычислениях, весьма разнообразен, в частности, в них используется значительно большее множество рациональных чисел. Это множество все равно остается конечным, но ограничения на допустимые размеры числа (количество знаков в его записи) связаны обычно с размерами оперативной памяти ЭВМ, что позволяет пользоваться практически любыми рациональными числами, операции над которыми выполняются за приемлемое время. При этом компьютерные операции над рациональными числами совпадают с соответствующими операциями в поле рациональных чисел. Таким образом, снимается одна из основных проблем вычислительных методов — оценка погрешности вычислений.

В компьютерной алгебре вещественные и комплексные числа практически не применяются, зато широко используется алгебраические числа. Алгебраическое число задается своим минимальным многочленом, а иногда для его задания требуется указать интервал на прямой или область в комплексной плоскости, где содержится единственный корень данного многочлена. Многочлены играют в символьных вычислениях исключительно важную роль. На использовании полиномиальной арифметики основаны теоретические методы аналитической механики, они применяются во многих областях математики, физики и других наук. Кроме того, в компьютерной алгебре рассматриваются такие объекты, как дифференциальные поля (функциональные поля), допускающие показательные, логарифмические, тригонометрические функции, матричные кольца (элементы матрицы принадлежат кольцам достаточно общего вида) и другие. Даже при арифметических операциях над такими объектами происходит разбухание информации, и для записи промежуточных результатов вычислений требуется значительный объем памяти ЭВМ.

Ограничения на алгоритмы решаемых компьютерной алгеброй задач накладываются имеющимися ресурсами ЭВМ и обозримостью времени счета. Однако ограничения по времени счета и по используемой памяти в символьных вычислениях существенно более обременительны, чем в вычислительных методах.

В научных исследованиях и технических расчетах специалистам приходится гораздо больше заниматься преобразованиями формул, чем собственно численным счетом. Тем не менее, с появлением

ЭВМ основное внимание уделялось автоматизации численных вычислений, хотя ЭВМ начали применяться для решения таких задач символьных преобразований, как, например, символьное дифференцирование, ещё в 50-х годах прошлого века. Активная разработка систем компьютерной алгебры началась в конце 60-х годов. С тех пор создано значительное количество различных систем, получивших различную степень распространения; некоторые системы продолжают развиваться, другие отмирают, и постоянно появляются новые.

Системы компьютерной алгебры. Системы компьютерной алгебры можно условно разделить на системы общего назначения и специализированные. К системам общего назначения относятся MACSYMA, REDUCE, MATEMATICA, MAPLE, AXIOM и другие системы. В 80-е годы прошлого века широкое распространение в СССР получила система REDUCE. Она первоначально предназначалась для решения физических задач, разрабатывалась на наиболее широко распространенных компьютерах, разработка до определенного времени не носила коммерческого характера (система до конца 80-х годов распространялась бесплатно), открытый характер системы позволил привлечь к ее разработке огромную армию пользователей, обогативших систему многочисленными пакетами для решения отдельных задач. MACSYMA, так же, как и REDUCE, является "старой" системой. В отличие от системы REDUCE, MACSYMA разрабатывалась с самого начала как коммерческий продукт. В ней более тщательно проработаны алгоритмические вопросы, ее эффективность существенно выше, но меньшее ее распространение можно объяснить двумя обстоятельствами: длительное время она была реализована только на малом числе "экзотических" компьютеров и распространялась только на коммерческой основе. Система MAPLE, созданная в 80-х годах прошлого века в Канаде, с самого начала была задумана как система для персональных компьютеров, учитывающая их особенности. Она развивается "вширь и вглубь", даже ее ядро переписывалось с одного алгоритмического языка на другой. В настоящее время MAPLE широко применяется во многих странах (в частности, в США и Канаде) в учебном процессе, а также в различных областях научных и технических исследований. В конце прошлого века получила широкое распространение и сейчас быстро развивается система MATEMATICA. Ее успех в значительной степени объясняется ее широкими графическими возможностями, а также электронной документацией, которую можно рассматривать как

электронную библиотеку, посвященную различным разделам математики и информатики. Особое место среди систем компьютерной алгебры занимает система AXIOM. В отличие от остальных систем, представляющих собой пакеты программ, общение с которыми осуществляется на некотором алголоподобном языке, система AXIOM, развившаяся из системы SCRATCHPAD-II, имеет дело с более привычными для математиков объектами. В частности, в ней ключевым понятием является понятие категории: здесь можно рассматривать, например, категории множеств, полугрупп, дифференциальных колец, левых модулей и т. д. Система имеет высокую степень универсальности, требует для своей реализации мощных компьютеров, распространяется за достаточно высокую плату, поэтому используется только в ограниченном числе мощных университетских и научных центров.

Специализированные системы отличаются более высокой эффективностью, но область их применения ограничена. К специализированным системам относятся такие системы, как CALEY и GAP — специализированные системы для вычислений в теории групп, MACAULEY, CoCoA, Singular — системы разной степени универсальности для вычислений в кольце многочленов, SCHOONSHIP — специализированная система для вычислений в физике высоких энергий, muMATH и ее правонаследница DERIVE — системы, широко используемые в учебном процессе (в частности, в Австрии лицензия на установку системы DERIVE приобретена для всех средних школ), и многие другие.

Алгоритмы компьютерной алгебры. Компьютерная алгебра имеет дело с алгоритмами, которые существенно отличаются от алгоритмов, используемых в вычислительной математике. Алгоритмы вычислительной математики должны давать возможность решать задачу с требуемой точностью при заданных вычислительных ресурсах, наиболее существенными из которых являются ограничения по используемой памяти и времени счета. В компьютерной алгебре вычисления обычно производятся без округления, анализу сходимости уделяется значительно меньше внимания, но используется значительно более широкий набор математических, в первую очередь алгебраических, объектов сложной структуры, и ограничения по времени счета, а особенно по используемой памяти, становятся гораздо более обременительными.

Применение компьютеров в алгебраических исследованиях поставило перед специалистами ряд новых задач и в то же время заставило заново пересмотреть задачи, считавшиеся решенными полностью и окончательно. В частности, к ним относились задачи, для которых был предложен метод, позволяющий решать их "за конечное число шагов". При этом методы решения конкретных задач обычно отличались большим разнообразием, и универсальные методы для конкретных вычислений практически не использовались. С применением компьютеров для алгебраических вычислений потребовалось реализовать универсальные алгоритмы в виде программ для ЭВМ, и оказалось, что они позволяют решать только очень небольшие задачи. С увеличением размера задачи резко возрастало время счета и необходимая память компьютера. Это сделало актуальным поиск более эффективных алгоритмов решения алгебраических задач.

В конце прошлого века бурно развивались исследования в трех областях компьютерной алгебры — теории базисов Грёбнера, факторизации многочленов и интегрирования в конечном виде. Именно эти вопросам, в первую очередь, посвящено настоящее пособие.

Оно начинается с рассмотрения проблемы представления данных, которую можно сформулировать в следующем виде. *Имеется множество объектов T и на нем отношение эквивалентности $\sim$. Требуется в каждом классе эквивалентных объектов выбрать единственного представителя этого класса*, для основных алгебраических областей: кольца целых чисел, поля рациональных чисел, конечных полей, кольца многочленов и поля рациональных функций, алгебраических и трансцендентных расширений полей. Кроме того, в главе 1 рассматриваются арифметические операции в этих областях.

Отдельная глава (глава 2) посвящена алгоритмам вычисления наибольших общих делителей целых чисел и многочленов. Здесь же приводятся некоторые оценки для коэффициентов делителя многочлена от одной переменной.

Задача представления данных для факторколец кольца многочленов приводит к введению понятия базисов Грёбнера полиномиальных идеалов. Рассматривая образующие полиномиального идеала как систему нелинейных алгебраических уравнений, базис Грёбнера можно трактовать как некоторую каноническую форму этой системы. Для случая многочленов от одной переменной над некоторым полем в качестве такой "канонической формы" можно рассматривать наибольший общий делитель этих многочленов, который может быть

получен, например, с помощью алгоритма Евклида. Для системы линейных уравнений от многих переменных в качестве "канонической формы" можно взять диагональную форму системы (т. е. систему вида $y_i = c_i$, $i = 1, \ldots, n$), которая может быть получена с помощью метода Гаусса. В общем случае алгоритмы построения базиса Грёбнера можно считать обобщением алгоритма Евклида и метода Гаусса.

Теория базисов Грёбнера рассматривается в главе 3. Изложение не ограничивается случаем полиномиальных идеалов: строится более общая теория, применимая также к подмодулям свободных полиномиальных, дифференциальных и разностных модулей. Наряду с классическими базисами Грёбнера рассматривается их специальный случай, называемый инволютивными базисами.

Базисы Грёбнера имеют многочисленные приложения. В частности, они позволяют определить, совместна ли система нелинейных алгебраических уравнений, и, если система совместна, то определить, сколько эта система имеет решений над алгебраически замкнутым полем (если множество решений бесконечно, то определить размерность многообразия решений). Эти вопросы изучаются в рамках теории размерностных многочленов (многочленов Гильберта). Свойства таких многочленов и алгоритмы их вычисления приведены в главе 4.

Глава 5 посвящена задаче разложения многочленов на неприводимые множители. Мы рассматриваем эту задачу в следующей постановке: дан многочлен $f(x) \in \mathbb{Z}[x]$ с целыми коэффициентами от одной переменной, требуется разложить его на неприводимые множители. С точки зрения "чистого" математика эта задача давно решена полностью и окончательно: получен алгоритм, позволяющий находить требуемое разложение "за конечное число шагов". Один из таких алгоритмов получен в 1882 году Кронекером, чьим именем он и называется в настоящее время, хотя за 100 лет до Кронекера этот алгоритм был известен австрийскому астроному Шуберту. Следующий шаг в исследовании алгоритмов факторизации был сделан только в 60-х годах прошлого столетия, когда был найден достаточно эффективный алгоритм для разложения на множители многочленов с коэффициентами из конечного поля. Использование этого алгоритма в сочетании с леммой Гензеля позволило получить алгоритмы факторизации многочленов с целыми коэффициентами, пригодные для практической реализации. С конца 60-х годов прошлого века появляется большое количество работ по факторизации. Предлагаются усовершенствования алгоритмов, направленные на увеличение

их быстродействия, на расширение области их применения, в частности, рассматривается задача факторизации многочленов от одной и многих переменных с коэффициентами из конечных полей, из полей алгебраических чисел и т. д. Крупным вкладом в теорию факторизации многочленов явилась работа [**24**], позволившая получить алгоритм факторизации, сложность которого оценивается полиномом от степени исходного многочлена.

Наконец, глава 6 посвящена одной из проблем дифференциальной компьютерной алгебры.

Дифференциальные кольца и поля, в которых наряду с арифметическими операциями имеется одна или несколько операций дифференцирования, — это активно исследуемые объекты компьютерной алгебры. Важным частным случаем дифференциальных полей являются поля элементарных функций, получающиеся из поля рациональных функций от одной переменной последовательным присоединением алгебраических элементов, экспонент и логарифмов (таким образом формализуется основная масса формул, с которыми мы привыкли иметь дело в курсе анализа). Алгебраические зависимости, которые могут существовать между образующими таких расширений, описывает так называемая структурная теорема. (В общем случае дифференциальные поля имеют очень сложную структуру и проблема представления данных для них алгоритмически неразрешима.)

Операция дифференцирования легко описывается алгебраически, и ее реализация не представляет трудностей. Гораздо сложнее обстоит дело с обратной операцией — интегрированием. Если F — дифференциальное поле и $f \in F$, то не обязательно существует $g \in F$ такой, что $g' = f$. Задача интегрирования в конечном виде в общем случае формулируется следующим образом. Пусть $\mathcal{A}$ и $\mathcal{B}$ — два класса дифференциальных полей. Требуется построить алгоритм, который для любого элемента f любого дифференциального поля F из класса $\mathcal{A}$ либо находит дифференциальное поле G в классе $\mathcal{B}$ и элемент $g \in G$ такой, что $g' = f$, либо доказывает, что такого элемента не существует ни в каком поле класса $\mathcal{B}$. В классической постановке задачи $\mathcal{A} = \mathcal{B}$ — класс полей элементарных функций. Различные методы интегрирования изучаются в курсе математического анализа, но до недавнего времени они не были оформлены в виде алгоритмов, применимых к широкому классу функций, в частности, эти методы часто позволяли проинтегрировать функцию, если элементарный интеграл у нее существует, но далеко не всегда позволяли доказать отсутствие элементарного интеграла.

Алгоритм интегрирования в конечном виде функций из чисто трансцендентного расширения поля рациональных функций, порожденного экспонентами и логарифмами, был сформулирован в 1969 году Ришем [**29**]. Проверка, принадлежит ли подынтегральная функция данному классу, осуществляется с помощью структурной теоремы. Далее теорема Лиувилля позволяет определить вид элементарного интеграла, если такой существует. Вычисление интеграла или доказательство его отсутствия производится методом неопределенных коэффициентов с использованием рекурсии. Алгоритм интегрирования алгебраических функций (элементов алгебраического расширения поля рациональных функций от одной переменной) был сформулирован Дж. Дэвенпортом [**6**] в 1982 г. Этот алгоритм использует глубокие результаты алгебраической геометрии и весьма сложен для реализации. Дальнейшее развитие алгоритмы интегрирования в конечном виде получили в работах различных математиков, из которых следует отметить Б. Трейгера и М. Бронштейна. Основные направления исследований — повышение эффективности алгоритмов, расширение области их применения и исследование более широкого класса дифференциальных полей, чем поля элементарных функций.

Обобщением задачи интегрирования можно считать задачу нахождения в классе $\mathcal{B}$ дифференциальных полей решений линейных дифференциальных уравнений с коэффициентами из дифференциального поля, принадлежащего классу $\mathcal{A}$. Частный случай этой задачи для уравнения первого порядка приходится решать при интегрировании элементарных функций (в этом случае мы ищем решения в том же поле, в котором лежат коэффициенты исходного уравнения). Алгоритм нахождения решения в классе полей элементарных функций для уравнений второго порядка с коэффициентами из поля рациональных функций был предложен Ковасиком в 1978 году и вскоре был реализован в различных системах компьютерной алгебры. Обобщение алгоритма на уравнения произвольного порядка было получено М. Сингером. Сложность алгоритма Сингера очень высока, и трудно рассчитывать на его реализацию в обозримом будущем (есть реализация для дифференциальных уравнений 3-го порядка). Задачу о разрешимости линейного дифференциального уравнения в элементарных функциях можно разделить на два этапа. Вначале исследуется разрешимость уравнения в классе лиувиллевых функций (лиувиллевы функции получаются путем расширения исходного дифференциального поля последовательным присоединением элементов, являющихся либо алгебраическими, либо интегралами, либо экспонентами интегралов). Вопрос о разрешимости уравнения в

лиувиллевых функциях решается дифференциальной теорией Галуа: линейное однородное дифференциальное уравнение разрешимо в лиувиллевых функциях тогда и только тогда, когда разрешима связная компонента его группы Галуа, являющейся линейной алгебраической группой. Далее задача сводится к уже рассмотренной задаче интегрирования. Рассмотрение задач, сформулированных в этом абзаце, выходит за рамки настоящего курса.

Компьютерная алгебра используется также при нахождении решений дифференциальных уравнений в виде степенных рядов, при анализе устойчивости решений, поиске периодических решений и в других задачах теории дифференциальных уравнений. Широко применяется компьютерная алгебра при построении разностных схем для численного решения дифференциальных уравнений.

Вопросы для самопроверки.

(1) Чем отличается компьютерная алгебра от вычислительной математики?
(2) Какие типы чисел применяются в компьютерной алгебре?
(3) Назовите несколько универсальных и специализированных систем компьютерной алгебры. Опишите область применения специализированных систем.
(4) Сформулируйте проблему представления данных.
(5) Для решения каких задач применяется алгоритм Евклида?
(6) Для решения каких задач применяется метод Гаусса?
(7) Какие задачи могут быть решены с использованием базисов Грёбнера?
(8) Для решения каких задач применяется алгоритм Кронекера?
(9) Сформулируйте задачу интегрирования в конечном виде.
(10) Назовите известные вам применения систем компьютерной алгебры.

Определения и обозначения

Следующие обозначения считаются фиксированными на протяжении всей книги:

$\mathbb{Z}$ — кольцо целых чисел;
$\mathbf{Z}_n$ — кольцо вычетов по модулю натурального числа n;
$\mathbb{Z}_+$ — множество неотрицательных целых чисел;
$\mathbb{Q}$ — поле рациональных чисел;
O_p — кольцо целых p-адических чисел;
R_p — поле рациональных p-адических чисел;
F — произвольное поле;
F_q — конечное поле из q элементов;
$\mathbb{R}$ — поле вещественных чисел;
$\mathbb{C}$ — поле комплексных чисел;
$\mathcal{Z}$ — кольцо гауссовых чисел (вида $a + bi$, $a, b \in \mathbb{Z}$, $i^2 = -1$);
$\mathcal{Q}$ — поле рационально-комплексных чисел;
$\mathcal{L}$ — логическая переменная (типа "да/нет").

Запись алгоритмов осуществляем в форме, по возможности близкой к тем, которые используются в курсе информатики для средней школы и на механико-математическом факультете МГУ в курсе программирования [**2**]. Алгоритм снабжаем именем, за которым в скобках следует список параметров с указанием их типа. В записи алгоритмов // означает, что далее в строке следуют комментарии.

При необходимости вводим новые типы данных, в частности, для коммутативного кольца R с единицей введем типы "многочлен" и "разложение" следующим образом:

```
R[x] — многочлен:
        запись(степень: Z+
                коэффициенты: вектор элементов типа R
                              с индексом 0..степень);
        разложение:
        запись(число_множителей: Z+
                множители: вектор элементов типа многочлен
                           с индексом 1..число_множителей).
```

Глава 1

Проблема представления данных

1. Задача представления данных

Проблему представления данных можно сформулировать в общем виде следующим образом. *Имеется множество объектов T и на нем отношение эквивалентности $\sim$. Требуется в каждом классе эквивалентных объектов выбрать единственного представителя этого класса.* В такой постановке могут быть сформулированы очень многие математические задачи, например:

(1) В качестве T возьмем множество натуральных чисел > 1, каждое из которых можно записать в виде арифметического выражения. В качестве канонического выбираем выражение, которое является произведением простых чисел, расположенных в порядке неубывания. Основная теорема арифметики утверждает, что любое натуральное число представляется в таком виде и такое представление единственно. Таким образом, задача разложения натурального числа на простые множители может рассматриваться как задача представления данных.

(2) Предыдущий пример непосредственно обобщается на любое кольцо с однозначным разложением на множители, элементы которого можно упорядочить. В частности, таковым является кольцо $\mathbb{Z}[x]$, и мы получаем задачу факторизации многочленов, рассматриваемую в главе 5.

(3) Основная теорема алгебры утверждает, что любой многочлен от одной переменной z с комплексными коэффициентами может быть представлен в виде $a \cdot (z - \alpha_1)(z - \alpha_2) \cdots \cdot (z - \alpha_n)$. Таким образом, в этом случае задача представления данных — это задача нахождения всех корней данного многочлена, т. е. задача решения алгебраического уравнения.

1.1. Упражнения. Переформулировать в виде задачи представления данных следующие задачи:

(1) решения системы линейных уравнений с коэффициентами из некоторого поля;
(2) нахождения НОД некоторого множества целых чисел;
(3) нахождения НОД некоторого множества многочленов от одной переменной с комплексными коэффициентами.

Естественно, что в рамках данного курса мы не можем обсуждать проблему представления данных в полном объеме.

Основная цель этой главы — сформулировать и дать некоторое решение задачи для систем многочленов с коэффициентами из некоторого поля (т. е. для систем нелинейных алгебраических уравнений).

Разнообразие структур данных, используемых в компьютерной алгебре, выдвигает задачу представления данных в ЭВМ на первый план. При аналитических вычислениях (вручную или с использованием ЭВМ) используются элементы таких множеств, как кольцо целых чисел $\mathbb{Z}$, поле рациональных чисел $\mathbb{Q}$, кольцо вычетов по некоторому модулю $\mathbb{Z}_n$, кольца многочленов, различные элементарные функции. Объекты этих множеств допускают неоднозначную запись в виде алгебраических выражений, т. е. представление в памяти ЭВМ. Из различных вариантов представления нужно, по возможности, выбрать оптимальное относительно некоторых критериев. Какими же критериями руководствуются математики при выборе представления конкретных элементов?

Наиболее существенным является требование о том, чтобы выбор представления был *каноническим*, т. е. в множестве всех эквивалентных выражений нужно выбрать единственное выражение, которое представляло бы этот класс эквивалентности. При этом предполагается, что известен алгоритм проверки эквивалентности двух выражений. В действительности такой алгоритм имеется не всегда. Это является одной из причин, почему иногда на представления налагаются более слабые требования, чем то, что они канонические.

Одним из таких условий является условие *нормальности*.

Как правило, рассматриваемая структура данных снабжена некоторым набором арифметических операций, часть из которых определена не для всех значений аргументов. В частности, недопустимо деление на нуль. Тем самым нуль приобретает некоторое особое положение, и возрастает значение задачи определения равенства эле-

мента нулю. Представление, в котором все эквивалентные нулю выражения представляются одним и тем же образом (0), называется *нормальным*. Любое каноническое представление является нормальным, но обратное верно не всегда. Однако во многих случаях наличие нормального представления позволяет построить каноническое. Если же рассматриваемая структура данных такова, что в ней имеются, кроме нуля, и другие "особые" элементы, то определение нормального представления должно быть усложнено.

Ключевое для канонического представления понятие эквивалентности объектов может быть самым различным. Могут использоваться различные определения эквивалентности объектов даже на одном и том же множестве. Например, на множестве многочленов с коэффициентами из конечного поля можно рассматривать отношение функционального равенства, а можно — отношение эквивалентности между многочленами, рассматриваемыми как элементы кольца многочленов с коэффициентами из заданного поля.

Другим требованием, предъявляемым к выбору представления, является требование *естественности*. Что понимается под этим требованием? Рассмотрим пример неестественного представления, основанного на *методе Брауна*. Предположим, что мы умеем определять, являются ли два выражения эквивалентными, и что наша ЭВМ обладает неограниченной памятью. В процессе появления выражений мы будем сравнивать каждое новое выражение с уже встречавшимися нам, которые хранятся в памяти ЭВМ. Если среди ранее встречавшихся выражений имеется эквивалентное исходному, то исходное выражение переписывается в форме эквивалентного ему выражения, уже хранящегося в памяти ЭВМ, в противном случае его форма объявляется каноническим представителем в данном классе эквивалентности и запоминается. К преимуществам такого метода следует отнести его универсальность — метод работает всегда, когда есть алгоритм проверки эквивалентности двух выражений. Недостатком метода является его неестественность, т. е. представление конкретного элемента зависит от того, в какой последовательности элементов он появляется (и в каком месте). Представление называется естественным, если представление каждого элемента определяется одними и теми же правилами, не зависящими от того, в какой последовательности появляется этот элемент.

Ниже будут рассмотрены некоторые из основных структур данных, используемых в компьютерной алгебре, и для них рассмотрена проблема представления данных. Хорошо известно, что в общем случае эта проблема неразрешима, т.е существуют отношения эк-

вивалентности, для которых нет алгоритма выбора канонического представителя в множестве эквивалентных выражений, и даже проверки эквивалентности двух выражений.

1.1. Кольцо целых чисел. Из курса программирования известно, что целое число может быть представлено в памяти компьютера разными способами, в частности, это представление зависит от того, как оно описано: как величина типа `integer`, или `real`, или `string`. При этом в большинстве языков программирования под целыми числами понимаются числа из весьма ограниченного диапазона: типичный случай — от $-2^{15} = -32768$ до $2^{15} - 1 = 32767$. Системы компьютерной алгебры имеют дело с большими целыми числами, в частности, любая такая система умеет вычислять и выводить в десятичной записи числа вида 1000! (более тысячи знаков).

В данном курсе мы будем рассматривать представление целых чисел в символьном виде и не вдаваться в подробности, какая память отводится для записи одного символа (бит, байт или другая).

Наиболее распространенным является представление целых чисел в позиционных системах счисления. Такая система определяется выбором основания счисления, например, 10. Множество десятичных целых чисел обычно описывается следующим образом:

```
целое число        == <натуральное число>|0|
                      -<натуральное число>
натуральное число  == <значащая цифра> |
                      <значащая цифра> <цифры>
значащая цифра     == 1|2|3|4|5|6|7|8|9
цифры              == <цифра>  |
                      <цифра> <цифры>
цифра              == 0 | <значащая цифра>
```

Выписанное определение целых чисел дает однозначность представления каждого такого числа, и аналогичное определение (только, может быть, с другим основанием) используется в большинстве систем компьютерной алгебры. Пользуясь таким представлением, удобно реализовать арифметические операции над целыми числами. При этом сложение и вычитание являются относительно “дешевыми” операциями, а умножение и деление — “дорогими”. При оценке сложности арифметических операций следует учитывать как стоимость элементарной операции (одноразрядной), так и количество одноразрядных операций для выполнения какого-либо действия над многозначными числами. Сложность умножения и деления обусловлена, в первую очередь, тем, что с ростом длины числа (его записи в

какой-либо системе счисления) количество элементарных операций увеличивается по квадратичному закону, в отличие от линейного для сложения и вычитания. К тому же, то, что мы обычно называем алгоритмом деления многозначных чисел, в действительности основано на переборе (часто весьма значительном) возможной очередной цифры частного, и при этом недостаточно просто воспользоваться правилами деления однозначных чисел. При большом основании системы счисления (часто оно может иметь порядок 2^{30}) этот способ малоэффективен.

Пусть A — натуральное число (записанное в десятичной системе). Чтобы получить его запись $A = \sum_{i=0}^{d_A} b_i k^i$ в k-ичной системе счисления, можно воспользоваться следующим алгоритмом ($[A/k]$ обозначает целую часть числа A/k):

Дано: A — натуральное число в десятичной системе счисления
$k > 1$ — натуральное число
Надо: A — запись числа A в k-ичной системе счисления

Начало
$i := 0$
цикл пока $A > 0$
$b_i := A \pmod k$
$A := [A/k]$
$i := i + 1$
конец цикла
$d_A := i - 1$
Конец

Для восстановления десятичного числа по последовательности $b_{d_A}, b_{d_A-1}, \ldots, b_1, b_0$ его k-ичной записи $\sum_{i=0}^{d_A} b_i k^i$ используется следующий алгоритм:

Дано: $k > 1$ — натуральное число
последовательность цифр, представляющих число A в k-ичной системе
Надо: A — запись числа A в десятичной системе счисления

Начало
$A := 0$
цикл пока не конец последовательности
$b :=$ очередной элемент последовательности
$A := A * k + b$
конец цикла
Конец

1.2. Упражнение. Объясните, почему для перевода числа из десятичной системы в k-ичную используется деление, а для перевода из k-ичной системы в десятичную — умножение.

Перемножая «столбиком» два двузначных числа в десятичной системе счисления, мы выполняем следующие операции:

$$(10a + b)(10c + d) = 100ac + 10(ad + bc) + bd,$$

т. е. 4 операции умножения одноразрядных чисел, 3 операции сложения и 2 операции умножения на степень основания счисления, которые сводятся к сдвигу. При оценке сложности можно учитывать все элементарные операции, не разделяя их по весам (в данном примере мы имеем 9 элементарных операций). Задача оптимизации алгоритма сводится при данном подходе к минимизации общего числа элементарных операций. Можно, однако, считать, что умножение является более «дорогой» операцией, чем сложение, которое, в свою очередь, «дороже» сдвига. Учитывая только наиболее дорогие операции, мы получаем, что *мультипликативная* сложность умножения двузначных чисел «столбиком» равна 4.

В параграфе 5 рассматриваются алгоритмы вычисления наибольших общих делителей и оценивается их сложность.

Рассмотренное представление не является единственным каноническим представлением целых чисел. Как уже отмечалось, для выбора канонического представления можно воспользоваться единственностью разложения натурального числа на простые множители. Такое представление целого числа может быть применено в тех задачах, где используются только операции умножения и деления, так как они становятся очень “дешевыми”, однако несоизмеримо возрастает стоимость операций сложения и вычитания, что препятствует использованию подобного представления. В некоторых задачах отказ от канонического представления дает значительный выигрыш в быстродействии, в частности, может использоваться частичное разложение числа на множители. Особенно полезен аналогичный метод при работе не с числами, а с многочленами.

Если известно, что при работе программы все встречающиеся в вычислениях целые числа ограничены по абсолютной величине некоторой заданной константой, то можно использовать для задания таких чисел их систему вычетов по модулям некоторых взаимно простых чисел, произведение которых превосходит упомянутую константу. Вычисления с классами вычетов выполняются, как правило, быстрее, чем арифметика многократной точности. А арифметикой

многократной точности при таком подходе нужно пользоваться только при вводе или выводе информации.

Отметим, что наряду с каноническими представлениями в системах компьютерной алгебры используются и другие представления. В частности, желательно, чтобы наличие или отсутствие знака '+' перед целым числом не влияло на восприятие его компьютером. Таким образом, для положительных чисел получается неоднозначное представление, хотя форма отрицательных чисел определена однозначно.

```
<положительное целое> == <натуральное число> |
                         + <натуральное число>
<отрицательное целое> == - <натуральное число>
```

Другое требование — на восприятие числа не должно влиять наличие нулей перед первой значащей цифрой.

1.3. Упражнения.

(1) Оценить количество одноразрядных умножений, используемых при умножении столбиком m-значного числа на n-значное.

(2) Показать, что два двузначных числа можно перемножить, используя только 3 умножения однозначных чисел и увеличив число сложений.

(3) Найти алгоритм деления длинных чисел, не требующий большого перебора при нахождении первой цифры частного.

(4) Описать алгоритм перевода натуральных чисел из m-ичной системы счисления в n-ичную.

(5) В *римской нумерации* для записи чисел используются следующие символы: I — единица, V — пять, X — десять, L — пятьдесят, C — сто, D — пятьсот, M — тысяча. Символ считается отрицательным, если правее него найдется символ большего числа, и положительным в противном случае. Например, число 1948 в этой системе запишется так: MCMXLVIII. Сформулировать алгоритм перевода числа из римской записи в десятичную и обратно. Реализовать полученный алгоритм на одном из алгоритмических языков (например, C). Ограничения на исходные данные: $1 \leqslant N < 3700$, в записи результата ни один символ не должен появляться больше 3 раз.

(6) Сформулировать алгоритм и написать программу сложения натуральных чисел в римской нумерации.

(7) Будем говорить, что мы имеем дело с системой счисления со *смешанным или векторным основанием*, если нам задан вектор из n натуральных чисел $M = (m_1, \ldots, m_n)$ (основание счисления) и запись $K = (k_0, k_1, \ldots, k_n)$ обозначает число $k = k_0 + m_1(k_1 + m_2(k_2 + \cdots + m_n \cdot k_n) \ldots))$. Написать программу, которая по данным (день недели, часы, минуты, секунды) определяет, сколько секунд прошло с начала недели (понедельник, $0, 0, 0) = 0$, и выполняет обратное преобразование.

1.2. Кольца вычетов и конечные поля. Кольца вычетов и конечные поля представляют собой наиболее простые объекты с точки зрения задачи представления данных. Каждому элементу такого кольца или поля, состоящего из n элементов, можно сопоставить, например, взаимно однозначно неотрицательное целое число из отрезка $[0, n-1]$. Для колец вычетов — это сопоставление каждому классу вычетов его единственного элемента, лежащего в $[0, n-1]$, при этом арифметические операции над такими "числами" выполняются как операции над целыми числами по модулю n. Часто в качестве системы представителей кольца вычетов $\mathbb{Z}/n\mathbb{Z}$ выбирается отрезок $[-(n-1)/2, (n-1)/2]$ при нечетном n и $[-n/2+1, n/2]$ при четном n. Арифметические операции $+$, $-$, $*$ реализуются очевидным образом, для реализации операции деления обычно используется *расширенный алгоритм Евклида* (см. § 5).

Хотя элементы конечного поля из n элементов также находятся во взаимнооднозначном соответствии с целыми числами из отрезка $[0, n-1]$, это соответствие не является таким же естественным, в частности, арифметические операции выполняются по более сложным правилам. Чаще используются другие формы представления, например, для записи элементов *простого поля* из p элементов используется система вычетов по модулю p, а поле $GF(p^k)$ представляется в виде факторкольца кольца многочленов $\mathbb{Z}_p[x]$ по идеалу, порожденному некоторым неприводимым по модулю p многочленом степени k.

Сформулируем основные результаты о конечных полях.

(1) Любая конечная область целостности является полем (следует из взаимной однозначности умножения на любой ненулевой элемент).

(2) Характеристика конечного поля является простым числом (следует из отсутствия делителей нуля).

(3) Любое конечное поле $GF(q)$ характеристики p состоит из $q = p^k$ элементов, где k — натуральное число (поскольку оно является векторным пространством над $\mathbb{Z}/p\mathbb{Z}$, k — размерность этого пространства).
(4) Мультипликативный порядок любого ненулевого элемента поля $GF(q)$ делит $q-1$ (ненулевые элементы образуют по умножению группу порядка $q-1$).
(5) Мультипликативная группа поля $GF(q)$ является циклической, т. е. существует элемент порядка $q-1$ (следует из однозначности разложения на множители многочленов x^m-1 над любым полем).
(6) Любые два конечных поля, содержащих одинаковое число элементов, изоморфны (следует из однозначности поля разложения для многочлена $x^{q-1}-1$).
(7) $GF(p^k) \subset GF(p^m) \iff k|m$.

Таким образом, существует два принципиально разных подхода к построению канонического представления элементов конечного поля $GF(p^k)$:

(1) (векторное представление) выбрать элемент x такой, что его степени $x^0 = 1, x, x^2, \ldots, x^{k-1}$ порождают наше поле как векторное пространство над простым подполем $\mathbb{Z}/p\mathbb{Z}$, и любой элемент записывать как вектор в этом базисе;
(2) (степенное представление) найти примитивный элемент α, порождающий мультипликативную группу этого поля, и любой элемент поля представлять в виде степени элемента α.

Отметим, что переход от степенного представления к векторному достаточно прост, а обратный переход (вычисление дискретного логарифма) — очень сложен. Сложность этой задачи используется в криптографии для построения систем кодирования с открытым ключом.

1.4. Упражнения.

(1) Показать, что кольцо вычетов по модулю p^2 не изоморфно конечному полю из p^2 элементов.
(2) Составить таблицу умножения и деления для колец $\mathbb{Z}_4$ и $\mathbb{Z}_9$ и для полей $GF(4)$ и $GF(9)$.
(3) Для заданной матрицы размера $p^2 \times p^2$, где $p = 2$ или 3, проверить, является ли она таблицей умножения в поле $GF(p^2)$ при какой-либо нумерации элементов этого поля.
(4) Реализовать алгоритм деления в кольце вычетов $\mathbb{Z}_n$ (учесть возможность получения неоднозначного результата).

(5) **Китайская теорема об остатках**. Дано k взаимно простых натуральных чисел $m_i > 1$. Для любого набора из k целых чисел a_i, $1 \leqslant i \leqslant k$, найти $a \in \mathbb{Z}$, $0 \leqslant a < \prod_{i=1}^{k} m_i$, такое, что $a \equiv a_i \pmod{m_i}$ для всех i от 1 до k.
(6) Обобщить предыдущую задачу на случай, когда числа m_i не обязательно взаимно просты.
(7) Найти все неприводимые над полем $\mathbb{Z}_p$ многочлены степени n (n небольшое).
(8) Найти число неприводимых над полем $\mathbb{Z}_p$ многочленов степени n.

1.3. Рациональные числа. Множество рациональных чисел $\mathbb{Q}$ определяется как фактормножество множества пар $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, $b \neq 0$, по отношению эквивалентности: $(a, b) \sim (c, d) \iff ad - bc = 0$. Если у нас фиксирована каноническая форма целого числа, то каноническую форму рационального числа мы можем получить, например, выбирая из эквивалентных пар целых чисел (a, b) такую, у которой $b > 0$ и НОД$(a, b) = 1$. Все сказанное выше о представлении целых чисел относится и к представлению рациональных чисел.

Естественно, приведенная выше каноническая форма рационального числа не является единственно возможной. Из школьного курса известно, что любое рациональное число можно представить в виде бесконечной десятичной периодической дроби. Также известно, что любая бесконечная периодическая дробь представляет рациональное число, причем соответствие между рациональными дробями и бесконечными десятичными периодическими дробями не является взаимно однозначным: рациональные числа, знаменатели которых имеют вид $2^n 5^m$, могут быть представлены периодическими дробями с периодами (0) и (9).

1.5. Упражнения. Пусть m — натуральное число, $m > 1$, рассматриваемое как основание системы счисления.

(1) Доказать, что рациональные числа могут быть представлены бесконечными периодическими m-ичными дробями, причем неоднозначно.
(2) Доказать, что любая бесконечная периодическая m-ичная дробь представляет некоторое рациональное число.
(3) Установить взаимнооднозначное соответствие между множеством рациональных дробей и некоторым подмножеством бесконечных периодических m-ичных дробей.
(4) Написать программу перевода рациональных чисел в бесконечные периодические m-ичные дроби и обратно.

(5) Сформулировать и реализовать алгоритмы арифметических операций над рациональными числами, представленными в виде бесконечных периодических m-ичных дробей.

Часто рациональные числа представляют в виде суммы целого числа и правильной дроби, т. е. положительного рационального числа $0 < \alpha < 1$. Исследователи утверждают, что в древнем Египте имелись обозначения только для дробей с числителем 1, остальные числа представлялись в виде суммы таких дробей.

1.6. Упражнения.

(1) Доказать, что любое положительное рациональное число $0 < \alpha < 1$ можно представить в виде суммы обратных величин различных натуральных чисел.
(2) Показать, что такое представление не единственно.
(3) Описать алгоритм, выбирающий из всех возможных представлений такого вида единственное.
(4) Написать программу, представляющую любое положительное рациональное число $0 < \alpha < 1$ в виде суммы обратных величин различных натуральных чисел.

1.4. Приближенные вычисления. Хотя выше и отмечалось, что в компьютерной алгебре вычисления обычно производятся точно, без округления, тем не менее в ней рассматриваются и задачи, требующие приближенного решения (например, нахождение вещественных корней многочлена). В отличие от численного анализа ответ в таких задачах представляется не в виде числа, а в виде интервала на вещественной оси (области в комплексной плоскости). С такими интервалами можно производить арифметические действия, соответствующая арифметика известна под названием *интервальной*. Как правило, интервальная арифметика комбинируется с арифметикой многократной точности, поскольку требуемая точность обычно весьма высока.

Когда мы говорим о приближенных вычислениях, то подразумеваем, что определено понятие *сходимости*. Из курса математического анализа известно, что поле вещественных чисел $\mathbb{R}$ можно определить как пополнение поля рациональных чисел $\mathbb{Q}$ по *архимедовой метрике*, когда расстояние между двумя рациональными числами определяется как модуль их разности. В математике, в частности, в теории чисел, рассматриваются также другие метрики поля рациональных чисел, так называемые p-адические. При пополнении поля $\mathbb{Q}$ по p-адической метрике получается *поле p-адических чисел*. Некоторые сведения о таких полях приведены в § 2.

При вычислениях с вещественными числами мы, в действительности, имеем дело обычно с их приближенными значениями, которые представляют собой десятичные (или двоичные, при использовании компьютера) дроби с фиксированным числом значащих цифр. При работе с приближенными значениями p-адических чисел получаются объекты, которые известны как *коды Гензеля*. Их описание можно найти в специальной литературе, например, [**5**].

1.7. Упражнения.

(1) Привести пример аксиомы поля вещественных чисел, не выполняющейся при работе с числами типа `float` на языке Си.
(2) Какие аксиомы поля вещественных чисел не выполняются при работе с числами типа `float` на языке Си?
(3) Привести пример аксиомы поля вещественных чисел, не выполняющейся для интервальной арифметики.
(4) Какие аксиомы поля вещественных чисел не выполняются для интервальной арифметики?

1.5. Алгебраические числа.

1.8. Определение. *Алгебраическим числом* называется число α, являющееся корнем многочлена от одной переменной с целыми коэффициентами. Если старший коэффициент этого многочлена равен 1, то алгебраическое число называется *целым*.

1.9. Предложение. *Существуют алгебраические числа, не выражающиеся через радикалы.*

Доказательство этого утверждения основано на теории Галуа и может быть найдено в учебниках по алгебре.

Таким образом, в поле алгебраических чисел можно выделить подполя алгебраических чисел, порожденных простыми радикалами (*простые радикальные расширения*) и вложенными радикалами (*вложенные радикальные расширения*), а также соответствующие подкольца в кольце целых алгебраических чисел.

Представление алгебраических чисел представляет собой значительно более трудную задачу. Если речь идет об одном алгебраическом числе, то для его задания нужно знать минимальный многочлен, корнем которого является данное число. В большинстве алгебраических задач несущественно различие между различными корнями одного и того же неприводимого многочлена. Однако в задачах,

где используются различные метрические свойства, часто приходится для задания алгебраического числа указывать не только соответствующий неприводимый многочлен, но и интервал на вещественной оси или область в комплексном пространстве, содержащую единственный корень указанного многочлена. При этом арифметические операции над алгебраическими числами оказываются очень трудоемкими. Нахождение минимального многочлена для суммы или произведения алгебраических чисел представляет собой нетривиальную задачу, методы его нахождения будут описаны ниже, при изучении базисов Грёбнера.

При работе с конкретным полем алгебраических чисел используется представление чисел этого поля, связанное с фиксированием *примитивного элемента* и с однозначностью представления элементов этого поля через фиксированный примитивный элемент. Упомянутые выше сложности возникают при необходимости производить операции над элементами из различных конечных расширений поля рациональных чисел. Эти сложности настолько значительны, что часто приходится отказываться от выбора примитивного элемента и рассматривать поля алгебраических чисел как расширения поля рациональных чисел с многими образующими. В частности, такое представление обычно используется при работе с радикальными расширениями, т. е. с расширениями поля рациональных чисел, получаемыми последовательным присоединением радикалов некоторых элементов (возможно, с вложениями).

1.10. Упражнения.

(1) Показать, что $\sqrt{2}$, $\sqrt{3}+\sqrt{2}$, $\sqrt{2+\sqrt{5}}$ — целые алгебраические числа.
(2) Показать, что целые алгебраические числа образуют кольцо.
(3) Показать, что алгебраические числа образуют поле.
(4) Найти минимальный многочлен над $\mathbb{Q}$ для $\sqrt{2}+\sqrt{3}$.
(5) Построить каноническое представление для элементов поля $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$.
(6) Построить алгоритм получения канонического представления для простых радикальных расширений (полей алгебраических чисел, порожденных несколькими радикалами без вложений).
(7) Построить алгоритм получения канонического представления для вложенных радикальных расширений.

1.6. Трансцендентные числа. Большинство систем компьютерной алгебры допускает работу с трансцендентными числами e и π, для которых фиксированы соответствующие свойства тригонометрических, логарифмических и показательных функций. Вычисления в трансцендентных расширениях производятся так же, как в полях рациональных функций. Задание конкретного трансцендентного числа какими-либо метрическими или функциональными свойствами и проверка его алгебраической независимости с уже имеющимися величинами представляет собой алгоритмически неразрешимую задачу.

2. p-адические числа

2.1. Целые p-адические числа. p-адические числа играют значительную роль в теории чисел, и для более подробного знакомства с ними читателю следует обратиться к литературе по теории чисел, например к книге [**3**]. Здесь мы только приведем основные определения и некоторые свойства p-адических чисел.

2.1. Определение. Пусть p — некоторое простое число. Последовательность целых чисел

$$\{x_n\} = \{x_0, x_1, \dots, x_n, \dots\},$$

обладающая тем свойством, что

$$x_n \equiv x_{n-1} \pmod{p^n} \tag{2.1}$$

для всех $n \geqslant 1$, определяет новый объект, называемый *целым p-адическим числом*. Две последовательности $\{x_n\}$ и $\{x'_n\}$ тогда и только тогда определяют одно и то же целое p-адическое число, когда $x_n \equiv x'_n \pmod{p^{n+1}}$ для всех $n \geqslant 0$.

В отличие от целых p-адических чисел, обычные целые числа часто называют целыми рациональными.

Каждому целому рациональному числу x можно сопоставить целое p-адическое число, определяемое последовательностью

$$\{x, x, \dots, x, \dots\}.$$

Это p-адическое число будем обозначать той же буквой x. Множество целых p-адических чисел будем обозначать O_p.

Укажем способ, при помощи которого из всех последовательностей, определяющих одно и то же p-адическое число, можно выбрать одну стандартную.

Пусть $\{x_n\}$ — целое p-адическое число. Обозначим через $\bar{x}_n$ наименьшее неотрицательное число, сравнимое с x_n по модулю p^{n+1}, т. е.

$$x_n \equiv \bar{x}_n \pmod{p^{n+1}}, \tag{2.2}$$

$$0 \leqslant \bar{x}_n < p^{n+1}. \tag{2.3}$$

Для любого целого p-адического числа $\{x_n\}$, последовательность, все члены которой удовлетворяют условиям (2.2) и (2.3), будем называть *канонической*.

Ставя в соответствие каждому целому p-адическому числу его каноническую последовательность, мы получаем взаимно однозначное соответствие между множеством целых p-адических чисел и множеством последовательностей вида

$$\{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \dots, \},$$

где $0 \leqslant a_i < p$.

2.2. Определение. Суммой и произведением целых p-адических чисел α и β, определяемых последовательностями $\{x_n\}$ и $\{y_n\}$, называются целые p-адические числа, определяемые соответственно последовательностями $\{x_n + y_n\}$ и $\{x_n y_n\}$.

2.3. Упражнение. Показать, что введенные выше операции определены корректно и превращают O_p в коммутативное кольцо с единицей.

Сформулируем несколько теорем, доказательство которых оставляется читателю в качестве упражнения (их можно найти, например, в [**3**]).

2.4. Теорема. *Целое p-адическое число α, определяемое последовательностью $\{x_0, x_1, \dots, x_n, \dots\}$, тогда и только тогда является единицей (т. е. обратимым) в O_p, когда $x_0 \not\equiv 0 \pmod{p}$.*

2.5. Теорема. *Всякое отличное от нуля целое p-адическое число α однозначно представляется в виде*

$$\alpha = p^m \varepsilon, \tag{2.4}$$

где ε — единица кольца O_p.

2.6. Теорема. *Для любого натурального n, всякое целое p-адическое число сравнимо с целым рациональным числом по модулю p^n. Два целых рациональных числа тогда и только тогда сравнимы по модулю p^n в кольце O_p, когда они сравнимы по этому модулю в кольце $\mathbb{Z}$.*

2.7. Определение. Число m в представлении (2.4) отличного от нуля целого p-адического числа α называется *p-показателем* числа α и обозначается $\nu_p(\alpha)$.

Индекс p в определении показателя мы будем часто опускать и говорить просто о *п*оказателе, обозначая его $\nu(\alpha)$. Доопределим показатель, полагая $\nu(0)=\infty$. Непосредственно проверяется, что

$$\nu(\alpha\beta)=\nu(\alpha)+\nu(\beta), \tag{2.5}$$

$$\nu(\alpha+\beta)\geqslant\min(\nu(\alpha),\nu(\beta)), \tag{2.6}$$

$$\nu(\alpha+\beta)=\min(\nu(\alpha),\nu(\beta)),\quad\text{если}\quad\nu(\alpha)\neq\nu(\beta). \tag{2.7}$$

2.2. Дробные p-адические числа.

2.8. Определение. Дробь вида $\frac{\alpha}{p^k}$, $\alpha\in O_p$, $k\geqslant 0$, определяет *дробное p-адическое число* или просто *p-адическое число*. Две дроби, $\frac{\alpha}{p^k}$ и $\frac{\beta}{p^m}$, определяют одно и то же p-адическое число, если $\alpha p^m=\beta p^k$ в O_p.

Совокупность всех p-адических чисел обозначается R_p. Легко проверить, что операции сложения и умножения продолжаются с O_p на R_p и превращают R_p в поле.

2.9. Теорема. *Всякое p-адическое число $\xi\neq 0$ единственным образом представляется в виде*

$$\xi=p^m\varepsilon, \tag{2.8}$$

где m — целое число, а ε — единица кольца O_p.

2.10. Теорема. *Всякое отличное от нуля p-адическое число ξ однозначно представляется в виде*

$$\xi=p^m(a_0+a_1p+\dots+a_np^n+\dots), \tag{2.9}$$

где $m=\nu_p(\xi)$, $1\leqslant a_0\leqslant p-1$, $0\leqslant a_n\leqslant p-1$ $(n=1,2,\dots)$.

2.3. Аксиоматическая характеристика поля p-адических чисел. Выбрав некоторое вещественное число ρ, такое, что $0<\rho<1$, (например, $\rho=1/p$) положим

$$\varphi_p(\xi)=\begin{cases}\rho^{\nu_p(\xi)} & \text{при } \xi\neq 0,\\ 0 & \text{при } \xi=0.\end{cases} \tag{2.10}$$

2.11. Определение. Функция $\varphi_p(\xi)$, $\xi\in R_p$, определенная условиями (2.10), называется *p-адической метрикой*. Значение $\varphi_p(\xi)$ называется *величиной p-адического числа ξ* в этой метрике.

Как и в случае показателя, функцию φ_p иногда будем называть просто метрикой и обозначать φ.

Легко проверяется, что p-адическая метрика обладает следующими свойствами:

$$\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta), \tag{2.11}$$

$$\varphi(\xi + \eta) \leqslant \max(\varphi(\xi), \varphi(\eta)), \tag{2.12}$$

$$\varphi(\xi + \eta) \leqslant \varphi(\xi) + \varphi(\eta). \tag{2.13}$$

Свойства (2.11) и (2.13) указывают, что введенное понятие является аналогом абсолютной величины в поле вещественных чисел.

2.12. Определение. Пусть k — произвольное поле. Функция φ, определенная на элементах α поля k и принимающая вещественные значения $\varphi(\alpha)$, называется *метрикой поля* k, если она обладает следующими свойствами:

(1) $\varphi(\alpha) > 0$ при $\alpha \neq 0$; $\varphi(0) = 0$;
(2) $\varphi(\alpha + \beta) \leqslant \varphi(\alpha) + \varphi(\beta)$;
(3) $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Поле k вместе с заданной в нем метрикой φ называется *метризованным полем*.

Из определения легко вытекают следующие свойства метрик:

$$\varphi(\pm 1) = 1;$$
$$\varphi(-\alpha) = \varphi(\alpha);$$
$$\varphi(\alpha - \beta) \leqslant \varphi(\alpha) + \varphi(\beta);$$
$$\varphi(\alpha \pm \beta) \geqslant |\varphi(\alpha) - \varphi(\beta)|;$$
$$\varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)} \quad (\beta \neq 0).$$

2.13. Пример. Метриками являются:

(1) абсолютная величина в поле рациональных чисел;
(2) абсолютная величина в поле вещественных чисел;
(3) модуль в поле комплексных чисел;
(4) p-адическая метрика φ_p в поле p-адических чисел R_p;
(5) функция $\varphi(\alpha)$, определенная в произвольном поле k условиями: $\varphi(0) = 0$, $\varphi(\alpha) = 1$ при $\alpha \neq 0$. Такая метрика называется *тривиальной*.

Если метрику φ_p поля R_p мы рассматриваем лишь на рациональных числах, то получаем некоторую новую метрику поля рациональных чисел $\mathbb{Q}$. Эта метрика, обозначаемая также через φ_p, называется p-адической метрикой поля $\mathbb{Q}$.

Аксиоматически поля вещественных и p-адических чисел можно определить следующим образом.

Поле вещественных чисел $\mathbb{R}$ — это пополнение поля рациональных чисел $\mathbb{Q}$ по метрике 1.

Поле p-адических чисел R_p — это пополнение поля рациональных чисел $\mathbb{Q}$ по p-адической метрике.

2.14. Упражнение. Представить число -1 в поле p-адических чисел в виде ряда (2.9).

2.15. Упражнение. Представить число $-\frac{2}{3}$ в поле 5-адических чисел в виде ряда (2.9).

2.16. Упражнение. Доказать для многочленов над полем p-адических чисел *признак неприводимости Эйзенштейна*: многочлен $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ с целыми p-адическими коэффициентами неприводим над полем R_p, если a_0 не делится на p, все остальные коэффициенты $a_1, \ldots, a_n$ делятся на p и свободный член a_n, делясь на p, не делится на p^2.

3. Многочлены и рациональные функции

3.1. Многочлены. Действия с многочленами лежат в основе любой системы компьютерной алгебры. Пусть K — некоторое кольцо, задача представления элементов которого уже решена. Представление элементов кольца многочленов $K[x]$ можно выбирать различными способами. Наиболее распространенным является представление многочлена в виде последовательности коэффициентов, упорядоченной по возрастанию или убыванию степеней одночленов. Представление многочленов, при котором запоминаются все коэффициенты, включая нулевые, называется *плотным*. Плотное представление используется в задачах, где рассматриваемые многочлены имеют сравнительно небольшое количество нулевых коэффициентов. Если степени многочленов достаточно высоки, а количество ненулевых коэффициентов мало (*разреженные многочлены*), то удобнее использовать *разреженное представление многочленов*, в котором указываются только ненулевые коэффициенты и соответствующие степени одночленов. При этом алгоритмы работы с такой формой записи становятся более сложными, но значительно экономится память ЭВМ, а во многих случаях — и время работы программы.

Приведенная выше форма представления многочленов в случае, когда кольцо коэффициентов является полем, основана на том факте, что одночлены составляют базис кольца многочленов, рассматриваемого как бесконечномерное векторное пространство над полем коэффициентов. В некоторых случаях целесообразно использовать другие базисы этого пространства. Например, в главе 4 изучаются многочлены вида $\binom{x+k}{k} = \frac{(x+k)(x+k-1)\ldots(x+1)}{k!}$, обладающие многими полезными свойствами. Часто оказывается полезным представление многочленов фиксированной степени набором значений в разных точках.

Многочлены от многих переменных можно рекурсивно рассматривать как многочлены от одной переменной, но с коэффициентами из кольца многочленов от меньшего числа переменных (*рекурсивное представление*). А можно на множестве одночленов ввести отношение порядка и записывать слагаемые в соответствии с выбранным порядком. Наиболее часто используются следующие три отношения порядка:

- лексикографическое упорядочение мономов, получающееся из фиксированного порядка на множестве переменных;
- упорядочение мономов по степеням, а мономы одной и той же степени упорядочиваются лексикографически;
- упорядочение мономов по степеням, а мономы одной и той же степени упорядочиваются в обратном лексикографическом порядке, т. е. при равенстве степеней бóльшим считается вектор с меньшей последней координатой, при равенстве последних координат — с меньшей предпоследней и т. д. Может показаться, что этот порядок совпадает с предыдущим, для "отраженных" векторов. При $n = 2$ это действительно так, однако в общем случае эти два отношения порядка различаются более существенно, что продемонстрировано в примере 3.1б), где предполагается, что $x > y > z$.

Более подробно вопросы, связанные с упорядочением мономов и каноническим представлением многочленов от нескольких переменных, будут рассмотрены ниже в разделе, посвященном базисам Грёбнера.

3.1. Примеры.

а) Пусть переменные x и y упорядочены так, что $x > y$. Тогда многочлен $(x+y)^2 + x + y + 1$ с учетом соответствующих порядков записывается в виде:

$x^2+2xy+x+y^2+y+1$ (лексикографический порядок);
$x^2+2xy+y^2+x+y+1$ (по степени, затем лексикографический);
$y^2+2xy+x^2+y+x+1$ (по степени, затем обратный лексикографический).

б) Рассмотрим разложение многочлена $(x+y+z)^3$. Из однородности многочлена следует, что первые два из рассматриваемых порядков для этого многочлена совпадают. Выпишем его представление с использованием второго и третьего порядка.
$x^3+3x^2y+3x^2z+3xy^2+6xyz+3xz^2+y^3+3y^2z+3yz^2+z^3$
и
$x^3+3x^2y+3xy^2+y^3+3x^2z+6xyz+3y^2z+3xz^2+3yz^2+z^3$
соответственно.

Можно пользоваться как плотной (когда записываются все коэффициенты от самого старшего до самого младшего или наоборот), так и разреженной (когда записываются только ненулевые коэффициенты и соответствующие степени) формой записи. В отличие от многочленов от одной переменной, для которых используется как разреженное, так и плотное представление, для многочленов от нескольких переменных плотное представление почти не применяется, поскольку уже при сравнительно небольших степенях количество коэффициентов в этих многочленах весьма велико и почти все они нулевые.

Отметим, что достаточно часто при действии с многочленами предпочтительнее пользоваться представлениями, отличными от канонического. Например, во многих отношениях запись $(x+y+z)^3$ более удобна, чем приведенные выше разложения этого многочлена. В частности, для многочленов задача разложения на множители представляет еще большую сложность, чем для целых чисел, и поэтому не всегда целесообразно раскрывать при умножении скобки, — часто бывает полезным в ущерб каноничности записи хранить многочлен в виде произведения.

3.2. Рациональные функции. Поле рациональных функций $K(x_1,\ldots,x_n)$, где K — некоторое поле, обычно определяется как поле частных кольца многочленов $K[x_1,\ldots,x_n]$. Имея каноническое представление элементов кольца многочленов, каноническое представление рациональных функций можно получить наложением

условия взаимной простоты числителя и знаменателя и нормировкой знаменателя (например, приравниванием старшего коэффициента знаменателя единице). Часто, однако, поле K само представляется как поле частных некоторой области целостности, например, поле $\mathbb{Q}(x)$ можно представить как поле частных кольца $\mathbb{Q}[x]$, а также как поле частных кольца $\mathbb{Z}[x]$. При представлении поля $\mathbb{Q}(x)$ как поля частных кольца $\mathbb{Z}[x]$ далеко не всегда можно в представлении рациональной функции приравнять старший коэффициент знаменателя единице. Множество обратимых элементов в $\mathbb{Z}$ состоит всего из двух элементов (1 и -1), и нормировку знаменателя можно осуществить, фиксируя знак старшего коэффициента.

3.3. Обобщенные многочлены и рациональные функции. В дифференциальной алгебре имеется ряд объектов, которые можно рассматривать как обобщение кольца многочленов. К ним относятся алгебры Вейля, кольца дифференциальных операторов и кольца дифференциальных многочленов. Строгое определение колец дифференциальных операторов и колец дифференциальных многочленов будет дано ниже, здесь отметим только, что элементы алгебры Вейля или кольца дифференциальных операторов могут быть представлены в виде суммы одночленов от фиксированного конечного множества переменных с коэффициентами из фиксированного поля, т. е. так же, как и элементы кольца многочленов (допускается как плотная, так и разреженная запись). Сложности вычислений в таких кольцах связаны с некоммутативностью умножения. Некоммутативность умножения особенно сказывается при рассмотрении тел частных для этих колец (существование их доказывается в курсах по теории колец): правое частное двух элементов может не совпадать с их левым частным, правые множители отличаются от левых множителей, приходится рассматривать правые и левые наибольшие общие делители и наименьшие общие кратные, которые для взаимно простых элементов не совпадают с их произведениями.

В этом параграфе приводятся основные определения и результаты из дифференциальной и разностной алгебры, которые понадобятся нам в дальнейшем.

3.2. Определение. Оператор δ, действующий на некотором кольце, называется *оператором дифференцирования* (или просто *дифференцированием*), если $\delta(a+b) = \delta a + \delta b$ и $\delta(ab) = (\delta a)b + a\delta b$ для всех элементов a, b этого кольца. *Дифференциальным кольцом* называется коммутативное кольцо R с конечным множеством $\Delta = \{\delta_1, \ldots, \delta_n\}$ операторов дифференцирования кольца R, таких,

что $\delta\delta' a = \delta'\delta a$ ($a \in R$, $\delta \in \Delta$, $\delta' \in \Delta$); если $n = 1$, то дифференциальное кольцо R называется *обыкновенным*, если $n > 1$, то R называется *кольцом с частными производными*. Если кольцо R является полем, то мы говорим о *дифференциальном поле*.

3.3. Упражнения.

(1) Показать, что любое кольцо можно рассматривать как дифференциальное кольцо с нулевым дифференцированием. Показать, что на кольцах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/m\mathbb{Z}$ нет ненулевых дифференцирований.

(2) Кольцо многочленов $R[x]$ от одной переменной над обыкновенным дифференциальным кольцом можно превратить в обыкновенное дифференциальное кольцо, произвольным образом задав значение δx. Показать, что значением δx продолжение дифференцирования δ на кольцо $R[x]$ определяется однозначно. Аналогичное утверждение верно для кольца формальных степенных рядов.

(3) Пусть R — дифференциальное кольцо без делителей нуля, F — его поле частных. Показать, что F можно единственным образом превратить в дифференциальное поле, содержащее дифференциальное кольцо R.

(4) Поле мероморфных в некоторой области вещественного n-мерного пространства функций можно рассматривать как дифференциальное поле, с множеством дифференцирований $\Delta = \{\partial/\partial x_i\}$.

3.4. Определение. Пусть R — дифференциальное кольцо с множеством операторов дифференцирования Δ. Под *дифференциальным модулем* над R или *дифференциальным R-модулем* мы понимаем R-модуль M, на котором действуют операторы множества Δ в соответствии со следующими правилами:

$$\delta(u+v) = \delta u + \delta v, \qquad \delta(au) = (\delta a)u + a\delta u,$$
$$(\delta \in \Delta, \quad u \in M, \quad v \in M, \quad a \in R).$$

Дифференциальный модуль можно рассматривать как левый модуль над кольцом косых многочленов $R[\Delta] = R[\delta_1, \ldots, \delta_n]$ дифференциального типа. Это кольцо мы будем называть *кольцом линейных дифференциальных операторов*. Пусть T обозначает свободную коммутативную полугруппу (записанную мультипликативно), порожденную элементами из множества Δ. Каждый элемент кольца

$R[\Delta]$ может быть единственным способом выражен в виде конечной суммы

$$\sum_{\theta\in T} a_\theta\theta = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n}\delta_1^{i_1}\delta_2^{i_2}\dots\delta_n^{i_n},$$

умножение образующих определяется правилами:

$$\delta_i\delta_j = \delta_j\delta_i, \quad \delta_i a = a\delta_i + \delta_i(a), \quad \text{где} \quad \delta_i, \delta_j \in \Delta,\ a \in R,$$

и на все кольцо $R[\Delta]$ распространяется по линейности.

В предположении, что для кольца коэффициентов R каноническое представление фиксировано, каноническое представление кольца дифференциальных операторов $R[\Delta]$ получается так же, как и для кольца многочленов: достаточно упорядочить полугруппу T. Обычно рассматриваются отношения порядка, перечисленные в параграфе 3.1.

3.5. Пример. Пусть R — кольцо многочленов над полем K, $R = K[x_1, \dots, x_m]$, и $\Delta = \{d_1, \dots, d_m\} = \{\partial/\partial x_1, \dots, \partial/\partial x_m\}$. Тогда кольцо линейных дифференциальных операторов $R[\Delta]$ называется *алгеброй Вейля* над K и обозначается $A_m(K)$.

Кольцо линейных дифференциальных операторов обладает многими свойствами, аналогичными свойствам кольца многочленов, в частности, если кольцо коэффициентов является дифференциальным полем, то в кольце дифференциальных операторов нет делителей нуля, для любых двух элементов существует наибольший общий делитель (правый или левый, причем в общем случае они не совпадают) и наименьшее общее кратное (правое и левое, снова не совпадающие); если F — δ-поле, то в $F[\delta]$ имеется алгоритм Евклида для нахождения левого (правого) наибольшего общего делителя.

3.6. Упражнения. Пусть F — обыкновенное дифференциальное поле с дифференцированием δ. Доказать следующие свойства кольца $R = F[\delta]$ линейных дифференциальных операторов над F:

(1) в R нет делителей нуля;
(2) R является кольцом главных левых (правых) идеалов;
(3) в R нет нетривиальных двусторонних идеалов;
(4) в R имеется алгоритм Евклида для нахождения левого (правого) НОД двух операторов;
(5) в R имеется расширенный алгоритм Евклида для нахождения левого (правого) НОД двух операторов;
(6) R не обязательно является кольцом с однозначным разложением на множители (привести пример дифференциального поля F, для которого это свойство не выполняется).

Кольцо $R[\Delta]$ иногда называют кольцом дифференциальных многочленов, но мы будем придерживаться терминологии, принятой в монографии [**23**], где кольцом дифференциальных многочленов над дифференциальным кольцом R называется кольцо $R\{y_1, \ldots, y_r\}$ многочленов от счетного множества переменных $\{\theta y_j : \theta \in T,\ 1 \leqslant j \leqslant r\}$ над кольцом R. В кольце $R\{y_1, \ldots, y_r\}$ операторы дифференцирования из множества Δ действуют на коэффициентах по определению дифференциального кольца, а на образующих θy — по правилу: $\delta(\theta y_j) = (\delta\theta)y_j$.

Кольцо дифференциальных многочленов с точки зрения теории колец представляет собой кольцо коммутативных многочленов от счетного множества переменных (каждый конкретный многочлен зависит только от конечного числа переменных). Таким образом, для решения задачи представления данных кольца дифференциальных многочленов и поля рациональных дифференциальных функций достаточно упорядочить кольцевые образующие. Кольцо дифференциальных многочленов является дифференциальным кольцом, т. е. наряду с операциями сложения и умножения в нем имеются унарные операции дифференцирования, переводящие кольцевую образующую в другую кольцевую образующую, отношение порядка на множестве кольцевых образующих выбирается так, чтобы оно было согласовано с дифференцированиями.

Аналогичные объекты — кольца разностных операторов и кольца разностных многочленов — рассматриваются в разностной алгебре. Кольцо разностных операторов отличается от кольца дифференциальных операторов коммутационными соотношениями, все сказанное выше о кольце дифференциальных операторов можно повторить и для кольца разностных операторов. В кольце разностных многочленов вместо операторов дифференцирования рассматриваются операторы трансляции, которые также переводят кольцевые образующие друг в друга, но на поле коэффициентов являются не дифференцированиями, а автоморфизмами (соответственно, для них можно рассматривать отрицательные степени).

3.7. Определение. *Разностное кольцо* определяется как кольцо R с фиксированным конечным множеством $\Delta = \{\tau_1, \ldots, \tau_n\}$ взаимно коммутирующих мономорфизмов кольца R в себя. Если все мономорфизмы τ_i — изоморфизмы, то R называется *инверсным разностным кольцом*. Если $n = 1$, то R называется *обыкновенным разностным кольцом*, в противном случае R называется *кольцом с частными разностями*. Элементы множества Δ называются *операторами трансляции*.

3.8. Упражнения.

(1) Любое кольцо можно рассматривать как разностное кольцо с тождественным изоморфизмом.

(2) Кольцо многочленов $R[x]$ от одной переменной над обыкновенным разностным кольцом можно превратить в обыкновенное разностное кольцо, произвольным образом задав значение $\tau(x)$. Показать, что значением $\tau(x)$ трансляция кольца $R[x]$ определяется однозначно.

(3) Показать, что не любой автоморфизм τ кольца $R[x]$ продолжается на кольцо формальных степенных рядов.

(4) Пусть R — разностное кольцо без делителей нуля, F — его поле частных. Показать, что F можно единственным образом превратить в разностное поле, содержащее разностное кольцо R.

(5) Поле формальных (сходящихся) рядов Лорана $K((x))$ можно рассматривать как обыкновенное разностное поле с оператором трансляции τ, таким, что $\tau(x) = k \cdot x$, где k — произвольный ненулевой элемент поля K.

3.9. Определение. Пусть R — разностное кольцо с множеством операторов трансляции Δ. Под *разностным модулем* над R, или *разностным R-модулем*, мы понимаем R-модуль M, на котором действуют операторы из множества Δ в соответствии со следующими условиями

$$\tau(u+v) = \tau u + \tau v, \qquad \tau(au) = (\tau a)\tau u,$$
$$(\tau \in \Delta, \quad u \in M, \quad v \in M, \quad a \in R).$$

Разностный модуль M можно рассматривать как левый модуль над кольцом косых многочленов $R[\Delta] = R[\tau_1, \ldots, \tau_n]$ разностного типа. Это кольцо мы будем называть *кольцом разностных операторов*. Пусть T — свободная коммутативная полугруппа (записываемая мультипликативно), порожденная элементами множества Δ. Каждый элемент кольца $R[\Delta]$ может быть единственным образом записан в виде конечной суммы

$$\sum_{\theta \in T} a_\theta \theta = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} \tau_1^{i_1} \tau_2^{i_2} \ldots \tau_n^{i_n},$$

умножение образующих задается соотношениями

$$\tau_i \tau_j = \tau_j \tau_i, \quad \tau_i a = \tau_i(a)\tau_i, \quad \text{где} \quad \tau_i, \tau_j \in \Delta, \ a \in R,$$

и по линейности распространяется на все кольцо $R[\Delta]$. Это кольцо иногда называют кольцом разностных многочленов, но мы будем придерживаться терминологии, принятой в монографии **[18]**,

где кольцом разностных многочленов над разностным кольцом R называют разностное кольцо $R\{y_1, \dots, y_r\}$ многочленов от счетного множества неизвестных $\{\theta y_j \colon \theta \in T,\ 1 \leqslant j \leqslant r\}$ над R. В кольце $R\{y_1, \dots, y_r\}$ операторы трансляции из множества Δ действуют на коэффициентах по определению разностного кольца, а на образующих θy_j — по правилу: $\tau(\theta y_j) = (\tau\theta) y_j$.

3.10. Упражнения. Пусть F — обыкновенное разностное поле с автоморфизмом τ. Доказать следующие свойства кольца $R = F[\tau]$ линейных разностных операторов над F:

(1) в R нет делителей нуля;
(2) R является кольцом главных левых (правых, двусторонних) идеалов;
(3) в R нет нетривиальных двусторонних идеалов;
(4) в R имеется алгоритм Евклида для нахождения левого (правого) НОД двух операторов;
(5) в R имеется расширенный алгоритм Евклида для нахождения левого (правого) НОД двух операторов;
(6) R не обязательно является кольцом с однозначным разложением на множители (привести пример разностного поля F, для которого это свойство не выполняется).

Кольца дифференциальных и разностных многочленов с точки зрения теории колец представляют собой кольца коммутативных многочленов от счетного множества переменных (каждый конкретный многочлен зависит только от конечного числа переменных). Таким образом, для решения задачи представления данных в кольце дифференциальных (разностных) многочленов и поле рациональных дифференциальных (разностных) функций достаточно упорядочить кольцевые образующие. Кольцо дифференциальных многочленов является дифференциальным кольцом, т. е. наряду с операциями сложения и умножения в нем имеются унарные операции дифференцирования, переводящие кольцевую образующую в другую кольцевую образующую, и отношение порядка на множестве кольцевых образующих выбирается так, чтобы оно было согласовано с дифференцированиями. Аналогично, кольцо разностных многочленов является разностным кольцом.

3.4. Векторные пространства и модули. В вычислительной математике и в алгебре понятие векторного пространства над некоторым полем K играет ключевую роль. При фиксированном базисе

пространства задача представления данных не представляет какой-либо сложности — два вектора совпадают тогда и только тогда, когда совпадают все их координаты в фиксированном базисе. Соответствующая структура данных — `вектор элементов типа` K `с индексом` $1..n$ — является одной из базисных структур данных в программировании. Для случая, когда коэффициенты образуют кольцо R, не являющееся полем, положение существенно сложнее — аналогом понятия векторного пространства (множество, замкнутое относительно сложения, вычитания и умножения на элементы кольца с естественными аксиомами сложения и умножения) является в этом случае понятие модуля. Важным частным случаем модуля является свободный модуль над кольцом R (R-модуль). В частности, любое кольцо с единицей можно рассматривать как свободный модуль над самим собой, любой идеал кольца является его подмодулем. С точки зрения задачи представления данных соответствующая структура данных также может быть при фиксированном базисе описана как `вектор элементов типа` R `с индексом` $1..n$.

С другой стороны, свободный модуль над алгеброй обобщенных многочленов можно рассматривать как бесконечномерное векторное пространство над основным полем. В качестве базиса этого пространства удобно выбрать всевозможные произведения мономов из кольца обобщенных многочленов на модульные образующие. Любой элемент модуля содержится в некотором конечномерном подпространстве, порожденном каким-то подмножеством базисных векторов. Выбор базисных векторов и отношения порядка на множестве базисных векторов определяет каноническую форму любого элемента свободного модуля над кольцом обобщенных многочленов.

К сожалению, множество свободных модулей незамкнуто относительно модульных гомоморфизмов, т. е. как подмодули, так и фактормодули свободного модуля не обязаны быть свободными модулями.

3.11. Упражнения.

(1) Привести пример идеала в кольце многочленов от двух переменных, не являющегося свободным модулем над этим кольцом.

(2) Привести пример факторкольца кольца многочленов от одной переменной, не являющегося свободным модулем над этим кольцом.

Глава 2

Наибольший общий делитель и последовательности полиномиальных остатков

5. Наибольший общий делитель. Определения и алгоритмы вычисления

В данном параграфе мы рассмотрим определение наибольшего общего делителя (НОД) двух элементов и алгоритмы его вычисления.

Пусть R — коммутативное кольцо с единицей, $a, b \in R$. Мы говорим, что a *делит* b и пишем $a \mid b$, если существует элемент $c \in R$, такой, что $b = a \cdot c$; если такого элемента не существует, то мы говорим, что a *не делит* b, и пишем $a \nmid b$. Заметим, что определение делимости зависит от рассматриваемого кольца. Так, например, $2 \mid 3$ в поле рациональных чисел $\mathbb{Q}$, но $2 \nmid 3$ в кольце целых чисел $\mathbb{Z}$.

5.1. Определение. Ненулевой элемент $a \in R$ такой, что $ab = 0$ для некоторого $b \neq 0$ называется *делителем нуля* кольца R, а элемент $\varepsilon \in R$, такой, что $\varepsilon \mid 1$ называется *обратимым*, или *делителем единицы*, или *единицей* кольца R.

5.2. Определение. Коммутативное кольцо с единицей и без делителей нуля называется *областью целостности* или просто областью.

5.3. Определение. Пусть R — коммутативное кольцо с единицей. Элемент $a \in R$ называется *неприводимым*, если из представления $a = bc$ в виде произведения двух элементов кольца R, следует, что хотя бы один из элементов b и c обратим в R.

5.4. Определение. Пусть R — коммутативное кольцо с единицей. Идеал $I \subset R$ называется *простым*, если из $bc \in I$ следует, что хотя бы один из элементов b и c лежит в I.

5.5. Определение. Мы говорим, что идеал I *порожден* элементами $b_1, \ldots, b_n$, и пишем $I = (b_1, \ldots, b_n)$, если $b_1, \ldots, b_n \in I$ и любой элемент $b \in I$ может быть записан в виде $b = \sum_{i=1}^{n} c_i b_i$, где $c_i \in R$.

5.6. Определение. Идеал I называется *главным*, если $I = (b)$ для некоторого элемента $b \in I$. Кольцо R называется *кольцом главных идеалов*, если любой идеал кольца R является главным.

5.7. Упражнение. Показать, что $\mathbb{Z}$ и $k[x]$ — кольца главных идеалов, а $\mathbb{Z}[x]$ и $k[x, y]$ — нет.

5.8. Упражнение. Показать, что главный идеал (b) является простым тогда и только тогда, когда b — неприводимый элемент.

5.9. Определение. Элементы a и b кольца R называются *ассоциированными*, если $a = \varepsilon \cdot b$, где ε — единица (обратимый элемент) кольца R.

5.10. Определение. Кольцо R называется *факториальным* или *кольцом с однозначным разложением на множители*, если любой элемент $a \in R$ можно представить в виде $a = \varepsilon \cdot p_1 \cdots p_n$, где ε — единица, а p_i — неприводимые, причем если $a = \varepsilon_1 \cdot q_1 \cdots q_m$ — другое такое разложение, то $m = n$ и для любого индекса i существует индекс j, такой, что p_i ассоциировано с q_j.

5.11. Лемма. *Пусть R — область главных идеалов. Если элемент $a \in R$ допускает разложение на неприводимые множители, то это разложение однозначно в смысле предыдущего определения.*

Доказательство оставим читателю в качестве упражнения. □

5.12. Упражнение. Показать, что $\mathbb{Z}[x]$ и $k[x, y]$ — факториальные кольца.

Сформулируем (без доказательства) теорему, которая позволяет получать новые факториальные кольца.

5.13. Теорема. *Если R — факториальное кольцо, то кольцо многочленов $R[x]$ также факториально.*

Приведем пример нефакториального кольца.

5.14. Пример. Кольцо $\mathbb{Z}[\sqrt{-5}]$ — нефакториально. В частности, $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ — два различных разложения числа 9 на неприводимые множители в этом кольце.

5.15. Определение. Пусть R — коммутативное кольцо с единицей, $a, b \in R$. Элемент $d \in R$ называется *наибольшим общим делителем* элементов a и b, если $d \mid a$, $d \mid b$ и для любого другого элемента d', такого, что $d' \mid a$ и $d' \mid b$ выполняется соотношение $d' \mid d$.

5.16. Упражнение. Показать, что в кольце $\mathbb{Z}$ для любых целых чисел a и b, не равных одновременно нулю, существует наибольшее

целое число, которое делит a и b, и это число является наибольших общим делителем чисел a и b в смысле определения 5.15. Показать, что определение 5.15 в кольце $\mathbb{Z}$ определяет НОД(a,b) неоднозначно.

5.17. Упражнение. Показать, что в кольце $k[x]$ многочленов от одной переменной x над полем k для любых многочленов a и b, не равных одновременно нулю, существует многочлен наибольшей степени, который делит a и b, и этот многочлен является наибольшим общим делителем элементов a и b в смысле определения 5.15. Показать, что определение 5.15 в кольце $k[x]$ определяет НОД(a,b) неоднозначно.

5.1. Свойства НОД(a,b) в $\mathbb{Z}$.

(1) НОД$(a,a) = \{a,-a\}$
(2) НОД$(a,0) = \{a,-a\}$
(3) НОД$(a,b) =$ НОД(b,a)
(4) НОД$(c\cdot a, c\cdot b) = c\cdot$ НОД(a,b)
(5) если НОД$(a,c) = \{1,-1\}$ (в частности, если $c=-1$), то НОД$(a,c\cdot b) =$ НОД(a,b)
(6) НОД$(a,b) =$ НОД$(a-b,b)$
(7) НОД$(a,b) =$ НОД(b,r), где r — остаток от деления a на b

Используя различные комбинации этих свойств, можно получить различные алгоритмы вычисления НОД(a,b) в кольце $\mathbb{Z}$. Пользуясь свойствами 3 и 5, можно свести задачу вычисления НОД в $\mathbb{Z}$ к той же задаче для множества неотрицательных целых чисел и ограничиться представителем только положительного числа в качестве результата. Например, используя свойства 1, 3, 6, можно получить один из простейших алгоритмов вычисления НОД; используя свойства 1, 4, 5 с $c=2$, получаем *бинарный алгоритм* вычисления НОД; а используя свойства 2 и 7, получаем *алгоритм Евклида* нахождения наибольшего общего делителя натуральных чисел.

5.18. Упражнение. Сформулировать перечисленные алгоритмы.

5.2. Евклидовы кольца. Свойство 7 использует понятие "остаток от деления одного числа на другое". На этом свойстве основан алгоритм Евклида, и распространение действия этого алгоритма на другие кольца достигается введением следующего определения.

5.19. Определение. Область целостности R называется *евклидовым кольцом*, если каждому ненулевому элементу $a\in R$ сопоставлено целое неотрицательное число $g(a)$ со следующими свойствами:

(1) если $a\neq 0$ и $b\neq 0$, то $g(ab)\geqslant g(a)$;

(2) для любых двух элементов $a, b \in R$, где $b \neq 0$ существует представление $a = qb + r$, в котором $r = 0$ или $g(r) < g(b)$.

5.20. Упражнение. Доказать, что следующие кольца являются евклидовыми:

(1) кольцо целых чисел $\mathbb{Z}$;
(2) кольцо многочленов $k[x]$ от одной переменной над любым полем k;
(3) любое поле k.

В качестве упражнения читателю предлагается доказать следующую теорему.

5.21. Теорема. *Любое евклидово кольцо является кольцом главных идеалов, а следовательно, факториальным кольцом.*

5.3. Алгоритмы вычисления НОД(a,b) в $\mathbb{Z}$. Сформулируем алгоритмы, предложенные ранее в качестве упражнения. Во всех предложенных ниже алгоритмах считаем, что a и b — натуральные числа, следовательно, ненулевые.

А1. Алгоритм (НОД1).
Дано: $a, b \in \mathbb{N}$
Надо: $d \in \mathbb{N}$,
Переменные: $x, y \in \mathbb{N}$

начало
$x := a$
$y := b$
цикл пока $x \neq y$
    если $x > y$, **то**
        $x := x - y$
    иначе
        $y := y - x$
    конец если
конец цикла
$d := x$
конец

Данный алгоритм использует операции сравнения натуральных чисел, вычитания натуральных чисел и присваивания переменной значения натурального числа. Оценивая сложность предложенного алгоритма, можно рассматривать эти операции как элементарные. В теле цикла «пока» выполняется две операции сравнения, одна операция вычитания и одна операция присваивания. Цикл выполня-

ется не более $\max(a,b)$ раз. Таким образом, сложность алгоритма равна $O(\max(a,b))$.

Однако, более естественно рассматривать в качестве элементарных битовые операции.

5.22. Упражнение. Показать, что если $\max(a,b)=n$, то сложность вычисления НОД(a,b) по предложенному алгоритму равна $O(n\log_2 n)$ битовых операций.

А2. Алгоритм (Евклида).
Дано: $a,b\in\mathbb{N}$
Надо: $d\in\mathbb{N}$,
Переменные: $r,x,y\in\mathbb{Z}_+$

начало
$x:=a$
$y:=b$
цикл пока $y\neq 0$
$\quad r:=x \pmod y$
$\quad x:=y$
$\quad y:=r$
конец цикла
$d:=x$
конец

В алгоритме Евклида использовано стандартное обозначение $x \pmod y$ для остатка от деления x на y. Легко показать, что после двух делений делимое уменьшается, как минимум, в два раза. Значит, количество повторений цикла равно $O(\log_2 n)$, где $n{=}\max(a,b)$. Определяя битовую сложность алгоритма Евклида, мы должны учитывать, что сложность операции деления зависит от количества цифр квадратично. Таким образом, мы получаем оценку $O(\log_2^3 n)$ для битовой сложности алгоритма Евклида. Более тщательный анализ позволяет доказать оценку $O(\log_2^2 n)$.

Можно показать, что, в определенном смысле, наихудший вариант для алгоритма Евклида представляют последовательные числа Фиббоначчи.

5.23. Упражнение. Показать, что если $a=F_{n+1}$, $b=F_n$ — соответствующие числа Фиббоначчи, то остатки в алгоритме Евклида принимают последовательно значения $F_{n-1},\dots,F_2=1$.

5.24. Упражнение. Показать, что если $a>b$ и $r_1,\dots,r_n\neq 0$ — последовательные остатки, получаемые в алгоритме Евклида, то $a\geqslant F_{n+1}$, где F_k — k-ое число Фиббоначчи.

Легко видеть, что алгоритм Евклида применим в любом евклидовом кольце, т. е. условия $a, b \in \mathbb{N}$, $d \in \mathbb{N}$ и $r, x, y \in \mathbb{Z}_+$ можно заменить на $a, b, d, r, x, y \in R$, где R — любое евклидово кольцо.

5.25. Упражнение. Что произойдет, если в алгоритме Евклида a и b — отрицательные или нулевые целые числа?

Следующий алгоритм использует специфику машинной арифметики, основанной на системе счисления по основанию 2, в которой операции умножения и деления на 2 сводятся к сдвигу, следовательно, выполняются очень быстро.

А3. Алгоритм (бинарный НОД).
Дано: $a, b \in \mathbb{N}$
Надо: $d \in \mathbb{N}$,
Переменные: $x, y \in \mathbb{N}$

начало
$x := a$
$y := b$
$d := 1$
цикл пока $x \pmod 2 = y \pmod 2 = 0$
    $d := 2d, \qquad x := x/2, \qquad y := y/2$
конец цикла
цикл пока $x \neq y$
    выбор
        при $x \pmod 2 = 0$ **делать** $x := x/2$
        при $y \pmod 2 = 0$ **делать** $y := y/2$
        при $x > y$ **делать** $x := x - y$
        при $x < y$ **делать** $y := y - x$
    конец выбора
конец цикла
$d := d \cdot x$
конец

5.26. Замечание. В конструкции **выбор** выполняются только действия для первого истинного условия в операторах **при**. Таким образом, на первые два условия мы можем попасть, когда один из аргументов четный, а другой — нечетный. На последние два условия можно попасть, только когда оба аргумента нечетны. Учитывая, что при вычитании нечетного числа из нечетного получается четное, можно результат сразу разделить на 2, т. е. строки

при $x > y$ **делать** $x := x - y$
при $x < y$ **делать** $y := y - x$

заменить строками

при $x > y$ делать $x := (x - y)/2$
при $x < y$ делать $y := (y - x)/2$

Очевидно, что при каждом повторении тела цикла последнего алгоритма хотя бы один аргумент уменьшается в два раза. Значит, количество повторений цикла равно $O(\log_2 n)$, где $n = \max(a, b)$. Определяя битовую сложность бинарного алгоритма, мы должны учитывать, что сложность операций, выполняемых в теле цикла, зависит от количества цифр линейно, т. е. битовая сложность бинарного алгоритма равна $O(\log_2^2 n)$.

Приведем еще алгоритм вычисления НОД, основанный на свойстве факториальности кольца $\mathbb{Z}$.

А4. Алгоритм (НОД через примарное разложение).
Дано: $a, b \in \mathbb{N}$
Надо: $d \in \mathbb{N}$,
Переменные: $x, y, p \in \mathbb{N}$, p — простое число

начало
$x := a$
$y := b$
$p := 2$
$d := 1$
цикл пока $x \neq 1$ или $y \neq 1$
  цикл пока $x \pmod p = y \pmod p = 0$
    $d = d \cdot p$, $x = x/p$, $y = y/p$
  конец цикла
  цикл пока $x \pmod p = 0$
    $x = x/p$
  конец цикла
  цикл пока $y \pmod p = 0$
    $y = y/p$
  конец цикла
  $p :=$ следующее простое число
конец цикла
конец

5.4. Расширенные алгоритмы вычисления НОД(a,b) в $\mathbb{Z}$. Наибольший общий делитель двух целых чисел обладает следующим важным свойством: *если* $d = НОД(a, b)$, *то существуют целые числа* u *и* v, *такие, что* $d = u \cdot a + v \cdot b$.

5.27. Упражнение. Доказать это свойство, пользуясь тем, что $\mathbb{Z}$ — кольцо главных идеалов.

Для нахождения целых чисел u и v используется метод, называемый *расширенным алгоритмом Евклида*.

А5. Алгоритм (Евклида расширенный).
Дано: $a, b \in \mathbb{N}$
Надо: $d \in \mathbb{N}$, $u, v \in \mathbb{Z}$
Переменные: R, X, Y — векторы элементов типа $\mathbb{Z}$ с индексом 0..2
$q \in \mathbb{Z}_+$
Обозначения: $r == R[0]$, $x == X[0]$, $y == Y[0]$

начало
$X := (a, 1, 0)$
$Y := (b, 0, 1)$
цикл пока $y \neq 0$
$q := [x/y]$ // целая часть дроби $\frac{x}{y}$
$R := X - q \cdot Y$
$X := Y$
$Y := R$
конец цикла
$(d, u, v) := X$
конец

Три компонента вектора X связаны соотношением:

$$X[0] = X[1] \cdot a + X[2] \cdot b.$$

Такое же соотношение справедливо для Y и R.

Чтобы распространить этот алгоритм на отрицательные и нулевые целые числа, достаточно заменить первые две строки следующими:

если $a \geqslant 0$, **то** $X := (a, 1, 0)$ **иначе** $X := (-a, -1, 0)$
если $b \geqslant 0$, **то** $Y := (b, 0, 1)$ **иначе** $Y := (-b, 0, -1)$

5.28. Упражнение. Доказать, что битовая сложность расширенного алгоритма Евклида равна $O(\log_2^2 n)$, где $n = \max(|a|, |b|)$.

5.29. Упражнение. Сформулировать расширенную версию алгоритма **А**1 и оценить его сложность.

До недавнего времени считалось, что расширенной версии бинарного алгоритма не существует. С.А. Абрамов и С.И. Рыбин [**1**] построили ее, допустив в рассмотрение вектор $(0, b/2^k, -a/2^k)$, где 2^k — степень 2 в НОД, который можно прибавлять к другим векторам или вычитать из них.

5.30. Упражнение. Написать расширенный бинарный алгоритм.

5.5. Эффективность вычисления НОД(a,b) в $\mathbb{Z}$. Алгоритм Евклида и бинарный алгоритм вычисления НОД являются достаточно эффективными для большинства приложений. При проектировании высокопроизводительных систем используются различные методы повышения быстродействия алгоритма вычисления НОД, в частности, алгоритм Лемера [**9**].

6. Алгоритмы вычисления НОД(a,b) в кольцах многочленов $k[x]$ и $\mathbb{Z}[x]$

6.1. Последовательности полиномиальных остатков. Алгоритмы **A**2 и **A**5 дословно переносятся на любое евклидово кольцо, в частности, на кольцо многочленов $k[x]$ от одной переменной над произвольным полем k.

Последовательность остатков полиномов, полученная при выполнении алгоритма Евклида, называется *последовательностью полиномиальных остатков* (PRS).

Рассмотрим пример, сконцентрировав наше внимание на росте коэффициентов членов последовательности полиномиальных остатков.

6.1. Пример. Рассмотрим полиномы $p_1(x) = x^3 - 7x + 7$ и $p_2(x) = 3x^2 - 7$ как элементы евклидова кольца $\mathbb{Q}[x]$. Применяя алгоритм Евклида, получаем такие последовательности:

$$\begin{aligned} p_1(x) &= x^3 - 7x + 7, \\ p_2(x) &= 3x^2 - 7, & q_1(x) &= (1/3)x, \\ p_3(x) &= (-14/3)x + 7, & q_2(x) &= (-9/14)x - 27/28, \\ p_4(x) &= -1/4, & q_3(x) &= (56/3)x - 28, \\ p_5(x) &= 0. \end{aligned}$$

Поскольку $p_4(x) = -1/4$, получаем НОД$[p_1(x), p_2(x)] = 1$.

Рост коэффициентов последовательности полиномиальных остатков может быть минимизирован, если каждый член, как только он получен, нормируется. В этом случае мы получаем

$$\begin{aligned} p_1(x) &= x^3 - 7x + 7, \\ p_2(x) &= x^2 - 7/3, & q_1(x) &= x, \\ p_3(x) &= x - 3/2, & q_2(x) &= x + 3/2, \\ p_4(x) &= 1, & q_3(x) &= x - 3/2, \\ p_5(x) &= 0. \end{aligned}$$

Действительно, мы видим, что коэффициенты растут медленнее, но расплачиваемся за это вычислением НОД целых чисел на каждом шаге, чтобы максимально редуцировать дроби.

Из этого примера видно, что использовать арифметику рациональных чисел для вычисления последовательности полиномиальных остатков нецелесообразно; с одной стороны, число требуемых для максимального редуцирования коэффициентов вычислений НОД целых чисел слишком велико, и с другой стороны, отказ от редукции ведет в стремительному росту выражения.

Коэффициенты многочленов в приведенных выше примерах являются целыми числами, т. е. мы можем рассматривать эти многочлены как элементы кольца $\mathbb{Z}[x]$. Поскольку это кольцо факториально (с однозначным разложением на неприводимые множители), для любых двух элементов этого кольца, не равных одновременно нулю, определен их наибольший общий делитель. С другой стороны, из вложения $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ следует, что мы можем рассматривать наибольший общий делитель этих же многочленов в кольце $\mathbb{Q}[x]$. Как связаны между собой эти наибольшие общие делители? Одно отличие мы уже знаем: НОД в кольце $\mathbb{Z}[x]$ определен с точностью до знака, а в кольце $\mathbb{Q}[x]$ — с точностью до умножения на любое ненулевое рациональное число. Покажем, что, по существу, этим отличие и ограничивается.

6.2. Лемма (Гаусса). *Если коэффициенты многочлена $f \in \mathbb{Z}[x]$ взаимно просты в совокупности и $f = g \cdot h$, где $g, h \in \mathbb{Q}[x]$ и НОД числителей коэффициентов каждого из многочленов g и h равен 1, то $g, h \in \mathbb{Z}[x]$.*

Доказательство. Проведем доказательство методом «от противного». Пусть $g = \sum\limits_{i=0}^{n} a_i x^i \notin \mathbb{Z}[x]$ и p — простое число, которое делит знаменатель какого-либо коэффициента a_i. Выберем максимальную степень числа p, которая делит знаменатель какого-либо коэффициента a_i, обозначим ее k. Без потери общности можем обозначить i_0 такой индекс, что знаменатели коэффициентов a_i при $i > i_0$ не делятся на p^k, а знаменатель коэффициента a_{i_0} делится на p^k. Рассмотрим теперь многочлен $h(x) = \sum\limits_{j=0}^{m} b_j x^j$. Пусть l — минимальная степень p, на которую делится хотя бы один коэффициент b_j ($l < 0$, если p делит знаменатель какого-либо коэффициента). По условию, $l \leqslant 0$. Пусть j_0 — наибольшее значение индекса, на котором этот

минимум достигается. Вычислим коэффициент $c_{i_0+j_0}$ при $x^{i_0+j_0}$ в произведении gh. Имеем

$$c_{i_0+j_0} = a_{i_0}b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i\neq i_0}} a_i b_j.$$

Знаменатель первого слагаемого делится на p^{k-l}, знаменатель ни одного из коэффициентов под знаком суммы на это число не делится. Таким образом, знаменатель коэффициента $c_{i_0+j_0}$ делится на $p^{k-l} > 1$, что противоречит условию леммы. □

Пользуясь леммой Гаусса 6.2, мы можем разбить вычисление НОД$(f(x), g(x))$ в кольце $\mathbb{Z}[x]$ на следующие этапы:

(1) найти наибольший общий делитель $d_c \in \mathbb{Z}$ коэффициентов многочленов $f(x)$ и $g(x)$;
(2) найти $d_q(x) = \text{НОД}(f(x), g(x))$ в кольце $\mathbb{Q}[x]$, нормированный таким образом, что $d_q(x) \in \mathbb{Z}[x]$ и коэффициенты многочлена $d_q(x)$ взаимно просты;
(3) $\text{НОД}(f(x), g(x)) = d_c \cdot d_q(x)$ в кольце $\mathbb{Z}[x]$.

Введем следующие определения.

6.3. Определение. Наибольший общий делитель коэффициентов многочлена $f(x) \in \mathbb{Z}[x]$ называется *содержанием* этого многочлена и обозначается $\operatorname{cont}(f)$. Многочлен $f(x)/\operatorname{cont}(f)$ называется *примитивной частью* многочлена $f(x)$ и обозначается $\text{p. p.}(f(x))$.

Обратимся теперь к задаче нахождения наибольшего общего делителя двух полиномов $p_1(x), p_2(x)$ в кольце $\mathbb{Z}[x]$, при условии, что все арифметические операции над коэффициентами выполняются не в поле $\mathbb{Q}$, а в кольце $\mathbb{Z}$, являющимся не полем, а только областью с однозначным разложением на множители. Из приведенных выше рассуждений ясно, что мы можем вывести следующие важные соотношения:

$$\operatorname{cont}\{\text{НОД}[p_1(x), p_2(x)]\} = \text{НОД}\{\operatorname{cont}[p_1(x)], \operatorname{cont}[p_2(x)]\},$$
$$\text{p. p.}\{\text{НОД}[p_1(x), p_2(x)]\} = \text{НОД}\{\text{p. p.}[p_1(x)], \text{p. p.}[p_2(x)]\}.$$

Поэтому задача нахождения наибольшего общего делителя произвольных полиномов сводится к задаче нахождения наибольшего общего делителя примитивных полиномов.

Рассмотрим два примитивных ненулевых полинома $p_1(x)$ и $p_2(x)$ в $\mathbb{Z}[x]$, у которых $\deg[p_1(x)] = m$ и $\deg[p_2(x)] = n$, $m > n$. Поскольку алгоритм деления полиномов с остатком требует точной делимости

старшего коэффициента делимого на старший коэффициент делителя, обычно этот процесс невозможно выполнить для полиномов $p_1(x)$ и $p_2(x)$ над целыми числами, не ослабляя требования делимости. Поэтому мы вводим процесс *псевдоделения*, который всегда дает нам *псевдочастное* и *псевдоостаток* (prem), коэффициенты которых являются целыми числами.

Псевдоделение означает предварительное умножение полинома $p_1(x)$ на $\{\mathrm{lc}[p_2(x)]\}^{m-n+1}$, а затем применение алгоритма деления многочленов, когда известно, что все частные существуют, т. е.

$$\{\mathrm{lc}[p_2(x)]\}^{m-n+1}p_1(x) = p_2(x)q(x) + r(x), \quad \deg[r(x)] < \deg[p_2(x)],$$

где $q(x)$ и $r(x)$ — псевдочастное и псевдоостаток соответственно.

6.4. Пример. Пользуясь псевдоделением в $\mathbb{Z}[x]$, разделим $p_1(x) = x^4 - 7x + 7$ на $p_2(x) = 3x^2 - 7$. Для того, чтобы вычислить $q(x)$ и $r(x)$, предварительно умножим $p_1(x)$ на $3^{4-2+1} = 27$, а затем, применяя алгоритм деления многочленов, получаем $q(x) = 9x^2 + 21$ и $r(x) = -189x + 336$. Читатель может убедиться, что алгоритм деления многочленов не будет работать, если мы предварительно домножим $p_1(x)$ только на 3.

Поэтому, пытаясь вычислить наибольший общий делитель полиномов $p_1(x)$ и $p_2(x)$, мы должны убедиться, что выполнимы все деления полиномов, встречающиеся в этом процессе, т. е. мы должны, используя псевдоделения, сформировать последовательность полиномиальных остатков. Таким образом, мы приходим к следующему обобщенному алгоритму Евклида для полиномов.

A6. Алгоритм (GEA-P). Обобщенный алгоритм Евклида для многочленов над целыми числами **G**eneralized **E**uclidean **A**lgorithm for **P**olynomials over the Integers.

Дано: $p_1(x), p_2(x)$ — ненулевые полиномы в $\mathbb{Z}[x]$;
$\deg[p_1(x)] = n_1$, $\deg[p_2(x)] = n_2$, $n_1 \geqslant n_2$.

Надо: НОД$[p_1(x), p_2(x)]$, НОД многочленов $p_1(x)$ и $p_2(x)$.

начало

1 [Вычисление НОД содержаний]
$c :=$ НОД$\{\mathrm{cont}[p_1(x)], \mathrm{cont}[p_2(x)]\}$. (Здесь мы используем алгоритм Евклида для вычисления наибольшего общего делителя двух целых чисел.)

2 [Вычисление примитивных частей]
$p_1'(x) := p_1(x)/\mathrm{cont}[p_1(x)]$; $p_2'(x) := p_2(x)/\mathrm{cont}[p_2(x)]$.

3 [Построение PRS]
Вычислить $p_1'(x), p_2'(x), p_3(x), \ldots, p_h(x)$.

4 [Выход]
Если $\deg[p_h(x)] = 0$, то вернуть НОД$[p_1(x), p_2(x)] := c$, иначе вернуть НОД$[p_1(x), p_2(x)] := c \cdot \text{p. p.}[p_h(x)]$.

конец

Ясно, что время работы этого алгоритма зависит от того, насколько эффективно мы можем вычислять последовательность полиномиальных остатков $p'_1(x), p'_2(x), p_3(x), \ldots, p_h(x)$. Заметим, что если $n_i = \deg[p_i(x)]$, то в общем случае мы можем утверждать, что члены этой последовательности удовлетворяют соотношениям

$$\begin{gathered}\{\mathrm{lc}[p_{i+1}(x)]\}^{n_i - n_{i+1}+1} p_i(x) = p_{i+1}(x)q_i(x) + \beta_i p_{i+2}(x), \\ \deg[p_{i+2}(x)] < \deg[p_{i+1}(x)],\end{gathered} \tag{6.1}$$

где $i = 1, 2, \ldots, h-1$ для некоторого h. [Разумеется, $p_i(x) := p'_i(x)$, $i = 1, 2$, где $p'_i(x)$, $i = 1, 2$ определены на шаге 2 алгоритма **GEA-P**]. Если дан метод выбора коэффициентов β_i, то выписанное соотношение дает алгоритм построения PRS; очевидно, что условие завершения этого семейства алгоритмов — равенство нулю псевдоостатка.

Ниже мы рассматриваем различные алгоритмы, полученные для разных значений β_i.

6.2. Евклидов алгоритм PRS. Здесь $\beta_i = 1$ для всех $i = 1, 2, \ldots, h-1$, т. е. каждый псевдоостаток используется в том виде, в котором он получен. Это один из худших методов построения PRS, приводящий к экспоненциальному росту коэффициентов.

6.5. Пример. Рассмотрим полиномы $p_1(x) = x^3 - 7x + 7$, $p_2(x) = 3x^2 - 7$ в $\mathbb{Z}[x]$. Очевидно, что $\mathrm{cont}[p_1(x)] = \mathrm{cont}[p_2(x)] = 1$ и $p_i(x) = p'_i(x)$, $i = 1, 2$. Мы имеем такую последовательность:

$$\begin{aligned} p_1(x) &= x^3 - 7x + 7, \\ p_2(x) &= 3x^2 - 7, & q_1(x) &= 3x, \\ p_3(x) &= -42x + 63, & q_2(x) &= -126x - 189, \\ p_4(x) &= -441, & q_3(x) &= 18522x - 27783, \end{aligned}$$

полученную при выполнении следующих псевдоделений:

$$\begin{aligned} (3)^2 p_1(x) &= p_2(x) \cdot (3x) + (-42x + 63), \\ (-42)^2 p_2(x) &= p_3(x) \cdot (-126x - 189) + (-441), \\ (-441)^2 p_3(x) &= p_4(x) \cdot (18522x - 27783) + 0. \end{aligned}$$

Из шага 4 алгоритма **GEA-P** следует, что НОД$[p_1(x), p_2(x)] = 1$. Отметим также, что в последнем псевдоделении коэффициенты имеют 8 десятичных цифр, поскольку $(-441)^2 p_3(x) = -8168202x + 12252303$.

Последовательность полиномиальных остатков этого примера называется *полной*, потому что степень каждого ее члена на единицу меньше степени предыдущего; два первых члена могут, конечно, иметь одинаковые степени. В противном случае последовательность называется *неполной*. Заметим, что не существует способа сказать *a priori*, будет ли PRS полной или неполной.

Экспоненциальный рост коэффициентов членов PRS в приведенном примере обусловлен тем, что полиномы этой последовательности не являются примитивными, т. е. то, что мы не избавляемся от их содержания, дает вредный эффект. Эта ситуация исправляется ниже.

6.3. Алгоритм примитивных PRS. В этом случае

$$\beta_i = \operatorname{cont}\{\operatorname{prem}[p_i(x), p_{i+1}(x)]\}, \quad i = 1, 2, \ldots, h-1,$$

где «prem» обозначает псевдоостаток, т. е. теперь мы удаляем содержание $(i+2)$-го члена PRS до того, как мы используем его. [Напомним, что для данного $p(x)$ удобно определять $\mathrm{p.p.}[p(x)]$ так, чтобы старший коэффициент был положительным.]

6.6. Пример. Рассмотрим те же полиномы, что и в предыдущем примере: $p_1(x) = x^3 - 7x + 7$, $p_2(x) = 3x^2 - 7$ в $\mathbb{Z}[x]$, где снова $p_i(x) = p_i'(x)$, $i = 1, 2$. Теперь мы получаем

$$\begin{aligned}
&p_1(x) = x^3 - 7x + 7, && && \\
&p_2(x) = 3x^2 - 7, && q_1(x) = 3x, && \\
&p_3(x) = 2x - 3, && q_2(x) = 6x + 9, && \beta_1 = -21, \\
&p_4(x) = 1, && q_3(x) = 2x - 3, && \beta_2 = -1,
\end{aligned}$$

что достигается выполнением следующих псевдоделений:

$$\begin{aligned}
(3)^2 p_1(x) &= p_2(x) \cdot (3x) + (-21)(2x - 3), \\
(2)^2 p_2(x) &= p_3(x) \cdot (6x + 9) + (-1), \\
(1)^2 p_3(x) &= p_4(x) \cdot (2x - 3) + 0.
\end{aligned}$$

Этот алгоритм дает наилучшие возможные результаты в отношении роста коэффициентов, однако, они достигаются достаточно сложными вычислениями НОД коэффициентов на каждом этапе. В монографии [**7**, § 2.3.3] утверждается, что лучшим из известных методов вычисления НОД многочленов, основанных на применении к многочленам с целыми коэффициентами алгоритма Евклида, является метод, в котором множители β_i выбираются следующим образом.

Предположим, что даны два многочлена $p_1(x), p_2(x) \in \mathbb{Z}[x]$. Для вычисления их НОД построим последовательность полиномиальных

остатков $p_3(x), p_4(x), \ldots, p_s(x), 0$. Введем обозначение c_i для старшего коэффициента многочлена $p_i(x)$ и δ_i для разности степеней многочленов $p_i(x)$ и $p_{i+1}(x)$. Последовательность полиномиальных остатков строим по формуле (6.1), в которой полагаем

$$\begin{aligned} \beta_1 &= (-1)^{\delta_1+1} \\ \beta_i &= -c_i\psi_i^{\delta_i}, \quad i>1, \end{aligned} \tag{6.2}$$

где

$$\begin{aligned} \psi_1 &= -1 \\ \psi_i &= (-c_i)^{\delta_{i-1}} i \psi_{i-1}^{1-\delta_{i-1}}, \quad i>1. \end{aligned} \tag{6.3}$$

Теорема о субрезультантах (см., например, [**12**]) утверждает, что все p_i являются многочленами с целыми коэффициентами.

6.7. Пример. Анализ вычисления НОД следующих многочленов выполнен Брауном [**17**]. Этот пример разобран также в монографии [**7**, § 2.3.3].

$$\begin{aligned} p_1(x) &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, \\ p_2(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21. \end{aligned}$$

Рассматривая эти многочлены как элементы кольца $\mathbb{Q}[x]$ и применяя алгоритм Евклида, мы получаем следующую последовательность:

$$\begin{aligned} p_3 &= \frac{-5}{9}x^4 + \frac{1}{9}x^2 - \frac{1}{3}, \\ p_4 &= \frac{-117}{25}x^2 - 9x + \frac{441}{25}, \\ p_5 &= \frac{233150}{19773}x - \frac{102500}{6591}, \\ p_6 &= \frac{1288744821}{543589225}. \end{aligned}$$

Все выписанные дроби являются несократимыми.

Выписанная последовательность достаточно трудоемка для вычислений вручную. Рекомендуется воспользоваться системой компьютерной алгебры Maple. Данная последовательность полиномиальных остатков получается с помощью функции `rem`, вычисляющей остатки. По умолчанию система Maple не упорядочивает слагаемые в многочленах, для этой цели используется функция `sort`. Последовательность команд может выглядеть следующим образом:

```
p[1]:=x^8+x^6-3*x^4-3*x^3+8*x^2+2*x-5;
p[2]:=3*x^6+5*x^4-4*x^2-9*x+21;
```

```
p[3]:=sort(rem(p[1],p[2],x));
p[4]:=sort(rem(p[2],p[3],x));
p[5]:=sort(rem(p[3],p[4],x));
p[6]:=sort(rem(p[4],p[5],x));
```

Применение нормализации делителя позволяет уменьшить коэффициенты, но не слишком сильно.

Для данного примера евклидова последовательность полиномиальных остатков имеет вид

$$p_3 = -15x^4 + 3x^2 - 9,$$
$$p_4 = 15795x^2 + 30375x - 59535,$$
$$p_5 = 1254542875143750x - 1654608338437500,$$
$$p_6 = 12593338795500743100931151992187500.$$

Для вычисления этой последовательности с помощью системы Maple нужно в приведенной выше программе заменить функцию `rem` на `prem`.

Наконец, применяя формулы (6.2) и (6.3), мы получаем последовательность

$$p_3 = 15x^4 - 3x^2 + 9,$$
$$p_4 = 65x^2 + 125x - 245,$$
$$p_5 = 9326x - 12300,$$
$$p_6 = 260708,$$

которая возрастает значительно медленнее, чем предыдущие последовательности.

6.4. Модулярный алгоритм вычисления НОД многочленов. Пусть p — простое число. Любое целое число m можно рассматривать как представитель соответствующего класса вычетов по модулю p, т. е. числу m можно однозначно поставить в соответствие некоторый элемент из поля $\mathcal{F}_p = \mathbb{Z}/p\mathbb{Z}$. В частности, любому многочлену $f(x) \in \mathbb{Z}[x]$ можно однозначно поставить в соответствие многочлен $f_p(x) \in \mathcal{F}_p[x]$.

Вернемся к примеру 6.7. Многочлены

$$a(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5,$$
$$b(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21.$$

можно рассматривать как элементы кольца $\mathcal{F}_p[x]$ для любого простого p. Можно вычислить их наибольший общий делитель в $\mathcal{F}_p[x]$. При

этом у нас не возникнет проблем с ростом коэффициентов, поскольку мы можем пользоваться системой представителей из множества $\{0, 1, \ldots .p-1\}$. Полагая $p = 5$, мы без особого труда убеждаемся, что многочлены $a(x)$ и $b(x)$ взаимно просты в кольце $\mathcal{F}_p[x]$. Можно ли из этого сделать вывод, что многочлены $a(x)$ и $b(x)$ взаимно просты в кольце $\mathbb{Z}[x]$? Оказывается, можно. Доказательство этого факта основано на следующих утверждениях.

6.8. Предложение. *Описанное выше отображение $\mathbb{Z}[x] \to \mathcal{F}[x]$, такое, что $f(x) \mapsto f_p(x)$ является гомоморфизмом колец, т. е. сумма переходит в сумму, а произведение — в произведение. В частности, если $g(x) \mid f(x)$ в $\mathbb{Z}[x]$, то $g_p(x) \mid f_p(x)$ в $\mathcal{F}[x]$.*

6.9. Предложение. *Предположим, что $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены и простое число p не делит старшие коэффициенты многочленов $a(x)$ и $b(x)$. Если НОД$(a_p(x), b_p(x)) = 1$ в $\mathcal{F}_p[x]$, то НОД$(a(x), b(x)) = 1$ в $\mathbb{Z}[x]$.*

6.10. Упражнение. Показать, что оба условия в предложении 6.9 являются существенными, т. е. если многочлены $a(x), b(x) \in \mathbb{Z}[x]$ не являются примитивными или p делит их старшие коэффициенты, то из НОД$(a_p(x), b_p(x)) = 1$ в $\mathcal{F}_p[x]$ не следует, что НОД$(a(x), b(x)) = 1$ в $\mathbb{Z}[x]$.

6.11. Предложение. *Предположим, что $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены, такие, что НОД$(a(x), b(x))=1$ в $\mathbb{Z}[x]$. Тогда НОД$(a_p(x), b_p(x))=1$ в $\mathcal{F}_p[x]$ для почти всех простых чисел p.*

Доказательство. Без потери общности мы можем считать, что рассматриваются только простые числа, которые не делят ни старший коэффициент многочлена $a(x)$, ни старший коэффициент многочлена $b(x)$. Условие НОД$(a_p(x), b_p(x)) = 1$ означает, что результант $\mathrm{Res}_p(a_p, b_p)$ этих многочленов, рассматриваемых как элементы кольца $\mathcal{F}_p[x]$, не обращается в нуль. Чтобы вычислить $\mathrm{Res}_p(a_p, b_p)$, нам достаточно вычислить результант $\mathrm{Res}(a, b)$ многочленов $a(x), b(x)$ в кольце $\mathbb{Z}[x]$ и взять образ этого результанта по модулю p. Результант $\mathrm{Res}(a, b)$ является ненулевым целым числом (так как исходные многочлены по условию взаимно просты) и делится только на конечное число простых чисел. □

6.12. Определение. Пусть $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены, такие, что НОД$(a(x), b(x))=1$ в $\mathbb{Z}[x]$. Простое число p назовем *плохой редукцией*, если либо p делит старший коэффициент хотя бы одного из многочленов $a(x), b(x)$, либо НОД$(a_p(x), b_p(x)) \neq 1$.

6.13. Задача. *Для примитивных многочленов $a(x), b(x) \in \mathbb{Z}[x]$ найти ограничение сверху для числа плохих редукций (или ограничение сверху для их произведения).*

Для решения этой задачи могут пригодиться результаты, приведенные в параграфе 7.

Итак, мы можем сформулировать следующий алгоритм проверки взаимной простоты примитивных многочленов $a(x), b(x) \in \mathbb{Z}[x]$.

А7. Алгоритм (Проверки взаимной простоты многочленов).
Дано: $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены
Надо: являются ли $a(x)$ и $b(x)$ взаимно простыми

начало
Найти ограничение сверху для числа плохих редукций
цикл пока ограничение сверху не превышено
выбрать следующее простое p
если НОД$(a_p(x), b_p(x)) = 1$ **то вернуть**(взаимно просты)
конец если
конец цикла
вернуть(не взаимно просты)
конец

В действительности, модулярный метод может быть применен не только для проверки взаимной простоты многочленов, но и для нахождения их НОД.

Следующее предложение обобщает предложение 6.11.

6.14. Предложение. *Предположим, что $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены и $d(x) = НОД(a(x), b(x))$ в $\mathbb{Z}[x]$. Предположим, что p — простое число, которое не делит ни старший коэффициент многочлена $a(x)$, ни старший коэффициент многочлена $b(x)$. Пусть $\tilde{d}(x) = НОД(a_p(x), b_p(x))$ в $\mathcal{F}_p[x]$. Тогда $\deg \tilde{d}(x) \geqslant \deg d(x)$ и $\deg \tilde{d}(x) = \deg d(x)$ для почти всех p.*

Доказательство. Из предложения 6.8 следует, что $d_p(x)$ является общим делителем многочленов $a_p(x)$ и $b_p(x))$ в $\mathcal{F}_p[x]$, т. е. $d_p(x) \mid \tilde{d}(x)$. Следовательно, $\deg \tilde{d}(x) \geqslant \deg d(x)$. Применяя предложение 6.11 к многочленам $a(x)/d(x)$ и $b(x)/d(x)$, получим, что $\deg \tilde{d}(x) = \deg d(x)$ для почти всех p. □

Обобщим определение 6.12 следующим образом.

6.15. Определение. Пусть $a(x), b(x) \in \mathbb{Z}[x]$ — примитивные многочлены. Простое число p назовем *плохой редукцией*, если либо p

делит старший коэффициент хотя бы одного из многочленов $a(x)$, $b(x)$, либо $\deg \text{НОД}(a_p(x), b_p(x)) > \deg \text{НОД}(a(x), b(x))$.

Можно ли утверждать, что $\tilde{d}(x) = d_p(x)$? Для ответа на этот вопрос вспомним, что НОД определен с точностью до умножения на обратимые элементы кольца, т. е. $d(x) = \text{НОД}(a(x), b(x))$, следовательно, и $d_p(x)$ определены с точностью до умножения на ± 1, а $\tilde{d}(x)$ определен с точностью до умножения на ненулевые элементы поля $\mathcal{F}_p$. Таким образом, среди возможных значений $\tilde{d}(x)$ будут $d_p(x)$, но, в общем случае, ими значения $\tilde{d}(x)$ не исчерпываются.

Наша ближайшая цель — разработать алгоритм вычисления наибольшего общего делителя примитивных многочленов с целочисленными коэффициентами, основываясь на следующих соображениях. Выбираем несколько простых чисел p, которые должны быть достаточно маленькими (чтобы вычисления в полях вычетов выполнялись без применения длинной арифметики). Вычисляем наибольшие общие делители многочленов с коэффициентами из полей вычетов по модулю p. Отбрасываем плохие редукции. Применяя китайскую теорему об остатках к коэффициентам многочленов, находим требуемый НОД.

Что касается необходимого количества редукций (количества простых чисел, по модулю которых выполняются вычисления), то можно поступить одним из следующих способов:

(1) оценить заранее достаточное число редукций, пользуясь, например, оценками для коэффициентов делителей заданного многочлена, приведенными в параграфе 7;

(2) после каждой редукции пересчитывать коэффициенты искомого НОД, пользуясь КТО; если применение новой редукции не меняет этих коэффициентов, то проверить, делит ли полученный многочлен исходные. Если да, то задача решена, иначе выполнять следующие редукции.

Отметим, что в этой задаче, применяя КТО, мы должны находить числа с данными вычетами не из множества неотрицательных чисел $\{0, 1, \ldots, m-1\}$, а из симметричной системы $\{-(m-1)/2, \ldots$ $\ldots, -1, 0, 1, \ldots, (m-1)/2\}$ (при четном m, т. е. когда в качестве одного из модулей используется 2, система получается немного несимметричной: от $-k+1$ до k, где $k = m/2$).

Основная же проблема состоит в том, как согласовать вычисления для различных значений p. Здесь можно предложить два подхода.

Во-первых, можно свести задачу к случаю, когда искомый НОД является нормированным многочленом. Для этого заметим, что старший коэффициент искомого НОД делит старшие коэффициенты исходных многочленов, а значит, делит НОД старших коэффициентов этих многочленов. Обозначим этот НОД через c. Перейдем от переменной x к переменной $y = cx$. Для этого нам понадобится домножить исходные многочлены на некоторые степени числа c, чтобы после замены $cx = y$ получить многочлены $a'(y)$ и $b'(y)$ с целочисленными коэффициентами. После этого решаем задачу для многочленов $a'(y)$ и $b'(y)$, выполняя все вычисления в кольцах вычетов над нормированными многочленами. Получаем $d'(y) = \text{НОД}(a'(y), b'(y))$ в $\mathbb{Z}[y]$. К сожалению, $d'(cx)$, в общем случае, не является искомым наибольшим общим делителем, а отличается от него некоторым целочисленным множителем. Чтобы найти искомый НОД, достаточно вычислить примитивную часть многочлена $d'(cx)$.

Недостаток этого метода в том, что при достаточно высоких степенях исходных многочленов коэффициенты промежуточных многочленов (от y) становятся очень большими, что требует бóльшего количества чисел p, используемых для редукций, и более громоздких вычислений при применении КТО.

А8. Алгоритм (Модулярный НОД).
Дано: $a(x), b(x) \in \mathbb{Z}[x]$
Надо: $d(x) = \text{НОД}(a(x), b(x))$

начало
$c := \text{НОД}(\text{lc}(a(x)), \text{lc}(b(x)))$
выбрать нечетное простое p
$m := p$
$d_m(x) := c * \text{НОД}(a_p(x), b_p(x))$ (в симметричной системе вычетов по модулю m);
цикл пока $p.p.(d_m(x))$ не делит $a(x)$ и $b(x)$ в $\mathbb{Z}[x]$
    выбрать следующее простое p
    $d_p(x) := \text{НОД}(a_p(x), b_p(x))$
    если $\deg d_p(x) < \deg d_m(x)$ **то**
        $m := p$
        $d_m(x) := c * d_p(x)$ (в симметричной системе вычетов по модулю m);
    иначе если $\deg d_p(x) = \deg d_m(x)$ **то**
        Применить КТО к $(m, p, d_m(x), c * d_p(x))$
    конец если
конец цикла
вернуть$(d_m(x))$

Предписание «Применить КТО к $(m, p, d_m(x), c*d_p(x))$» означает следующее. На входе: p — простое число, m — натуральное число, не делящееся на p, коэффициенты многочленов $d_m(x) = \sum\limits_{i=0}^{n} a_i x^i$ и $c * d_p(x) = \sum\limits_{i=0}^{n} b_i x^i$ рассматриваются как представители смежных классов по модулю m и p соответственно. Вычисляются числа a'_i, такие что $a'_i \equiv a_i \pmod m$ и $a'_i \equiv b_i \pmod p$, $-mp/2 < a'_i \leqslant mp/2$, $i = 0, 1, \ldots, n$. На выходе $m := m * p$ и $d_m(x) = \sum\limits_{i=0}^{n} a'_i x^i$.

6.16. Задача. *Доказать корректность представленного алгоритма.*

6.17. Пример. Пользуясь модулярным алгоритмом, вычислим НОД многочленов $f(x) = 28x^3 + 216x^2 - 193x - 51$ и $g(x) = 8x^3 + +78x^2 + 33x - 442$.

Наибольший общий делитель старших коэффициентов равен 4. Вычисляя НОД$(f(x), g(x)) \pmod 3$, получим $d_3(x) = x + 1$. Домножая $d_3(x)$ на 4 и переходя к симметричной системе вычетов, снова получим $x+1$. Легко проверить, что полученный многочлен не делит ни один из исходных многочленов.

В качестве следующего простого числа берем $p = 5$. Вычисляя НОД$(f(x), g(x)) \pmod 5$, получим $d_5(x) = x^2 + 3x + 2$. Поскольку $\deg(d_5) > \deg(d_3)$, заключаем, что $p=5$ является «плохой редукцией».

Переходим к $p = 7$. Получаем $d_7(x) = $НОД$(f(x), g(x)) \pmod 7 = =x+5$. Домножая на 4, получим $4x + 20 \equiv 4x + 6 \pmod 7$. Пользуясь китайской теоремой об остатках, решаем систему сравнений $\begin{cases} a \equiv 1 \pmod 3, \\ a \equiv 6 \pmod 7. \end{cases}$ Получаем $a \equiv 13 \pmod{21}$. Переходя к симметричной системе вычетов, получаем $d_{21}(x) = 4x - 8$. Убеждаемся, что $d_{21}(x)$ не делит исходные многочлены в $\mathbb{Q}[x]$.

Берем $p = 11$. Получаем $d_{11}(x) =$ НОД$(f(x), g(x)) \pmod{11} = = x + 3$. Домножая на 4, получим $4x + 12 \equiv 4x + 1 \pmod 7$. Пользуясь китайской теоремой об остатках, решаем систему сравнений $\begin{cases} a \equiv 13 \pmod{21}, \\ a \equiv 1 \pmod{11}. \end{cases}$ Получаем $a \equiv 34 \pmod{231}$. Переход к симметричной системе вычетов ничего не меняет, и в итоге мы получаем $d_{231}(x) = 4x + 34$. Убеждаемся, что $d_{231}(x)$ делит исходные многочлены в $\mathbb{Q}[x]$ и $p.p.(d_{231}(x)) = 2x + 17$ является наибольшим общим делителем исходных многочленов.

7. Границы для коэффициентов делителя полинома

Вычисляя евклидову последовательность полиномиальных остатков, мы видели, что коэффициенты промежуточных многочленов могут расти достаточно быстро. При этом коэффициенты наибольшего общего делителя, как правило, оказываются небольшими. В этом параграфе мы постараемся найти оценки для коэффициентов многочленов, делящих заданный многочлен с целыми коэффициентами. Первая гипотеза, приходящая на ум, состоит в том, что если $f(x), g(x) \in \mathbb{Z}[x]$ и $g(x) | f(x)$, то коэффициенты делителя не превосходят по абсолютной величине коэффициентов делимого. К сожалению, это предположение неверно, как показывает следующий пример.

7.1. Пример. Рассмотрим многочлены

$$f(x) = x^3 + x^2 - x - 1 = (x+1)^2(x-1),$$
$$g(x) = x^4 + x^3 - x - 1 = (x+1)^2(x^2 - x + 1).$$

Легко видеть, что НОД$(f(x), g(x)) = x^2 + 2x + 1 = (x+1)^2$.

Этот пример легко обобщается, например, путем умножения обоих исходных многочленов на $(x+1)^2$.

7.1. Неравенство Коши. Оценку для коэффициентов делителей полинома будем выводить из известного неравенства Коши, которое дает оценку абсолютной величины корня полинома.

7.2. Теорема. *Пусть $d \geqslant 1$,*

$$P(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d, \qquad a_0 \neq 0 \tag{7.1}$$

— полином с комплексными коэффициентами. Тогда любой корень z полинома $P(x)$ удовлетворяет неравенству

$$|z| < 1 + \frac{\max\{|a_1|, \ldots, |a_d|\}}{|a_0|}. \tag{7.2}$$

Доказательство. Пусть $P(z) = 0$. Если $|z| \leqslant 1$, то утверждение теоремы тривиально. Предположим, что $|z| > 1$ и положим $H = \max(|a_1|, \ldots, |a_d|)$. По предположению

$$a_0 z^d = -a_1 z^{d-1} - \cdots - a_d,$$

следовательно,

$$|a_0|\,|z|^d \leqslant H\left(|z|^{d-1} + \cdots + 1\right) < \frac{H\,|z|^d}{|z| - 1},$$

то есть $|a_0|(|z| - 1) < H$. □

Разумеется, эта оценка не является единственно возможной. Ниже приведены еще две оценки, первая из которых также принадлежит Коши, а вторая — Кнуту:

$$|z| \leqslant \max\left(\left|\frac{da_1}{a_0}\right|, \left|\frac{da_2}{a_0}\right|^{1/2}, \left|\frac{da_3}{a_0}\right|^{1/3}, \ldots, \left|\frac{da_d}{a_0}\right|^{1/d}\right),$$

$$|z| \leqslant 2\max\left(\left|\frac{a_1}{a_0}\right|, \left|\frac{a_2}{a_0}\right|^{1/2}, \left|\frac{a_3}{a_0}\right|^{1/3}, \ldots, \left|\frac{a_d}{a_0}\right|^{1/d}\right).$$

Каждая из этих оценок дает также границу и для минимального модуля корня полинома (в предположении, что свободный член полинома ненулевой) — заменяем в исходном полиноме x на $1/x$, другими словами, ищем наибольший корень полинома $a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$, обратный к которому будет наименьшим корнем исходного полинома.

Воспользуемся неравенством Коши для получения оценки коэффициентов делителя полинома, которая известна как неравенство Ландау.

7.2. Неравенство Ландау. Пусть $F = \sum_{k=0}^{m} c_k x^k$. Положим

$$\|F\| = \left(\sum_{k=0}^{m} |c_k|^2\right)^{1/2}. \tag{7.3}$$

Рассматриваем формулу (7.3) как некоторое удобное обозначение. Можно доказать, что эта формула задает на пространстве полиномов метрику, но мы не пользуемся этим фактом, необходимые нам свойства этой метрики будут доказаны.

7.3. Теорема. *Предположим, что полином $P(x)$ задан формулой* (7.1). *Пусть $z_1, \ldots, z_d$ — корни полинома $P(x)$. Положим*

$$M(P) = |a_0| \prod_{j=1}^{d} \max\{1, |z_j|\}.$$

Тогда $M(P) \leqslant \|P\|$.

Для доказательства теоремы нам понадобится

7.4. Лемма. *Если Q — полином и z — комплексное число, то*

$$\|(x+z)Q(x)\| = \|(\bar{z}x+1)Q(x)\|. \tag{7.4}$$

Доказательство. Пусть $Q(x)=\sum_{k=0}^{m} c_k x^k$. Тогда квадрат выражения в левой части равенства (7.4) равен

$$\sum_{k=0}^{m+1}(c_{k-1}+zc_k)(\bar{c}_{k-1}+\bar{z}\bar{c}_k)=(1+|z|^2)\|Q\|^2+\sum_{k=0}^{m+1}(zc_k\bar{c}_{k-1}+\bar{z}\bar{c}_k c_{k-1})$$

(полагаем $c_{-1}=c_{m+1}=0$). Этому же выражению равен и квадрат правой части. □

Доказательство теоремы. Пусть $z_1,\dots,z_k$ — корни полинома $P(x)$, лежащие вне единичного круга. Тогда $M(P)=|a_0|\cdot|z_1\cdot\dots\cdot z_k|$. Положим

$$R(x)=a_0\prod_{j=1}^{k}(\bar{z}_j x-1)\prod_{j=k+1}^{d}(x-z_j)=b_0x^d+\dots+b_d.$$

k-кратное применение леммы дает $\|P\|=\|R\|$. Однако $\|R\|^2\geqslant\|b_0\|^2=$ $=[M(P)]^2$. □

7.5. Теорема. *Пусть $Q=b_0x^q+b_1x^{q-1}+\dots+b_q$, $b_0\neq 0$ — делитель полинома $P(x)$, задаваемого формулой (7.1). Тогда*

$$|b_0|+|b_1|+\dots+|b_q|\leqslant\left|\frac{b_0}{a_0}\right|\cdot 2^q\|P\|.$$

Доказательство. Легко проверяется, что

$$|b_0|+|b_1|+\dots+|b_q|\leqslant 2^qM(Q),$$

но $M(Q)\leqslant|b_0/a_0|M(P)$, и из неравенства Ландау следует, что $M(P)\leqslant\|P\|$. □

7.6. Упражнение. Пусть $f(x)\in\mathbb{Z}[x]$ и $h(x)$ — делитель полинома $f(x)$. Предположим, что $\deg(h)\leqslant m$. Тогда

$$\|h\|\leqslant\binom{2m}{m}^{1/2}\|f\|.$$

(Символ $\binom{n}{k}$ используется здесь и неоднократно в дальнейшем для обозначения биномиальных коэффициентов, т. е. числа сочетаний из n по k.)

Другие полезные границы можно найти, например, в работе [**25**].

Глава 3

Базисы Грёбнера

8. Определение базисов Грёбнера

Следующей рассматриваемой задачей будет задача выбора канонического представления для элементов кольца регулярных на некотором алгебраическом многообразии функций. Это кольцо представляет собой факторкольцо кольца многочленов $R = K[x_1, \ldots, x_n]$, где K — поле, по некоторому идеалу I. Предполагаем, что идеал I задан конечной системой образующих: $I = (f_1, \ldots, f_m)$. Теорема Гильберта о базисе утверждает, что таким образом может быть задан любой идеал кольца многочленов R. Любой элемент факторкольца R/I — это смежный класс элементов кольца R относительно идеала I. При фиксированном каноническом представлении элементов кольца R, задача о представлении элементов факторкольца R/I сводится к задаче выбора канонического представителя в смежном классе. Будем пытаться решить ее в следующей формулировке: в кольце многочленов $R = K[x_1, \ldots, x_n]$ дано конечное множество элементов $\{f_1, \ldots, f_m\}$. Требуется построить алгоритм, который для любого многочлена $g \in R$ выбирал бы канонического представителя в соответствующем смежном классе по идеалу I.

Кольцо многочленов R можно рассматривать как бесконечномерное векторное пространство над полем K, базис которого образует счетное множество мономов $T = \{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid i_1 \geqslant 0, \ldots, i_n \geqslant 0\}$. Идеал I, а, следовательно, и факторкольцо R/I, также являются векторными K-пространствами. Наша задача состоит в построении отображения $i\colon R/I \to R$, правого обратного к каноническому гомоморфизму $j\colon R \to R/I$, т. е. $ji(x) = x$ для любого $x \in R/I$, Таким образом, мы получаем разложение R в прямую сумму векторных пространств I и $i(R/I)$. Задачу выбора канонического представления решает тогда отображение $ij\colon R \to R$, получающееся проектированием прямой суммы векторных пространств на одно из слагаемых. Достаточно выбрать новый базис кольца R, рассматриваемого как векторное K-пространство, пересечение которого с идеалом I представляет базис векторного пространства I.

8.1. Пример. Пусть идеал I является мономиальным, т. е. порожден мономами $f_1, \ldots, f_m$. Тогда $T \cap I$ является базисом векторного пространства I, а $T \setminus (T \cap I)$ — базисом факторкольца R/I, рассматриваемого как векторное пространство. Каноническое представление получается, если в разложении любого многочлена по базису T отбрасывать элементы, принадлежащие I.

Хотя только что рассмотренный пример носит частный характер, он указывает на общий подход к решению поставленной задачи: выбрать такой базис векторного пространства R, пересечение которого с идеалом I представляет собой базис векторного пространства I.

8.2. Предложение. *Пусть M — векторное пространство (возможно, бесконечномерное) и $M' \subseteq M$ — его подпространство. Предположим, что базис Γ векторного пространства M выбран таким образом, что $\Gamma' = \Gamma \cap M'$ представляет собой базис пространства M'. Тогда каноническое представление факторпространства M/M' в M получается, если базис пространства M/M' отождествить с $\Gamma'' = \Gamma \setminus \Gamma'$.*

Доказательство получается немедленно из разложения векторного пространства M в прямую сумму векторных пространств с базисами Γ' и Γ'', которые изоморфны пространствам M' и M'' соответственно. □

Пусть идеал I порожден многочленами $f_1, \ldots, f_n$. Обозначим $F = \{f_1, \ldots, f_n\}$. Тогда счетное множество многочленов $T \times F = \{\theta \cdot f_i \mid \theta \in T,\ f_i \in F\}$ порождает векторное пространство I, однако эти многочлены не являются линейно независимыми. Наша ближайшая задача состоит в построении достаточно простого алгоритма выбора в множестве $T \times F$ линейно независимого подмножества. Для этого построим отображение $\varphi : T \times F \to T$, такое, что прообразы различных элементов из T линейно независимы, и выберем в прообразе каждого элемента единственного представителя (если этот прообраз не пуст). Получим систему Σ линейно независимых векторов в идеале I, которая, однако, может не порождать идеал I как векторное пространство.

Следующими задачами являются: проверка, порождает ли получившееся линейно независимое множество векторное пространство I, и если ответ отрицательный, то пополнение его до базиса.

Предположим, что множество T упорядочено таким образом, что:

а) $1 < \theta$ для любого монома $\theta \neq 1$;

б) если $\theta_1 < \theta_2$, то $\theta_1 t < \theta_2 t$ для любого монома t.

Как уже сказано в параграфе 3.1, наиболее часто используются следующие три отношения порядка:

- лексикографическое упорядочение мономов, получающееся из фиксированного порядка на множестве переменных;
- упорядочение мономов по степеням, а мономы одной и той же степени упорядочиваются лексикографически;
- упорядочение мономов по степеням, а мономы одной и той же степени упорядочиваются в обратном лексикографическом порядке.

Отображение φ ставит в соответствие любому многочлену f его старший моном (присутствующий в f с ненулевым коэффициентом).

8.3. Упражнение. Показать, что многочлены с различными старшими мономами линейно независимы.

8.4. Упражнение. Показать, что свойство системы Σ порождать или не порождать векторное пространство I не зависит от выбора представителей в прообразах элементов из T.

8.5. Упражнение. Показать, что система Σ порождает векторное пространство I тогда и только тогда, когда полугруппа, порожденная в T старшими мономами элементов множества F, совпадает с полугруппой старших мономов элементов идеала I.

8.6. Упражнение. Показать, что система Σ порождает векторное пространство I тогда и только тогда, когда идеал, порожденный старшими мономами элементов множества F, совпадает с ассоциированным градуированным идеалом идеала I (относительно фильтрации с одномерными факторами, определяемой введенным отношением порядка).

Рассматриваемая ситуация укладывается в следующую более общую схему: имеется градуированное некоторым вполне упорядоченным множеством векторное пространство $\operatorname{gr} M$ с одномерными однородными компонентами. Фиксирован базис Γ этих компонентов. На пространстве M рассматривается фильтрация, совместная с градуировкой. Выбирается множество Γ' элементов фильтрованного пространства M, такое, что при переходе к градуированному пространству $\operatorname{gr} M$ различные элементы множества Γ' переходят в различные элементы множества Γ. Тогда множество $\Gamma' \cup (\Gamma \operatorname{gr} \Gamma')$ является базисом пространства M и определяет разложение пространства M

в прямую сумму подпространств M' и M'', где M' — пространство с базисом Γ', а пространство M'' изоморфно факторпространству M/M' и, следовательно, определяет каноническое представление пространства M/M' в M.

В случае кольца многочленов градуировка осуществляется полугруппой $\mathbb{N}_0^n$, где $\mathbb{N}_0$ — множество неотрицательных целых чисел. В дальнейшем мы будем рассматривать также градуировку множеством $\mathbb{N}_0^n \times (\mathbb{Z}/k\mathbb{Z})$, где к свободной коммутативной полугруппе добавляется конечная. Такое множество соответствует, например, свободному конечнопорожденному модулю над кольцом многочленов (не обязательно коммутативных). Конечная компонента соответствует образующим свободного модуля. Примеры упорядочений рассматривались в пункте 3.1.

Вернемся к рассмотрению полиномиальных идеалов. Как уже отмечалось, в качестве базиса Γ выбирается множество мономов T. Утверждение о том, что R является градуированным векторным пространством с базисом T, означает, что любой многочлен можно записать в виде $f = a_0 m_0 + \sum\limits_j a_j m_j$, $j \geqslant 1$, где $m_0 > m_j$ для всех $j \geqslant 1$. Переход от фильтрации к градуировке означает выделение старшего одночлена: $\mathrm{gr}(f) = a_0 m_0$.

В частности, такое представление имеет место для всех образующих f_i идеала I, причем мы можем выбрать эти образующие так, чтобы старшие коэффициенты у них были равны 1, так как мы предполагаем, что K — поле:

$$f_i = m_{i0} + \sum_j a_{ij} m_{ij}, \qquad i = 1..m. \tag{8.1}$$

В качестве Γ' можно выбрать любое подмножество $\Sigma \subset T \times F$, где $F = \{f_1, \ldots, f_m\}$ — произвольная система образующих идеала I, руководствуясь двумя требованиями: во-первых, различные элементы множества Σ должны иметь разные старшие мономы; во-вторых, система Σ должна быть максимальна в том смысле, что для любого элемента $\xi \in T \times F$ существует элемент $\sigma \in \Sigma$ с таким же старшим мономом. Например, можно включить в Σ множество $T \cdot f_1$, далее добавить к нему те элементы множества $T \cdot f_2$, старшие мономы которых отличаются от старших мономов всех элементов, уже включенных в множество Σ и т. д.

8.7. Определение. Систему образующих F идеала I назовем *базисом Грёбнера* этого идеала, если подмножество Σ, введенное выше, образует базис векторного пространства I.

Из сформулированных выше упражнений следует корректность определения базиса Грёбнера, т. е. независимость его от конкретного выбора множества Σ.

8.8. Пример. Пусть I — главный идеал, порожденный многочленом f. Тогда f является базисом Грёбнера идеала I.

8.9. Пример. Многочлены $f_1 = x^2 - 1$ и $f_2 = x^3 - 1$ не составляют базис Грёбнера порождаемого ими идеала в кольце $\mathbb{Q}[x]$. Доказать.

В следующих примерах рассматривается кольцо многочленов $K[x_1, \ldots, x_n]$, которое содержит идеал I, заданный множеством образующих $F = \{f_1, \ldots, f_m\}$. Предполагается, что одночлены в записи элементов f_i упорядочены в соответствии с одним из введенных выше отношений порядка и нормированы таким образом, что их старшие коэффициенты равны 1.

8.10. Пример. Если $I = K[x_1, \ldots, x_n]$, то F является базисом Грёбнера идеала I тогда и только тогда, когда $1 \in F$.

8.11. Пример. Если поле K алгебраически замкнуто и I — максимальный идеал, то $F \subset I$ является базисом Грёбнера идеала I тогда и только тогда, когда для любой переменной x_i найдется элемент $f(i) \in F$ со старшим мономом x_i.

8.12. Пример. Если поле K не является алгебраически замкнутым, то утверждение предыдущего примера неверно.

Следует заметить, что введенное выше определение базиса Грёбнера не является конструктивным: не указано алгоритма для проверки, что некоторая система многочленов представляет базис Грёбнера порождаемого ими идеала, и тем более не дан алгоритм, позволяющий для идеала, заданного некоторой системой образующих, построить его базис Грёбнера.

В следующем параграфе определение базиса Грёбнера будет дано в более общей ситуации, а также будут приведены алгоритмы проверки, является ли данная система образующих идеала его базисом Грёбнера, и, в случае отрицательного ответа, — алгоритм, позволяющий пополнить эту систему до базиса Грёбнера.

9. Базисы Грёбнера в полиномиальных, дифференциальных и разностных модулях

Пусть $X = \{x_1, \ldots, x_m\}$ — конечная система элементов. Через $T = T(X)$ обозначим свободную коммутативную полугруппу с единицей (записываемую мультипликативно), порожденную элемента-

ми множества X. Элементы этой группы будем называть *мономами*. Пусть $\theta \in T$, $\theta = x_1^{e_1} \dots x_m^{e_m}$. *Порядком* монома θ будем называть сумму $e_1 + \dots + e_m$ и обозначать ее будем $\operatorname{ord}\theta$. Предположим, что мономы линейно упорядочены так, что для любого элемента $\theta \in T$ выполняются следующие условия:

$$1 \leqslant \theta. \tag{9.1}$$

Если $\theta_1 < \theta_2$, то

$$\theta\theta_1 < \theta\theta_2. \tag{9.2}$$

Тогда будем говорить, что на множестве мономов T задан *ранжир*. Следующие примеры показывают, что для одного и того же конечного множества X существуют различные ранжиры.

9.1. Пример (лексикографическое упорядочение мономов). Пусть

$$\theta_1 = x_1^{e_1} \dots x_m^{e_m}, \quad \theta_2 = x_1^{i_1} \dots x_m^{i_m}.$$

Тогда $\theta_1 < \theta_2$, если либо $e_1 < i_1$, либо $e_j = i_j$ для $j = 1, \dots, k$ и $e_{k+1} < i_{k+1}$ для некоторого k $(1 < k < m)$.

9.2. Пример (стандартный ранжир). Предположим, что

$$\theta_1 = x_1^{e_1} \dots x_m^{e_m} < \theta_2 = x_1^{i_1} \dots x_m^{i_m},$$

если либо $\operatorname{ord}\theta_1 < \operatorname{ord}\theta_2$, либо $\operatorname{ord}\theta_1 = \operatorname{ord}\theta_2$ и $\theta_1 < \theta_2$ относительно лексикографического упорядочения.

9.3. Пример (упорядочение по полной степени, затем обратное лексикографическое). Пусть $\theta_1 = x_1^{e_1} \dots x_m^{e_m}$, $\theta_2 = x_1^{i_1} \dots x_m^{i_m}$. Положим $\theta_1 < \theta_2$, если либо $e_1 + e_2 + \dots + e_m < i_1 + i_2 + \dots + i_m$, либо $e_1 + e_2 + \dots + e_m = i_1 + i_2 + \dots + i_m$ и существует k, $0 < k < m$, такое, что $e_j = i_j$ для $j = 1, \dots, k-1$ и $e_k > i_k$.

Пусть K — поле и P — векторное K-пространство с базисом $T = T(X)$. Определим на P функцию "`выделение лидера`" следующим образом: каждый элемент g из P может быть представлен в виде суммы $g = \sum\limits_{\theta \in T} a_\theta \theta$, где лишь конечное число коэффициентов $a_\theta \in K$ отлично от нуля (такое представление определено однозначно с точностью до порядка слагаемых). Среди всех мономов, входящих в это разложение с ненулевым коэффициентом, выберем максимальный относительно порядка, введенного на множестве мономов T. Этот моном будем называть *лидером* элемента $g \in P$ и обозначать через $\mathbf{u}_g$. Корректность такого определения следует из однозначности разложения элемента векторного пространства по базису и из линейной упорядоченности множества T.

9.4. Определение. Пусть задан ранжир на множестве мономов $T = T(X)$ и P — векторное K-пространство с базисом T. Предположим далее, что P является K-алгеброй, и $\mathbf{u}_{AB} = \mathbf{u}_A\mathbf{u}_B$ для всех $A, B \in P$. Кроме того, предположим, что $1\theta_1 \cdot 1\theta_2 = 1\theta_1\theta_2 \in P$ для любых $\theta_1, \theta_2 \in T$; в частности, образующие $x_1, \ldots, x_m$ коммутируют между собой. Такое кольцо будем называть *кольцом обобщенных многочленов от переменных* $X = \{x_1, \ldots, x_m\}$.

9.5. Пример (кольцо коммутативных многочленов над полем). Рассмотрим любой ранжир на множестве $X = \{x_1, \ldots, x_m\}$. В качестве P возьмем алгебру многочленов $K[x_1, \ldots, x_m]$ от коммутирующих переменных $x_1, \ldots, x_m$ над полем K. Нетрудно увидеть, что условие $\mathbf{u}_{AB} = \mathbf{u}_A\mathbf{u}_B$ будет выполнено для всех $A, B \in P$, а, следовательно, мы можем рассматривать $K[x_1, \ldots, x_m]$ как кольцо обобщенных многочленов от переменных $x_1, \ldots, x_m$.

9.6. Пример (кольцо дифференциальных операторов над полем). Пусть K — дифференциальное поле с базисным множеством $\Delta = \{d_1, \ldots, d_m\}$ попарно коммутирующих между собой дифференцирований. Ранжир на множестве T так же, как и в примере 9.5, может быть любым. Тогда кольцо $D = K[d_1, \ldots, d_m]$ линейных дифференциальных операторов над K (см. определение 3.4) будет являться кольцом обобщенных многочленов от неизвестных $d_1, \ldots, d_m$.

9.7. Пример (кольцо дифференциальных операторов над кольцом многочленов). Пусть K — дифференциальное поле с базисным множеством дифференцирований $\Delta = \{d_1, \ldots, d_m\}$, и пусть R — кольцо коммутативных многочленов от переменных $y_1, \ldots, y_n$ над полем K. Определим дифференцирования $\Delta' = \{d'_1, \ldots, d'_m\}$ кольца R следующим образом: если $1 \leqslant i \leqslant m$, то $d'_i(y_j) = 0$ для всех $j = 1, \ldots, n$. Выберем теперь для каждого $i \in \mathbb{N}_m$ число $j \in \mathbb{N}_n$ и положим $d'_i(k) = d_i(k)y_j$ для всех $j = 1, \ldots, n$ и $k \in K$. Тогда кольцо D_R линейных Δ'-операторов над кольцом R будет являться кольцом обобщенных многочленов от переменных $X = \{d'_1, \ldots, d'_m, y_1, \ldots, y_n\}$. Действительно, если мы рассмотрим такой ранжир, что $d'_i > y_j$ для всех $i = 1, \ldots, m$, $j = 1, \ldots, n$, то, как легко доказать, условие $\mathbf{u}_f\mathbf{u}_g = \mathbf{u}_{fg}$ будет выполнено.

9.8. Пример (кольцо разностных операторов над полем). Пусть K — разностное поле с базисным множеством попарно коммутирующих автоморфизмов $\{\alpha_1, \ldots, \alpha_m\}$. Тогда кольцо $R = K[\alpha_1, \ldots, \alpha_m]$ линейных разностных операторов (см. определение 3.9) будет являться кольцом обобщенных многочленов от переменных $\alpha_1, \ldots, \alpha_m$. В качестве ранжира можно выбрать любое упорядочение, удовлетворяющее условиям (9.1)–(9.2).

9.9. Пример (кольцо дифференциально-разностных операторов над полем). Обобщением примеров 9.6 и 9.8 является случай кольца $R = K[d_1, \dots, d_m, \alpha_1, \dots, \alpha_q]$, когда часть переменных соответствует дифференцированиям, а другая часть — автоморфизмам.

Пусть теперь D — кольцо обобщенных многочленов от переменных $X = \{x_1, \dots, x_m\}$ над полем K, и F — свободный D-модуль с базисом $\mathcal{B} = \{b_1, \dots, b_n\}$. Как векторное пространство над K модуль F имеет в качестве базиса прямое произведение $T \times \mathcal{B}$ множеств $T = T(X)$ и $\mathcal{B}$. Это множество мы будем называть множеством *термов* модуля F,

$$T_F = \{x_1^{i_1} \dots x_m^{i_m} b_j \mid (i_1, \dots, i_m) \in \mathbb{N}_0^m,\ j = 1, \dots, n\}.$$

Термы перемножать нельзя, однако определено произведение терма на моном из соответствующего кольца многочленов. В дальнейшем мы будем обычно отождествлять терм $x_1^{i_1} \dots x_m^{i_m} b_j$ с вектором $(j, i_1, \dots, i_m) \in \mathbb{N}_0^{m+1}$.

9.10. Определение. *Ранжиром* на множестве термов T_F будем называть отношение полного порядка на T_F, удовлетворяющее следующим условиям:

(1) $\varphi \leqslant \theta\varphi$ для любого терма $\varphi \in T_F$ и любого монома $\theta \in T$;
(2) если $\varphi_1 \leqslant \varphi_2$, где $\varphi_1, \varphi_2 \in T_F$, то $\theta\varphi_1 \leqslant \theta\varphi_2$ для всех $\theta \in T$.

9.11. Определение. Ранжир назовем *правильным*, если из условия $\operatorname{ord}\theta_1 < \operatorname{ord}\theta_2$ $(\theta_1, \theta_2 \in T)$ следует $\theta_1 b_i < \theta_2 b_j$ для всех $1 \leqslant i, j \leqslant n$.

9.12. Пример. Пусть задан ранжир на множестве мономов T. Будем сравнивать термы вида (θ, i) по их последней координате i и только в случае равенства ее для двух термов переходить к сравнению мономов. Полученный таким образом ранжир на T_F не является правильным.

9.13. Пример. Пусть $\varphi_1, \varphi_2 \in T_F$. Будем считать, что $\varphi_1 = (j_1, \theta_1) < \varphi_2 = (j_2, \theta_2)$ тогда и только тогда, когда

- либо $\operatorname{ord}\theta_1 < \operatorname{ord}\theta_2$;
- либо $\operatorname{ord}\theta_1 = \operatorname{ord}\theta_2$ и $j_1 < j_2$;
- либо $\operatorname{ord}\theta_1 = \operatorname{ord}\theta_2$, $j_1 = j_2$ и $\theta_1 < \theta_2$ относительно лексикографического порядка при фиксированной нумерации переменных.

Этот ранжир является правильным. Мы будем называть его *стандартным*.

Отметим, что по определению ранжира множество термов T_F вполне упорядочено относительно каждого ранжира.

9.14. Определение. Пусть задан ранжир на множестве термов T_F, и пусть $\varphi_1, \varphi_2 \in T_F$. Будем говорить, что терм φ_1 *ниже* (*выше*) рангом, чем φ_2, если $\varphi_1 < \varphi_2$ ($\varphi_1 > \varphi_2$).

Кроме отношения порядка $<$ на T_F, определим отношение частичного порядка $\ll$ следующим образом:

$$\varphi_1 \ll \varphi_2 \iff \exists \theta \in T \mid \theta\varphi_1 = \varphi_2. \tag{9.3}$$

В этом случае будем говорить, что терм φ_1 *делит* φ_2. Из (1) следует, что отношение $<$ совместно с $\ll$, т. е.

$$\varphi_1 \ll \varphi_2 \implies \varphi_1 \leqslant \varphi_2. \tag{9.4}$$

9.15. Определение. Любой элемент $f \in F \setminus \{0\}$ допускает единственное представление в виде конечной суммы:

$$f = \sum_{i=1}^{r} c(f, \varphi_i)\varphi_i, \quad 0 \neq c(f, \varphi_i) \in K,\ \varphi_i \in T_F, \qquad \varphi_r < \varphi_{r-1} < \cdots < \varphi_1. \tag{9.5}$$

Определим *лидер* элемента f как $\mathbf{u}_f = \varphi_1$ и старший коэффициент как $\operatorname{Hcoeff}(f) = c(f, \varphi_1)$. Определим $\mathbf{u}_0 = 0$, $\operatorname{Hcoeff}(0) = 0$. Аналогично, $\mathbf{u}_B = \{\mathbf{u}_f \mid f \in B\}$ для любого конечного множества $B \subseteq F$, $\mathbf{u}_M$ для любого подмодуля $M \subseteq F$ обозначает подмодуль, порожденный множеством $\{\mathbf{u}_f \mid f \in M\}$.

Пусть F — свободный D-модуль и $f, g \in F$. Будем говорить, что элемент f *ниже рангом*, чем g, и писать $\operatorname{rk} f < \operatorname{rk} g$, если $\mathbf{u}_f < \mathbf{u}_g$. Будем говорить, что элемент f *выше рангом*, чем g, и писать $\operatorname{rk} f > \operatorname{rk} g$, если $\mathbf{u}_f > \mathbf{u}_g$. Если $\mathbf{u}_f = \mathbf{u}_g$, то будем говорить, что элементы f и g *имеют одинаковый ранг*. Ясно, что различные элементы могут иметь одинаковый ранг.

9.16. Определение. Пусть $B \subset F \setminus \{0\}$ — конечное множество образующих некоторого D-модуля $M \subseteq F$ (без потери общности можно предположить, что $\operatorname{Hcoeff}(g) = 1$ для любого $g \in B$). Определим *процесс редукции* следующим образом: $f \underset{B}{\to} f'$, если $f, f' \in F$ и существуют терм $t \in T_F$, $\zeta \in T(X)$ и $g \in B$, такие, что $c = c(f, t) \neq 0$, $t = \zeta\mathbf{u}_g$, $f' = f - c\zeta g$.

9.17. Лемма. *Пусть* $f, f' \in F$ *и* $f \underset{B}{\to} f'$. *Тогда* $\operatorname{rk} f \geqslant \operatorname{rk} f'$.

Доказательство. Утверждение леммы следует из того, что отношение $>$ является линейным порядком на множестве термов T_F и свойства (2). □

В дальнейшем будем опускать указание на множество B, если это не приведет к двусмысленности или если выбор множества B несуществен. Символ $\xrightarrow[B]{+}$ обозначает транзитивное, а $\xrightarrow[B]{*}$ — рефлексивно-транзитивное замыкание отношения $\underset{B}{\to}$. Элемент f называется *нередуцируемым*, если не существует элемента $f' \neq f$, такого, что $f \underset{B}{\to} f'$, в противном случае f называется *редуцируемым*.

9.18. Примеры.

(1) Пусть $m = 0$, т. е. F — векторное пространство над полем K. Рассмотрим стандартный ранжир на T_F. Если $\boldsymbol{v}$ — вектор, у которого первая ненулевая координата стоит на i-м месте, то редукция вектора $\boldsymbol{w}$ относительно $\boldsymbol{v}$ приводит к обнулению i-й координаты вектора $\boldsymbol{w}$ путем вычитания соответствующего кратного вектора $\boldsymbol{v}$.

(2) Пусть K — поле, $n = 1$ и $m = 1$, т. е. F — кольцо многочленов от одной переменной. Рассмотрим стандартный ранжир на T_F. Пусть $B = \{x^3 - 1; x^2 - 1\}$. Тогда $x^4 \underset{B}{\to} x$ и $x^4 \underset{B}{\to} x^2 \underset{B}{\to} 1$.

9.19. Определение. Пусть на свободном D-модуле F дано отношение редукции $\underset{B}{\to}$ и вычислимая функция $\mathrm{Sel} : F \to F$ такая, что $f \underset{B}{\to} \mathrm{Sel}(f)$ для любого редуцируемого элемента $f \in F$. Рассмотрим вычислимую функцию S, определяемую рекурсивно формулой

$$S(f) := \begin{cases} f, & \text{если } f \text{ нередуцируем;} \\ S(\mathrm{Sel}(f)), & \text{если } f \text{ редуцируем.} \end{cases}$$

Функцию S такого вида назовем *нормальной редукцией* или *алгоритмом нормальной формы* для $\xrightarrow[B]{*}$. Например, редуцируемые термы выбираются в порядке убывания относительно полного упорядочения термов, а при фиксированном терме соотношения выбираются в том порядке, как они располагаются в множестве B.

9.20. Определение. *Частичную редукцию* определим как нормальную редукцию, осуществляемую только до тех пор, пока редуцируется лидер.

9.21. Лемма. *Если $f \xrightarrow[B]{*} f'$, то элементы f и f' принадлежат одному и тому же смежному классу модуля F/M, где M — подмодуль, порожденный множеством B.*

Доказательство. $g \in B$, следовательно, $c\zeta g \in M$. □

9.22. Лемма. *Пусть F — свободный D-модуль и B — конечное подмножество модуля F. Тогда отношение редукции $\underset{B}{\to}$ является нетеровым, т. е. не существует бесконечных цепочек вида $f \underset{B}{\to} f_1 \underset{B}{\to} \dots \underset{B}{\to} f_k \dots$. Следовательно, для любого элемента f существует (не обязательно единственный) нередуцируемый элемент f', такой, что $f \overset{*}{\underset{B}{\to}} f'$.*

Доказательство. Предположим противное. Всякий ранжир, по определению, вполне упорядочивает множество термов T_F. Поэтому мы можем выбрать среди всех бесконечных цепочек редукций цепочку, начинающуюся с элемента g с минимальным относительно ранжира лидером t. Возможны две ситуации: либо на некотором шаге редукции терм t редуцируется и оставшаяся часть цепочки начинается с элемента, все слагаемые которого меньше, чем t; либо t не редуцируется ни на каком шаге редукции. В обоих случаях получается противоречие с минимальностью выбранной цепочки: в первом случае можно выбрать хвост исходной цепочки, остающийся после редуцирования t; во втором — вычесть из всех элементов цепочки терм t. □

9.23. Предложение. *Множество нередуцируемых относительно отношения $\underset{B}{\to}$ элементов является векторным K-пространством.*

Доказательство. Нужно проверить, что если f и g — нередуцируемые элементы и $c \in K$, то элементы $f+g$ и cf также нередуцируемы. Это немедленно следует из того, что в $f+g$ и cf присутствуют с ненулевыми коэффициентами только те слагаемые, которые присутствуют в f и g. □

9.24. Лемма. *Если множество G порождает подмодуль $M \subset F$ и $f - f' \in M$, то существует целое $s \geqslant 0$ и элементы $f = f_0, f_1, \dots \dots, f_s = f'$, такие, что для всех i от 1 до s либо $f_{i-1} \to f_i$, либо $f_i \to f_{i-1}$.*

Доказательство. Поскольку G порождает модуль M, элемент $f - f'$ можно представить в виде суммы

$$\sum_{i=1}^{r} c_i \cdot \eta_i \cdot g_i,$$

где c_i — коэффициенты, $\eta_i \in T(X)$, $g_i \in G$ (могут совпадать при различных значениях i). Доказательство леммы будем вести индук-

цией по минимальной длине r такого представления. Если $r = 0$, то $f = f'$, и утверждение леммы выполнено. Для произвольного r мы можем предполагать, что $\varphi = \mathbf{u}_{\eta_r \cdot g_r} \geqslant \mathbf{u}_{\eta_i \cdot g_i}$ для всех i. Положим $f_1 = f - c(f,\varphi)\cdot\eta_r\cdot g_r$, $f_2 = f_1 - (c_r - c(f,\varphi))\cdot\eta_r\cdot g_r$. Тогда $f \to f_1 \leftarrow f_2$ и $f_2 - f' = f - f' - c_r\cdot\eta_r\cdot g_r = \sum\limits_{i=1}^{r-1} c_i\cdot\eta_i\cdot g_i$, так что можно применить предположение индукции. □

9.25. Определение. На прямом произведении $F \times F$ определим функцию S, такую, что $S(f,f') = 0$, если $f = 0$, или $f' = 0$, или $\mathrm{НОК}(\mathbf{u}_f, \mathbf{u}_{f'})$ не определен; в остальных случаях

$$S(f,f') = \mathrm{Hcoeff}(f')\varphi f - \mathrm{Hcoeff}(f)\zeta f',$$

где $\varphi, \zeta \in T(X)$ и $\varphi\mathbf{u}_f = \mathrm{НОК}(\mathbf{u}_f, \mathbf{u}_{f'}) = \zeta\mathbf{u}_{f'}$.

9.26. Определение. Пусть D — кольцо обобщенных многочленов от переменных $X = \{x_1, \ldots, x_m\}$ над полем K, F — свободный D-модуль. Предположим, что $M \subseteq F$ — подмодуль свободного модуля F, $G \subset M$ — конечное множество и $<$ — ранжир на множестве термов T_F. Множество G называется *базисом Грёбнера* (G-*базисом*) подмодуля M, если для любого ненулевого элемента $f \in M$ имеется *представление Грёбнера* (G-*представление*):

$$f = \sum_{i=1}^{r} c_i\theta_i g_i, \quad 0 \neq c_i \in K,\ \theta_i \in T(X),\ g_i \in G, \tag{9.6}$$

$$\theta_i\mathbf{u}_{g_i} > \theta_{i+1}\mathbf{u}_{g_{i+1}},$$

откуда, в частности, следует, что

$$\mathbf{u}_f = \theta_1\mathbf{u}_{g_1}.$$

Недостатком введенного определения является то, что для одного и того же элемента могут существовать различные G-представления. Например, если $g_1 = t^2 - 1$, $g_2 = t^3 - 1$, то $(t^2-1)(t^3-1) = t^3\cdot g_1 - g_1 = t^2\cdot g_2 - g_2$ — два различных G-представления одного и того же многочлена. С другой стороны, достаточно сложно проверить, что некоторый элемент не допускает G-представления. От этих недостатков можно избавиться, если потребовать, чтобы любой одночлен мог появляться в G-представлении в качестве лидера слагаемого $\theta_i g_i$ не более чем для одного элемента $g_i \in G$. В частности, можно предполагать, что элементы множества G упорядочены, и при выборе линейно независимых элементов вида $\theta_i g_i$ мы руководствуемся правилами, сформулированными в определении

нормальной редукции 9.19. Представление такого вида мы будем называть *нормальным G-представлением*.

Для формулировки основного результата настоящего параграфа введем некоторые обозначения и докажем две леммы.

9.27. Определение. Для элементов $f, f' \in F$ будем писать $f \nabla f'$, если существует элемент $f'' \in F$, такой, что $f \xrightarrow{*} f''$ и $f' \xrightarrow{*} f''$.

9.28. Лемма. *Пусть $f, f', f'' \in F$ и $f \xrightarrow{*} f'$. Тогда $f + f'' \nabla f' + f''$.*

Доказательство. Пусть $f = f' + c \cdot \eta \cdot g$, где $\mathbf{u}_{\eta \cdot g} = \varphi$ и $c = c(f, \varphi) \neq 0$, $c(f', \varphi) = 0$. Если $c'' = c(f'', \varphi)$, то $f'' = c'' \cdot \eta \cdot g + h$, где $c(h, \varphi) = 0$, тогда

$$f + f'' = f' + c \cdot \eta \cdot g + c'' \cdot \eta \cdot g + h = f' + h + (c + c'') \cdot \eta \cdot g \xrightarrow{*} f' + h$$

и

$$f' + f'' = f' + h + c'' \cdot \eta \cdot g \xrightarrow{*} f' + h.$$

□

9.29. Определение. Будем говорить, что отношение редукции $\to$ удовлетворяет *условию слияния*, если для любого элемента f из условий $f \xrightarrow{*} f'$ и $f \xrightarrow{*} f''$ следует, что $f' \nabla f''$.

9.30. Определение. Будем говорить, что отношение редукции $\to$ удовлетворяет *локальному условию слияния*, если для любого элемента f из $f \to f'$ и $f \to f''$ следует, что $f' \nabla f''$.

9.31. Определение. Будем говорить, что отношение редукции $\to$ удовлетворяет *псевдолокальному условию слияния*, если для всех $f, f', f'' \in F$, таких, что $f \to f'$ и $f \to f''$, существует целое $s \geqslant 0$ и элементы $f' = f_0, f_1, \ldots, f_s = f''$, такие, что $f \xrightarrow{*} f_i$ и $f_{i-1} \nabla f_i$ для всех $i = 1, \ldots, s$.

9.32. Лемма. *Если нетерово отношение $\to$ удовлетворяет псевдолокальному условию слияния, то отношение $\to$ удовлетворяет условию слияния.*

Доказательство. Применим "нётерову" индукцию, т. е. покажем, что если утверждение леммы верно для всех g таких, что $f \to g$, то оно верно и для f. Такой индукции достаточно для доказательства леммы, поскольку в противном случае некоторый элемент f, для которого утверждение леммы не выполняется, мог бы быть выбран в качестве первого элемента бесконечной цепочки

$f \to f_1 \to \cdots \to f_n \to \ldots$, для всех элементов которой утверждение леммы также не выполняется.

Итак, фиксируем f и предположим, что для всех элементов $f^{\#}$ таких, что $f \xrightarrow{+} f^{\#}$, утверждение леммы выполняется. Покажем, что оно выполняется и для f. Без потери общности мы можем предполагать, что данные элементы f' и f'' отличны от f, т. е. имеют место редукции $f \to g_1 \xrightarrow{*} f'$ и $f \to g_2 \xrightarrow{*} f''$. Элементы g_1 и g_2 удовлетворяют псевдолокальному условию слияния при некотором s.

Доказательство будем вести индукцией по s. Основание индукции по s предполагает $s = 1$, т. е. g_1 и g_2 удовлетворяют локальному условию слияния. Из условия локального слияния следует, что существует g_3, такой, что $g_2 \xrightarrow{*} g_3$ и $g_1 \xrightarrow{*} g_3$. По предположению внешней индукции для элементов f' и g_3 существует элемент g_4, такой, что $f' \xrightarrow{*} g_4$ и $g_3 \xrightarrow{*} g_4$, а также элемент g_5, такой, что $f'' \xrightarrow{*} g_5$ и $g_4 \xrightarrow{*} g_5$. Этот элемент удовлетворяет условию леммы (см. рис. 1).

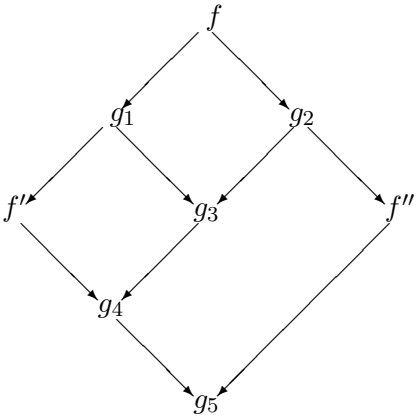


Рис. 1

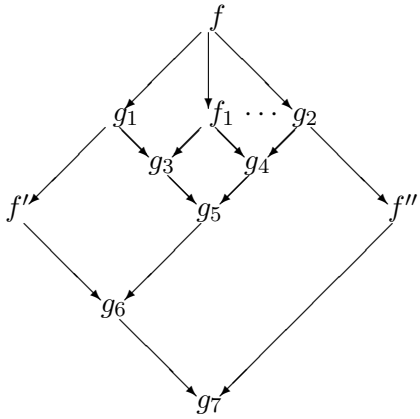


Рис. 2

Переход от s к $s+1$ иллюстрируется следующей диаграммой (рис. 2). Пусть g_1 и g_2 удовлетворяют псевдолокальному условию слияния с цепочкой из $s+2$ элементов: $g_1{=}f_0, f_1, \ldots, f_s, f_{s+1}{=}g_2$. По предположению индукции элементы f_1 и g_2 удовлетворяют условию слияния (элемент g_4). Существование элементов g_5, g_6 и g_7 в приведенной диаграмме следует из предположения о том, что элементы, которые получены редукцией элементов, следующих за f, в частности, g_1, f_1, g_2, удовлетворяют условию слияния. □

Следующая теорема перечисляет ряд условий, которые равносильны определению базиса Грёбнера. Следует отметить, что среди

них содержатся условия (6′) и (7′), позволяющие за конечное число шагов проверить, является ли выписанная система образующих подмодуля M его базисом Грёбнера.

9.33. Теорема. *Пусть F — свободный D-модуль, $M \subseteq F$ — его D-подмодуль, $G \subset M$ — конечное множество, $<$ — ранжир на множестве термов T_F. Предположим, что множество G нормализовано таким образом, что* $\mathrm{Hcoeff}(g_i) = 1$ *для всех $g_i \in G$. Тогда эквивалентны следующие условия:*

(1) *G является G-базисом модуля M;*

(1′) *любой элемент модуля M допускает нормальное G-представление;*

(2) *$\mathbf{u}_G$ порождает $\mathbf{u}_M$;*

(3) *для любого $f \in M$ имеет место $f \xrightarrow[G]{*} 0$;*

(3′) *для любого $f \in M$ имеет место $f \xRightarrow[G]{*} 0$;*

(4) *если $f - f' \in M$ и f, f' нередуцируемы, то $f = f'$;*

(5) *если $f \in M$ и f нередуцируем, то $f = 0$.*

Следующие условия являются необходимыми для выполнения предыдущих, и, если множество G порождает M, то они являются и достаточными:

(6) *если $f, f' \in G$ и $S(f, f') \neq 0$, то $S(f, f')$ допускает G-представление;*

(6′) *если $f, f' \in G$ и $S(f, f') \neq 0$, то $S(f, f')$ допускает нормальное G-представление;*

(7) *если $f, f' \in G$ и $НОК(\mathbf{u}_f, \mathbf{u}_{f'})$ определен, то в G существуют элементы $f = f_0, \ldots, f_i, \ldots, f_s = f'$, такие, что*

$$НОК\{\mathbf{u}_{f_i} : i = 0, \ldots, s\} = НОК(\mathbf{u}_f, \mathbf{u}_{f'}) \qquad (9.7)$$

и каждый S-элемент $S(f_{i-1}, f_i)$, $i = 1, \ldots, s$, допускает G-представление;

(7′) *если $f, f' \in G$ и $НОК(\mathbf{u}_f, \mathbf{u}_{f'})$ определен, то в G существуют элементы $f = f_1, \ldots, f_i, \ldots, f_s = f'$, удовлетворяющие условию* (9.7)*, такие, что каждый S-элемент $S(f_{i-1}, f_i)$, $i = 1, \ldots, s$, допускает нормальное G-представление;*

(8) *если $f \xrightarrow[G]{*} f'$, $f \xrightarrow[G]{*} f''$ и f' и f'' нередуцируемы, то $f' = f''$;*

(9) *если $f \xrightarrow[G]{*} f'$, $f \xrightarrow[G]{*} f''$, то существует элемент $h \in F$, такой, что $f' \xrightarrow[G]{*} h$, $f'' \xrightarrow[G]{*} h$, т. е. $\xrightarrow[G]{*}$ удовлетворяет условию слияния;*

(10) $S(f,f') \xrightarrow[G]{*} 0$ *для любых* $f, f' \in G$;

(10′) $S(f,f') \xRightarrow[G]{*} 0$ *для любых* $f, f' \in G$;

(11) *если* $f, f' \in G$ *и* НОК$(\mathbf{u}_f, \mathbf{u}_{f'})$ *определен, то в* G *существуют элементы* $f = f_0, \ldots, f_i, \ldots, f_r = f'$, *удовлетворяющие условию* (9.7) *и такие, что* $S(f_{i-1}, f_i) \xrightarrow[G]{*} 0$ *для всех* $i = 1, \ldots, r$;

(11′) *если* $f, f' \in G$ *и* НОК$(\mathbf{u}_f, \mathbf{u}_{f'})$ *определен, то в* G *существуют элементы* $f = f_0, \ldots, f_i, \ldots, f_r = f'$, *удовлетворяющие условию* (9.7) *и такие, что* $S(f_{i-1}, f_i) \xRightarrow[G]{*} 0$ *для всех* $i = 1, \ldots, r$.

Доказательство. Докажем следующие импликации:

$(3) \to (10) \to (11)$

$(3') \to (10') \to (11') \to (11)$

$(3) \to (4) \to (5) \to (3') \to (3)$

$(3) \to (2) \to (1') \to (1) \to (6) \to (7) \to (11) \to (9) \to (3)$

$(1') \to (6') \to (7') \to (7)$

$(4) \to (8) \to (9)$

$(3) \to (10)$. Тривиально, поскольку $S(f,f') \in M$.

$(3') \to (10')$. Аналогично.

$(10) \to (11)$. Достаточно положить $r = 1$.

$(10') \to (11')$. Аналогично.

$(11') \to (11)$. Тривиально.

$(3) \to (4)$. По предложению 9.23 множество нередуцируемых элементов является векторным пространством, значит, если f и f' нередуцируемы, то и их разность нередуцируема. Поскольку $f - f' \in M$, из 3 и предыдущего замечания следует, что $f - f' = 0$, т. е. (4).

$(4) \to (5)$. Полагаем $f' = 0$.

$(5) \to (3')$. Достаточно применить леммы 9.21 и 9.22.

$(3') \to (3)$. Очевидно.

$(3) \to (2)$. Пусть $u \in M$ и $\mathbf{u}_u \notin (\mathbf{u}_G)$. Тогда элемент u не может редуцироваться к 0, что противоречит (3).

$(2) \to (1')$. Пусть существуют $0 \neq u \in M$, для которых нет нормального G-представления. Среди таких элементов выберем элемент с минимальным $\mathbf{u}_u$. По условию (2) можно применить шаг редукции, сокращающий $\mathbf{u}_u$. Полученное противоречие с минимальностью $\mathbf{u}_u$ доказывает (1′)).

$(1') \to (1)$. Очевидно.

$(1) \to (6)$. Достаточно заметить, что если $f \in G$, $f' \in G$, то $S(f, f') \in M$.

$(1') \to (6')$. Аналогично.

$(6) \to (7)$. Очевидно.

$(6') \to (7')$. Также очевидно.

$(7') \to (7)$. Очевидно.

$(7) \to (11)$. Пусть $1 \leqslant i \leqslant r$, $u = S(f_{i-1}, f_i)$ и $u = \sum\limits_{j=1}^{r} c_j \theta_j g_j$, $0 \neq c_j \in K$, $\theta_j \in T(X)$, $g_j \in G$, $\theta_i \mathbf{u}_{g_i} > \theta_{i+1} \mathbf{u}_{g_{i+1}}$ — G-представление элемента u. Положим $u_k = \sum\limits_{j=k}^{r} c_j \theta_j g_j$. Тогда

$$u = u_1 \underset{G}{\longrightarrow} u_2 \underset{G}{\longrightarrow} \ldots \underset{G}{\longrightarrow} u_r \underset{G}{\longrightarrow} 0.$$

$(11) \to (9)$. Ввиду леммы 9.32, достаточно доказать, что отношение редукции удовлетворяет псевдолокальному условию слияния. Пусть $f \to f'$, $f \to f''$. Это означает существование элементов $g', g'' \in G$, $\eta', \eta'' \in T(X)$, $\varphi' = \eta' \mathbf{u}_{g'}$, $\varphi'' = \eta'' \mathbf{u}_{g''}$, таких, что $f' = f - c' \eta' g'$, $f'' = f - c'' \eta'' g''$, где $c' = c(f, \varphi') \neq 0$, $c'' = c(f, \varphi'') \neq 0$, но $c(f', \varphi') = c(f'', \varphi'') = 0$. Можно предполагать, что $\varphi'' \leqslant \varphi'$. Обозначим $R(\xi) = \xi - \operatorname{Hcoeff}(\xi) \mathbf{u}_\xi$ для любого $\xi \in F$.

Выделим в f слагаемое $c'\varphi'$, т. е. $f = f_1 + c'\varphi' + f_2$, где f_1 состоит из слагаемых, которые больше, чем $c'\varphi'$, а f_2 — из слагаемых, меньших $c'\varphi'$. Нужно рассмотреть два случая: $\varphi'' < \varphi'$ и $\varphi'' = \varphi'$. В первом из них, полагая $f_2'' = f_2 - c'' \eta'' g''$ и $f_0 = f_1 - c' \eta' R(g') + f_2''$, по лемме 9.28 получаем $f' = (f_1 - c' \eta' R(g')) + f_2 \nabla (f_1 - c' \eta' R(g')) + f_2'' = f_0$, откуда $f' \nabla f''$.

В случае, когда $\varphi' = \varphi''$, одновременно выполняются условия $\mathbf{u}_{g'} \ll \varphi'$ и $\mathbf{u}_{g''} \ll \varphi''$. Поэтому определен $\operatorname{НОК}(\mathbf{u}_{g'}, \mathbf{u}_{g''})$. По условию 11 доказываемой теоремы в G существует последовательность $g' = g_0, \ldots, g_i, \ldots, g_t = g''$, удовлетворяющая условию (9.7) и такая, что $S(g_{i-1}, g_i) \xrightarrow{*} 0$ для любого i. Значит, $\mathbf{u}_{g_i} \ll \varphi'$ для любого i, поэтому существуют $\eta_i \in T$, такие, что $\eta_i \mathbf{u}_{g_i} = \varphi'$, $c'\varphi' \to -c' \eta_i R(g_i)$ и $f \to f_1 - c' \eta_i R(g_i) + f_2 = h_i$, $i = 1, \ldots, t$. Покажем, что $h_{i-1} \nabla h_i$. Это следует из того, что

$$h_i - h_{i-1} = c' \eta_{i-1} R(g_{i-1}) - c' \eta_i R(g_i) = c' \theta S(g_i, g_{i-1}) \xrightarrow{*} 0,$$

где $\theta \in T(X)$ и удовлетворяет условию $\theta \cdot \operatorname{НОК}(\mathbf{u}_{g_i}, \mathbf{u}_{g_{i-1}}) = \varphi'$. Следовательно, отношение $\to$ удовлетворяет псевдолокальному условию слияния.

(9) $\to$ (3). Если множество G порождает M, то по лемме 9.24 существуют элементы $f = f_0, \ldots, f_i, \ldots, f_s = 0$, такие, что для любого i либо $f_{i-1} \to f_i$, либо $f_i \to f_{i-1}$. Пусть k обозначает наибольший индекс, для которого не выполняется условие $f_i \xrightarrow{*} 0$. Тогда $f_{k+1} \xrightarrow{*} 0$ и $f_{k+1} \to f_k$. По условию 9 $0 \nabla f_k$, и получаем противоречие с выбором k, поскольку 0 редуцируется только в самого себя.

(4) $\to$ (8). $f' - f'' = (f' - f) - (f'' - f) \in M$, следовательно, $f' = f''$.

(8) $\to$ (9). Пусть $f \xrightarrow{*} f'$ и $f \xrightarrow{*} f''$. Выберем нередуцируемые f_1' и f_1'' такие, что $f' \xrightarrow{*} f_1'$, $f'' \xrightarrow{*} f_1''$. Из (8) следует, что $f_1' = f_1''$, т. е. отношение $\to$ удовлетворяет условию слияния. $\square$

Поскольку вопрос о G-представимости элемента может быть решен алгоритмически, пункт (6′) дает нам возможность сформулировать алгоритм проверки, является ли данная система образующих подмодуля его базисом Грёбнера. Пункт (7′) этой же теоремы позволяет нам оптимизировать полученный алгоритм, проверяя G-представимость не всего множества S-элементов, а только некоторого его подмножества.

9.34. Упражнение. Показать, что многочлены

$$f_1 = x^3yz - xz^2,$$
$$f_2 = xy^2z - xyz,$$
$$f_3 = x^2y^2 - z^2$$

не составляют базис Грёбнера порождаемого ими идеала (упорядочение по степени, затем обратное лексикографическое, $x > y > z$).

9.35. Упражнение. Показать, что многочлены

$$f_1 = x^3yz - xz^2, \qquad f_6 = yz^3 - z^3,$$
$$f_2 = xy^2z - xyz, \qquad f_7 = xyz^2 - xz^2,$$
$$f_3 = x^2y^2 - z^2, \qquad f_8 = z^4 - x^2z^2,$$
$$f_4 = x^2yz - z^3, \qquad f_9 = x^3z^2 - xz^2$$
$$f_5 = xz^3 - xz^2,$$

образуют базис Грёбнера идеала, введенного в предыдущем упражнении.

9.36. Упражнение. Показать, что, используя теорему 9.33.11, в предыдущем упражнении достаточно рассмотреть S-элементы для пар (2,3), (2,4), (5,6), (4,7), (2,7), (5,7), (5,8), (6,8), (4,9), (5,9).

9.37. Упражнение. Пусть D — кольцо обобщенных многочленов над полем от конечного числа неизвестных, F — свободный D-модуль и ранжир на множестве термов T_F правильный. Пусть H — подмодуль модуля F и G — базис Грёбнера подмодуля H. Показать, что для каждого элемента $f \in H$ существует представление $f = \sum\limits_{j=1}^{r} \lambda_j g_j$, где $\lambda_j \in D$, $g_j \in G$, такое, что $\deg f \geqslant \deg \lambda_j g_j$ для всех $j = 1, \ldots, r$.

Если данная система элементов не является базисом Грёбнера порождаемого ею подмодуля, то ее можно расширить, присоединяя поочередно элементы, получающиеся редуцированием S-элементов.

9.38. Упражнение. Доказать конечность следующего рекурсивного алгоритма построения базиса Грёбнера полиномиального идеала (алгоритм пополнения).

Алгоритм `Groebner(`$\mathcal{A}$`)`

Дано: $\mathcal{A}$ — конечное множество образующих идеала I,
$\Longrightarrow$ — алгоритм нормальной формы.

Надо: $\mathcal{A}$ — базис Грёбнера идеала I.

Начало

если $\exists g_1, g_2 \in \mathcal{A}$, такие, что $S(g_1, g_2) \xrightarrow[\mathcal{A}]{*} g'$,
где $g' \neq 0$ — нередуцируемый относительно $\mathcal{A}$ многочлен,
то `Groebner(`$\mathcal{A} \cup \{g'\}$`)`

конец если

Конец

Очевидно, что сформулированный алгоритм не является оптимальным. Учитывая роль, которую базисы Грёбнера играют в компьютерной алгебре, и высокую сложность алгоритмов их построения, оптимизация этих алгоритмов приобретает особое значение. Вопросы оптимизации будут рассмотрены несколько позже.

Базис Грёбнера для любого подмодуля M определен неоднозначно. В частности, после присоединения к базису Грёбнера модуля M любого элемента $h \in M$ снова получаем базис Грёбнера модуля M. Естественно возникает вопрос о минимальных базисах Грёбнера.

Следующая терминология пришла из дифференциальной алгебры.

9.39. Определение. Подмножество $G = \{g_i : i \in I\}$ свободного модуля F называется *авторедуцированным множеством*, если любой элемент $g_i \in G$ нередуцируем относительно $G \setminus \{g_i\}$.

Из определения немедленно следует, что лидеры всех элементов, принадлежащих авторедуцированному множеству, различны.

9.40. Предложение. *Пусть D — кольцо обобщенных многочленов от переменных $X = \{x_1, \ldots, x_m\}$ над полем K и F — свободный D-модуль с базисом $E = \{e_1, \ldots, e_n\}$. Любое авторедуцированное множество в F состоит из конечного числа элементов, следовательно, его элементы можно упорядочить по возрастанию лидеров.*

Доказательство. Доказательство немедленно следует из леммы 12.1. □

Зафиксировав ранжир $<$ на множестве термов T_F, можно ввести отношение частичного порядка на множестве авторедуцированных множеств.

Пусть $\mathcal{A} = \{a_1, \ldots, a_p\}$ и $\mathcal{B} = \{b_1, \ldots, b_q\}$ — авторедуцированные множества, элементы которых упорядочены по возрастанию лидеров. Будем считать, что $\mathcal{A} < \mathcal{B}$, если,

- либо существует i, $1 \leqslant i \leqslant \min(p, q)$, такое, что $\mathbf{u}_{a_i} < \mathbf{u}_{b_i}$ и $\mathbf{u}_{a_j} = \mathbf{u}_{b_j}$ для всех $j < i$,
- либо $p > q$ и $\mathbf{u}_{a_j} = \mathbf{u}_{b_j}$ для $1 \leqslant j \leqslant q$.

9.41. Лемма. *Любое множество $\mathbb{A} = \{\mathcal{A}_i,\ i \in I\}$ авторедуцированных подмножеств содержит минимальный элемент относительно введенного частичного порядка. Минимальный элемент в множестве всех авторедуцированных подмножеств некоторого подмодуля M свободного D-модуля является базисом Грёбнера модуля M.*

Доказательство. По предложению 9.40 мы можем предполагать, что элементы в наших авторедуцированных множествах упорядочены по возрастанию старших термов. Зафиксируем минимальное значение лидера для первых элементов рассматриваемых авторедуцированных множеств (это значение определено однозначно, поскольку множество термов вполне упорядочено). Обозначим этот лидер φ_1. В системе авторедуцированных множеств $\mathbb{A} = \{\mathcal{A}_i \mid i \in I\}$ рассмотрим подсистему $\mathbb{A}' = \{\mathcal{A}_i \mid i \in I'\}$ множеств $\mathcal{A}_i = \{a_1^i, \ldots, a_{k_i}^i\}$, таких, что $\mathbf{u}_{a_1^i} = \varphi_1$. В $\mathbb{A}'$ найдем минимальное значение лидера вторых элементов, обозначим его φ_2. Продолжая подобным обра-

зом, получим авторедуцированную систему термов, упорядоченную по возрастанию ранга их лидеров. По предложению 9.40 эта система должна обрываться на конечном шаге. Выбор системы лидеров осуществлялся таким образом, чтобы всегда существовало авторедуцированное множество, лидеры элементов которого имели вид $\varphi_1, \ldots, \varphi_i$. Авторедуцированное множество, соответствующее полной системе $\varphi_1, \ldots, \varphi_n$, является минимальным.

Для доказательства того, что $\mathcal{A}$ — базис Грёбнера модуля M, воспользуемся условием 2 теоремы 9.33. Предположим противное, тогда существует элемент $g \in M$, старший терм g которого редуцирован относительно $\mathcal{A}$. Можно предполагать, что он сам также редуцирован относительно $\mathcal{A}$. Рассмотрим множество

$$\mathcal{A}' = \{a_i \in \mathcal{A} \mid a_i < g\} \cup \{g\}.$$

Это множество авторедуцировано и его ранг меньше ранга $\mathcal{A}$, что противоречит предположению о минимальности $\mathcal{A}$. □

9.42. Следствие. *Пусть D — кольцо обобщенных многочленов над полем, F — свободный конечнопорожденный D-модуль. Тогда для каждого подмодуля M модуля F существует базис Грёбнера.*

9.43. Следствие. *Всякое кольцо обобщенных многочленов над полем является (слева) нетеровым.*

Доказательство. Как следует из следствия 9.42, во всяком левом идеале такого кольца существует базис Грёбнера. Как видно из определения 9.26, базис Грёбнера конечен и порождает этот идеал. □

9.44. Определение. Базис Грёбнера G модуля $M \subseteq F$ назовем *авторедуцированным*, если множество G авторедуцировано.

9.45. Предложение. *Авторедуцированный базис Грёбнера модуля M определен однозначно с точностью до умножения его элементов на константы из поля K.*

Доказательство. Среди всех авторедуцированных подмножеств модуля M выберем минимальное. Обозначим его $\mathcal{A}$ и предположим, что его элементы нормированы так, что все их старшие коэффициенты равны 1. Покажем, что этим условием множество $\mathcal{A}$ определено однозначно и что оно является базисом Грёбнера модуля M.

Предположим, что $\mathcal{A} = \{a_1, \ldots, a_r\}$ и $\mathcal{B} = \{b_1, \ldots, b_s\}$ — два множества, удовлетворяющих сформулированным выше условиям.

Из условия минимальности следует, что $r = s$ и $\mathbf{u}_{a_i} = \mathbf{u}_{b_i}$ для любого i. Предположим, что существует i, для которого $a_i \neq b_i$. Ненулевой элемент $a_i - b_i \in M$ редуцирован относительно a_j для $j < i$, поскольку нередуцируемость зависит только от множеств лидеров для $\mathcal{A}$ и $\mathcal{B}$, а эти множества лидеров совпадают. По лемме 9.41 $\mathcal{A}$ — базис Грёбнера модуля M, что противоречит нетривиальности элемента $a_i - b_i$. □

9.46. Определение. Пусть $\mathcal{B} = \{b_1, \ldots, b_s\}$ — G-базис модуля $M \subseteq F$, относительно некоторого упорядочения термов из T_F. Назовем базис $\mathcal{B}$ *редуцируемым*, если для некоторого i, $1 \leqslant i \leqslant s$, существует G-представление $b_i = \sum_{j \neq i} c_j b_j$, в противном случае $\mathcal{B}$ называем *нередуцируемым*.

9.47. Определение. G-базис $\mathcal{B}$ модуля M, содержащий s элементов, назовем *минимальным*, если не существует G-базиса $\mathcal{B}'$ модуля M, содержащего менее s элементов.

9.48. Предложение. *Понятия минимальности и нередуцируемости G-базисов совпадают. Каждый авторедуцированный G-базис минимален, и каждый минимальный G-базис квазиавторедуцирован, т. е. множество его лидеров авторедуцировано (это множество определяется модулем M однозначно).*

Доказательство. Очевидно, что редуцируемый G-базис не является минимальным. Таким образом для доказательства предложения достаточно показать, что лидеры элементов нередуцируемого базиса определены однозначно. Доказательство проходит во многом аналогично доказательству предложения 9.45 и оставляется читателю в качестве самостоятельного упражнения. □

9.49. Примеры.

(1) Пусть K — поле и $m = 0$. Если матрица системы линейных многочленов приведена к ступенчатому виду, т. е. нет строк, которые начинаются с одного и того же столбца, то эта система представляет собой базис Грёбнера порождаемого ею модуля. Показать, что обратное, в общем случае, неверно, т. е. могут существовать базисы Грёбнера векторного подпространства, первые ненулевые элементы различных векторов которых стоят в одном и том же столбце.

(2) Пусть K — поле, $n = m = 1$. Множество $\mathcal{B}$ является базисом Грёбнера порождаемого им идеала тогда и только тогда,

когда оно содержит НОД всех своих элементов. Минимальный базис Грёбнера в этом случае состоит из одного элемента.

(3) Базис Грёбнера в упражнении 9.35 не является минимальным. После удаления из него первого элемента он становится минимальным и даже авторедуцированным.

9.50. Упражнение. Показать, что система алгебраических уравнений не имеет решений в алгебраическом замыкании поля коэффициентов тогда и только тогда, когда базис Грёбнера идеала, порожденного этой системой, содержит константу.

9.51. Упражнение. Показать, что система алгебраических уравнений из $K[x_1, \ldots, x_n]$ имеет конечное множество решений в алгебраическом замыкании поля коэффициентов тогда и только тогда, когда базис Грёбнера идеала, порожденного этой системой, содержит для любого $i = 1, \ldots, n$ многочлен со старшим мономом, являющимся степенью x_i.

9.52. Упражнение. Построить теорию базисов Грёбнера для идеалов в кольце многочленов с коэффициентами из кольца $\mathbb{Z}$.

10. Инволютивные базисы

Напомним основные определения и результаты теории базисов Грёбнера в простейшей постановке, т. е. для полиномиальных идеалов.

Пусть K — поле, $R = K[x_1, \ldots, x_n]$ — кольцо многочленов над полем K, I — идеал кольца R. Как идеал I, так и фактор-кольцо R/I являются линейными K-пространствами, в общем случае бесконечномерными. Как найти базисы этих пространств? В кольце R, рассматриваемом как K-пространство, имеется базис, состоящий из множества T всех мономов. Естественно попытаться разбить множество T на две части $T = T_1 \cup T_2$ так, что образы элементов из T_1 в фактор-кольце R/I образуют базис K-пространства R/I, а элементы базиса K-пространства I находятся во взаимно-однозначном соответствии с элементами множества T_2.

Предположим, что на множестве мономов задан допустимый порядок, т. е. отношение $<$, удовлетворяющее условиям:

(1) $1 < m$ для любого нетривиального монома m;

(2) если мономы t_1 и t_2 удовлетворяют соотношению $t_1 < t_2$, то $t_1 m < t_2 m$ для любого монома m.

Таким образом для любого многочлена f можно определить его *старший моном* $\mathrm{lm}(f)$ и *старший коэффициент* $\mathrm{lcoef}(f)$, и множество мономов T разбивается на два подмножества: T_1 состоит из мономов, которые не являются старшими мономами ни для одного элемента $f \in I$, и T_2 состоит из мономов, которые являются старшими мономами для элементов из I.

Теперь возникает вопрос: как описать множества T_1 и T_2 конструктивно?

Ответ на него, а также на многие другие вопросы конструктивной теории полиномиальных идеалов, дает теория базисов Грёбнера. Имеется несколько эквивалентных определений базисов Грёбнера (см., например, [**26**] или [**16**], в [**14**, стр. 40] эти определения рассматриваются с учетом выбора алгоритма нормальной формы). Например, множество $G \subset I$ называется *базисом Грёбнера* идеала I, если любой элемент $f \in I$ допускает представление вида $f = \sum_{i=1}^{N} c_i m_i g_i$, где $c_i \in K$, $m_i \in T$, $g_i \in G$ и выполнено условие $\mathrm{lm}(m_i g_i) > \mathrm{lm}(m_j g_j)$ при $j > i$ (представление такого вида называется G-представлением). Это определение, во-первых, не является конструктивным, во-вторых, определяет базис Грёбнера неоднозначно. Конструктивный метод построения базиса Грёбнера дает *алгоритм пополнения* (см. упражнение 9.38). Для того, чтобы выделить из всех базисов Грёбнера некоторый однозначно определенный, введем понятие авторедуцированного множества.

Множество многочленов $G = \{g_\alpha : \alpha \in \mathbb{I}\}$ называется *авторедуцированным*, если для любого $\alpha \in \mathbb{I}$ ни один из одночленов, входящих в g_α с ненулевым коэффициентом, не делится ни на один из мономов $\mathrm{lm}(g_\beta)$ для $\beta \neq \alpha$. Базис Грёбнера, который является авторедуцированным множеством и старшие коэффициенты элементов которого равны 1, определен однозначно для любого идеала I. Назовем такой базис *авторедуцированным базисом Грёбнера*.

Предположим, что мы знаем авторедуцированный базис Грёбнера G идеала I. Чтобы получить базис I как линейного пространства, нам достаточно указать процедуру, которая каждому моному $m \in T_2$ ставит в соответствие некоторый элемент $g(m) \in G$, старший моном которого делит m, т. е. $m = t(m) \cdot \mathrm{lm}(g(m))$ для некоторого монома $t(m)$. Тогда множество многочленов $t(m) \cdot g(m) \mid m \in T_2$ образует базис линейного пространства I. Любую такую процедуру назовем *алгоритмом нормальной формы*.

10.1. Пример. Простейший алгоритм нормальной формы состоит в том, что элементы авторедуцированного базиса Грёбнера нумеру-

ются в каком-либо порядке индексами от 1 до k и каждому моному $m \in T_2$ ставится в соответствие элемент g_i с минимальным индексом, такой, что $\mathrm{lm}(g_i)|m$. Существуют, однако, и более сложные алгоритмы нормальной формы.

Рассмотрим этот пример подробнее. Пусть авторедуцированный базис Грёбнера идеала I состоит из многочленов $g_1, \ldots, g_k$. Тогда базис линейного пространства I получается объединением следующих множеств множества $\mathcal{B}_1$ всех произведений $m \cdot g_1$, где $m \in T$;

множества $\mathcal{B}_2$ произведений $m \cdot g_2$, таких, что $\mathrm{lm}(m \cdot g_2) \notin \mathrm{lm}(\mathcal{B}_1)$;
множества $\mathcal{B}_3$ произведений $m \cdot g_3$, таких, что $\mathrm{lm}(m \cdot g_3) \notin \mathrm{lm}(\mathcal{B}_1) \cup \mathrm{lm}(\mathcal{B}_2)$;
...
множества $\mathcal{B}_k$ произведений $m \cdot g_k$, таких, что $\mathrm{lm}(m \cdot g_k) \notin \bigcup_{i=1}^{k-1} \mathrm{lm}(\mathcal{B}_i)$.

Этот же базис можно описать несколько по-другому.

Для каждого g_i выделим максимальное подмножество переменных $x_{i_1}, \ldots, x_{i_s}$ такое, что произведение g_i на любой моном, включающий только эти переменные (обозначим множество таких мономов $S(g_i)$), принадлежит $\mathcal{B}_i$. Назовем эти переменные *мультипликативными* для монома $\mathrm{lm}(g_i)$, остальные переменные назовем *немультипликативными*. Исключим из $\mathcal{B}_i$ моном g_i и все его произведения на мономы из $S(g_i)$. Если полученное множество непусто, то возьмем в нем младший моном g_i' и повторим процесс для него. Таким образом мы можем представить базис линейного пространства I в виде объединения конечного набора множеств, каждое из которых описывается некоторым многочленом и набором мультипликативных переменных для этого многочлена. Полученный базис представляет собой пример *инволютивного базиса*. В коммутативную алгебру понятие инволютивного базиса было введено Жарковым и Блинковым [**8, 30**].

Итак, для построения инволютивного базиса мы воспользовались базисом Грёбнера, алгоритмом нормальной формы и процедурой разделения переменных на мультипликативные и немультипликативные для некоторого набора мономов.

Напомним алгоритмы проверки того, что заданное множество является базисом Грёбнера порождаемого им идеала и построения базиса Грёбнера по заданной системе образующих идеала I (этот алгоритм называется *алгоритмом пополнения*).

Пусть дано множество многочленов G и отношение порядка на множестве мономов $<$. Для проверки того, что G является бази-

сом Грёбнера идеала $I = (G)$ относительно порядка $<$, используется некоторый алгоритм нормальной формы, от выбора которого результат не зависит. Алгоритм состоит в том, что формируется множество S-полиномов и проверяется, что каждый из этих полиномов редуцируется к нулю. Для повышения эффективности алгоритма используются различные критерии, позволяющие сузить круг рассматриваемых S-полиномов, например, "правило треугольника".

Как сказано выше, множество многочленов $G = \{g_1, \ldots, g_k\}$ и алгоритм нормальной формы позволяют сформировать множества $\mathcal{B}_i$, каждое из которых получается путем умножения многочлена g_i на некоторое множество мономов. S-полиномы соответствуют многочленам g_i и мономам m_i, таким, что m_i является минимальным (относительно деления мономов) мономом, для которого $m_i \cdot g_i \notin \mathcal{B}_i$. В действительности, проверять редуцируемость к нулю нужно только для таких многочленов (заметим, что при этом рассматриваются не все S-полиномы, автоматически используется "правило треугольника"). Естественно потребовать, чтобы множество G было авторедуцированным.

Алгоритм пополнения основан на описанном выше методе S-полиномов и отличается от приведенного выше алгоритма тем, что в случае нередуцируемости S-полинома его нормальная форма добавляется к множеству G. При этом, как правило, меняется алгоритм нормальной формы, т. е. множества $\mathcal{B}_i$, описанные выше.

Как правило, для повышения эффективности алгоритмов построения базисов Грёбнера совершенствуются методы перебора S-полиномов, но мало внимания уделяется рассмотрению возможных алгоритмов нормальной формы.

До настоящего момента мы никак не ограничивали выбор алгоритма нормальной формы, т. е. формирование множеств $\mathcal{B}_i$ для заданной системы многочленов $G = \{g_i\}$. Теперь предположим, что на множестве мономов задано некоторое отношение "делимости" $|_L$, удовлетворяющее следующим аксиомам (аксиомы *глобального инволютивного деления*, см., например, [**22**]):

(1) $u\big|_L v \implies u|v$ (в смысле обычного деления);
(2) $1\big|_L u$;
(3) $u\big|_L w \wedge v\big|_L w \implies u\big|_L v \vee v\big|_L u$;
(4) $u\big|_L uvw \iff u\big|_L uv \wedge u\big|_L uw$;
(5) $u\big|_L v \wedge v\big|_L w \implies u\big|_L w$ (транзитивность).

В случае, если имеет место отношение $u\big|_L v$, мы будем говорить, что u *инволютивно делит* v.

Аксиомы 3 и 4 для случая двух переменных можно наглядно представить следующим образом.

Изобразим мономы вида $x^i y^j$ на плоскости точками с координатами (i, j). Тогда

- множества инволютивных кратных для любых двух мономов либо не пересекаются, либо одно из них содержится в другом;
- множество кратных монома $x^i y^j$ представляется либо одной точкой (i, j), либо вертикальным или горизонтальным лучом, выходящим из этой точки, либо углом между вертикальным и горизонтальным лучами, выходящими из этой точки.

Обобщение на случай нескольких переменных очевидно.

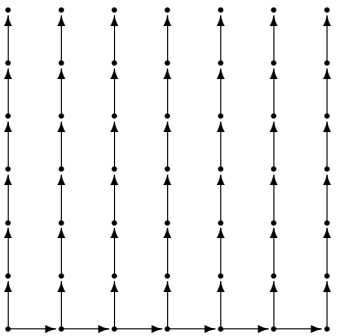
10.2. Упражнение. Показать, что глобальное инволютивное деление определяет для каждого монома u множество $M(u)$ его *мультипликативных переменных* как множество таких переменных, что u инволютивно делит любое произведение u на моном, включающий только мультипликативные переменные. Остальные переменные назовем *немультипликативными* для монома u (обозначение $NM(u)$).

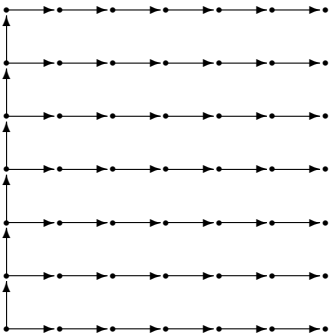
Примеры глобальных инволютивных делений:

10.3. Примеры.

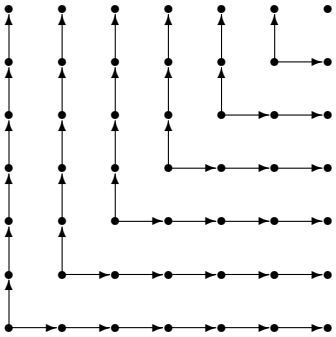
(1) $M(x_1^{i_1} \dots x_k^{i_k}) = \{x_k, \dots, x_n\}$ — *правое деление Поммаре*.
(2) $M(x_k^{i_k} \dots x_n^{i_n}) = \{x_1, \dots, x_k\}$ — *левое деление Поммаре*.
(3) $M(x_1^{i_1} \dots x_n^{i_n}) = \{x_k \ : \ i_k = \max_{m=1}^{n} i_m\}$.

Для двух переменных правое и левое деление Поммаре можно проиллюстрировать следующим образом:





Для третьего примера геометрическая интерпретация выглядит следующим образом:



10.4. Упражнение. В кольце многочленов $K[x,y,z]$ найти мультипликативные и немультипликативные переменные для мономов x^5, x^3y^2, xyz для каждого из глобальных инволютивных делений, рассмотренных в примерах 10.3.

Можно рассмотреть более общую ситуацию, когда фиксировано некоторое конечное множество U мономов, а инволютивное деление зависит от этого множества. При этом в левой части отношения $u\big|_L v$ могут стоять только мономы из множества U.

10.5. Определение. Согласно [**21**], на моноиде M задано *инволютивное деление* L, если для каждого конечного подмножества $U \subset M$ и для каждого монома $u \in U$ определен подмоноид $L(u,U)$ моноида M, удовлетворяющий следующим условиям:

(1) Если $w \in L(u,U)$ и $v|w$, то $v \in L(u,U)$;
(2) Если $u,v \in U$ и $uL(u,U) \cap vL(v,U) \neq \emptyset$, то $u \in vL(v,U)$ или $v \in uL(u,U)$;
(3) Если $v \in U$ и $v \in uL(u,U)$, то $L(v,U) \subseteq L(u,U)$;
(4) Если $V \subseteq U$, то $\forall\, u \in V\ L(u,U) \subseteq L(u,V)$.

Образующие моноида $L(u,U)$ называются *мультипликативными переменными* для u. Если $w \in uL(u,U)$, то пишут $u\big|_L w$, и моном u называется *(L-)инволютивным делителем монома* w, а моном w называется *(L-)инволютивным кратным* монома u. В этом случае равенство $w = uv$ мы будем записывать в виде $w = u \times v$, в противном случае — в виде $w = u \cdot v$, и моном v будем называть *немультипликативным* для u.

10.6. Упражнение. Показать, что глобальное инволютивное деление является инволютивным делением в смысле определения 10.5.

10.7. Определение. Мы говорим, что многочлен f *инволютивно редуцируется к многочлену* g *с помощью многочлена* h *по моному* m, входящему в f, и пишем, опуская упоминание о мономе m, $f \xrightarrow[\text{inv } h]{} g$, если f редуцируется к g в обычном смысле, и $\mathrm{lm}(h)|_L m$. Естественным образом определяется отношение $\xrightarrow[\text{inv } G]{}$ для произвольного множества G многочленов и его транзитивное $\xrightarrow[\text{inv } G]{+}$ и рефлексивно-транзитивное $\xrightarrow[\text{inv } G]{*}$ замыкания.

Если задано отношение редукции, то определена *нормальная форма*, которая в данном случае называется *инволютивной*.

Немультипликативным продолжением многочлена будем называть его произведение на некоторую немультипликативную для его старшего монома переменную.

10.8. Пример. Пусть $U \subset M$ — конечное подмножество. Для каждого $1 \leqslant i \leqslant n$ разделим множество U на группы, помеченные неотрицательными целыми числами $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{u \in U \mid d_j = \deg_j(u),\ 1 \leqslant j \leqslant i\}.$$

Переменная x_i мультипликативна для $u \in U$, если $i = 1$ и $\deg_1(u) = \max\{\deg_1(v) \mid v \in U\}$, или $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$ и $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$. (Здесь $\deg_j$ обозначает степень по переменной x_j.)

10.9. Определение. Пусть $R = K[x_1, \ldots, x_m]$ — кольцо многочленов от переменных $X = \{x_1, \ldots, x_m\}$, I — идеал кольца R, $G \subset I$ — конечное множество и $|_L$ — инволютивное деление на множестве мономов T. Множество G называется *инволютивным базисом* идеала I, если для любого ненулевого элемента $f \in I$ имеется *инволютивное представление*:

$$f = \sum_{i=1}^{r} c_i \theta_i g_i, \quad 0 \neq c_i \in K,\ \theta_i \in T(M(\mathrm{lm}(g_i))),\ g_i \in G. \qquad (10.1)$$

10.10. Теорема. *Пусть* $R = K[x_1, \ldots, x_m]$ *— кольцо многочленов от переменных* $X = \{x_1, \ldots, x_m\}$, I *— идеал кольца* R, $G \subset I$ *— конечное множество и* $|_L$ *— инволютивное деление на множестве мономов* T. *Предположим, что множество* G *нормализовано таким образом, что* $\mathrm{Hcoeff}(g_i) = 1$ *для всех* $g_i \in G$. *Тогда эквивалентны следующие условия:*

(1) G *является инволютивным базисом идеала* I;

(2) $\mathbf{u}_G$ *инволютивно порождает* $\mathbf{u}_I$;

(3) *для любого* $f \in I$ *имеет место* $f \xrightarrow[inv\ G]{*} 0$;

(4) *если* $f - f' \in I$ *и* f, f' *инволютивно нередуцируемы, то* $f = f'$;

(5) *если* $f \in I$ *и* f *инволютивно нередуцируем, то* $f = 0$.

Следующие условия являются необходимыми для выполнения предыдущих, и если множество G *порождает* I*, то они являются и достаточными:*

(6) *Если* $f \in G$ *и* $x_i \in NM(\mathrm{lm}(f))$*, то* $x_i f$ *допускает инволютивное представление;*

(7) $x_i f \xrightarrow[inv\ G]{*} 0$ *для любых* $f \in G$ *и* $x_i \in NM(\mathrm{lm}(f))$.

Доказательство оставляется читателю в качестве упражнения.

Инволютивный базис может быть легко построен, если мы знаем авторедуцированный базис Грёбнера соответствующего идеала и инволютивное деление. Это построение сводится к домножению элементов базиса Грёбнера на немультипликативные переменные.

Имея инволютивный базис $G = \{g_i\}$ и инволютивное деление, можно построить алгоритм нормальной формы следующим образом: для каждого многочлена g_i образуем множество его инволютивных кратных $\mathcal{B}_i$; множество $\bigcup_i \mathcal{B}_i$ является базисом линейного пространства I, причем любой моном может присутствовать не более, чем в одном элементе этого базиса. Для любого многочлена f мы можем исключать те его слагаемые, которые присутствуют в качестве старших мономов в множестве инволютивных кратных. Легко показать, что нередуцируемый многочлен, получающийся после таких исключений, не зависит от порядка этих исключений. Однако, чтобы избежать повторных исключений одного и того же монома (с разными коэффициентами), естественно проводить эти действия в порядке убывания мономов. Таким образом мы получаем алгоритм нормальной формы.

Естественно, не всякий алгоритм нормальной формы может быть получен таким образом. Возникает задача описания тех алгоритмов нормальной формы, которые определяются с помощью инволютивных базисов.

10.11. Предложение. *Если множество старших мономов многочленов из идеала разбивается на непересекающиеся конусы так, что элементы одного конуса редуцируются по одному многочлену из базиса, то соответствующее инволютивное деление выглядит следующим образом:*
для вершины конуса мультипликативными являются переменные, соответствующие образующим, а внутри конуса деление задается произвольным образом.

Доказательство. Формально указанное инволютивное деление $\big|_L$ задается так: пусть $\big|_{Ls}$ — произвольное инволютивное деление, соответствующее конусу C_s с вершиной в мономе s. Положим

$$\forall u, v \in C_s \; u\big|_L v \;\Leftrightarrow\; u\big|_{Ls} v.$$

Если же $\not\exists s : \; u, v \in C_s$, то положим $u \not|_L v$. Положим $\forall u \; 1\big|_L u$. Аксиомы инволютивного деления выполнены:

(1) $u\big|_L v \;\Rightarrow\; \exists s : \; u \in C_s,\, u\big|_{Ls} v \;\Rightarrow\; u|v$;

(2) $1\big|_L u$ — по определению $\big|_L$;

(3) $u\big|_L w,\, v\big|_L w \;\Rightarrow\; \exists s_1, s_2 : \; u, w \in C_{s_1},\, v, w \in C_{s_2}$, но тогда $C_{s_1} \cap C_{s_2} \neq \emptyset$, значит, $s_1 = s_2 =: s$. Отсюда $u\big|_{Ls} w,\, v\big|_{Ls} w \;\Rightarrow\; u\big|_{Ls} v \vee v\big|_{Ls} u \;\Rightarrow\; u\big|_L v \vee v\big|_L u$;

(4) $u\big|_L uvw \;\Rightarrow\; \exists s : \; u\big|_{Ls} uvw \;\Rightarrow\; u\big|_{Ls} uv \wedge u\big|_{Ls} uw \;\Rightarrow\; u\big|_L uv \wedge u\big|_L uw \;\Rightarrow\; \exists s : \; u, uv, uw \in C_s,\, u\big|_{Ls} uv \wedge u\big|_{Ls} uw \;\Rightarrow\; u\big|_{Ls} uvw \;\Rightarrow\; u\big|_L uvw$;

(5) $u\big|_L v,\, v\big|_L w \;\Rightarrow\; \exists s : \; u, v, w \in C_s,\, u\big|_{Ls} v,\, v\big|_{Ls} w \;\Rightarrow\; u\big|_{Ls} w \;\Rightarrow\; u\big|_L w$.

По определению $\big|_L$, любой старший моном многочлена идеала инволютивно редуцируется к вершине соответствующего конуса, кроме того, инволютивная нормальная форма всегда единственна. Алгоритм нормальной формы, заданный этими конусами, устроен так же. Поэтому соответствие алгоритма нормальной формы и инволютивного деления установлено. □

Глава 4

Целозначные многочлены

11. Определение целозначных многочленов и их основные свойства

11.1. Определение. Многочлен $f(t)$ от переменной t с рациональными коэффициентами называется *целозначным*, если $f(t) \in \mathbb{Z}$ для всех достаточно больших $t \in \mathbb{Z}$.

Очевидно, что всякий многочлен с целыми коэффициентами является целозначным. В качестве примера целозначного многочлена, коэффициенты которого не являются целыми числами, рассмотрим многочлен

$$\binom{t}{m} = \frac{t(t-1)\dots(t-m+1)}{m!} \quad (m \in \mathbb{Z}, m \geqslant 1), \tag{11.1}$$

который для любого целого $t \geqslant m > 0$ задает число сочетаний из t по m.

Иногда мы будем рассматривать выражение $\binom{t}{m}$ для неположительных значений m, полагая

$$\binom{t}{0} = 1, \quad \binom{t}{m} = 0 \quad \text{для } m < 0. \tag{11.2}$$

Мы также полагаем

$$\binom{t}{m}_+ = \begin{cases} \binom{t}{m} & \text{если } t \geqslant 0 \\ 0 & \text{если } t < 0. \end{cases}$$

Непосредственными вычислениями проверяется, что

$$\binom{t+1}{m} = \binom{t}{m} + \binom{t}{m-1} \quad \text{для всех } m \in \mathbb{N}. \tag{11.3}$$

Следующее предложение дает некоторые соотношения между "биномиальными" целозначными многочленами, которые будут использоваться в дальнейшем.

11.2. Предложение. *Следующие соотношения выполняются для всех* $n, p, r \in \mathbb{N}$:

$$\sum_{i=0}^{n} \binom{t+i}{r} = \binom{t+n+1}{r+1} - \binom{t}{r+1}; \tag{11.4}$$

$$\sum_{i=0}^{n} \binom{t+i}{i} = \binom{t+n+1}{n}; \tag{11.5}$$

$$\sum_{i=0}^{n} \binom{t}{i}\binom{k}{n-i} = \binom{t+k}{n}; \tag{11.6}$$

$$\sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i} = \sum_{i=0}^{n} \binom{n}{i}\binom{t+i}{n}; \tag{11.7}$$

$$\sum_{i=0}^{n} 2^i \binom{n}{i}\binom{t}{i} = \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i}\binom{t+i}{i}. \tag{11.8}$$

Доказательство. Справедливость равенств (11.4) и (11.5) может быть легко выведена из (11.3) индукцией по n.

Прежде чем доказывать (11.6)–(11.8), заметим, что если значения целозначных многочленов $f(t)$ и $g(t)$ совпадают для всех достаточно больших целых значений t, то $f(t) \equiv g(t)$. Поэтому при доказательстве (11.6)–(11.8) мы можем (и будем) предполагать, что $t \in \mathbb{Z}$, $t \geqslant n$.

Сравнивая коэффициенты при x^n в тождестве $(1+x)^{t+k} = (1+x)^t(1+x)^k$, мы получим (11.6). Для того, чтобы получить (11.7), сначала докажем, что

$$\sum_{i=0}^{n} \binom{n}{i}\binom{i}{n-k} = 2^k \binom{n}{k} \tag{11.9}$$

для всех $k, n \in \mathbb{N}$ (как обычно, мы полагаем $\binom{n}{k} = 0$ для $k > n$). Действительно, используя непосредственно проверяемое тождество

$$\binom{n}{i}\binom{i}{n-k} = \binom{n}{k}\binom{k}{i+k-n},$$

получаем

$$\sum_{i=0}^{n} \binom{n}{i}\binom{i}{n-k} = \sum_{i=0}^{n} \binom{n}{k}\binom{k}{i+k-n} = \binom{n}{k} \sum_{i=n-k}^{n} \binom{k}{i-(n-k)}$$

$$= \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j} = \binom{n}{k}(1+1)^k = 2^k \binom{n}{k}.$$

Теперь для завершения доказательства (11.7) достаточно воспользоваться (11.6) и (11.9):

$$\sum_{i=0}^{n}\binom{n}{i}\binom{t+i}{n}=\sum_{i=0}^{n}\binom{n}{i}\sum_{k=0}^{n}\binom{t}{k}\binom{i}{n-k}$$
$$=\sum_{k=0}^{n}\binom{t}{k}\sum_{i=0}^{n}\binom{n}{i}\binom{i}{n-k}=\sum_{k=0}^{n}2^k\binom{n}{k}\binom{t}{k}.$$

Теперь мы можем применить (11.6) и очевидное тождество

$$\binom{n}{i}\binom{i}{k}=\binom{n}{k}\binom{n-k}{i-k}\quad(n,k,i\in\mathbb{N}),$$

чтобы получить (11.8):

$$\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{t+i}{i}=\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\sum_{k=0}^{i}\binom{t}{k}\binom{i}{i-k}$$
$$=\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\sum_{k=0}^{n}\binom{t}{k}\binom{i}{k}$$
$$=\sum_{k=0}^{n}\binom{t}{k}\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n}{i}\binom{i}{k}$$
$$=\sum_{k=0}^{n}\binom{t}{k}\binom{n}{k}\sum_{i=0}^{n}(-1)^{n-i}2^i\binom{n-k}{i-k}$$
$$=\sum_{k=0}^{n}\binom{n}{k}\binom{t}{k}2^k\sum_{i=k}^{n}(-1)^{n-i}2^{i-k}\binom{n-k}{n-i}$$
$$=\sum_{k=0}^{n}2^k\binom{n}{k}\binom{t}{k}\sum_{j=0}^{n-k}(-1)^{(n-k)-j}2^j\binom{n-k}{n-k-j}$$
$$=\sum_{k=0}^{n}2^k\binom{n}{k}\binom{t}{k}(2-1)^{n-k}=\sum_{k=0}^{n}2^k\binom{n}{k}\binom{t}{k}.$$

Доказательство предложения закончено. □

Заметим, что если $f(t)$ — целозначный многочлен, то его первая разность $\Delta f(t)=f(t+1)-f(t)$ и следующие разности $\Delta^2 f(t)=$ $=\Delta(\Delta f(t))$, $\Delta^3 f(t)=\Delta(\Delta^2 f(t))$, и т. д. также являются целозначными многочленами. В частности, из (11.3) следует, что

$$\Delta\binom{t}{m}=\binom{t}{m-1}\quad(m\in\mathbb{N}).\tag{11.10}$$

11.3. Предложение. *Пусть $f(t)$ — целозначный многочлен степени m. Тогда $f(t)$ можно представить в виде*

$$f(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i}, \tag{11.11}$$

где $a_0, a_1, \ldots, a_m$ — целые числа, однозначно определенные многочленом $f(t)$.

Доказательство. Разделив многочлен $f(t)$ на $\binom{t+m}{m}$ в кольце $\mathbb{Q}[t]$, мы получим $f(t) = a_m\binom{t+m}{m} + r(t)$, где $a_m \in \mathbb{Q}$ и $\deg r(t) \leqslant m-1$. Разделив $r(t)$ на $\binom{t+m-1}{m-1}$ (в $\mathbb{Q}[t]$), мы получим $f(t) = a_m\binom{t+m}{m} + a_{m-1}\binom{t+m-1}{m-1} + r_1(t)$, где $\deg r_1(t) \leqslant m-2$. Продолжая этот процесс, мы придем к выражению

$$f(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i}, \quad a_i \in \mathbb{Q} \quad (i = 0, 1, \ldots, m), \tag{11.12}$$

где рациональные числа $a_0, a_1, \ldots, a_m$ однозначно определены многочленом $f(t)$. Нам нужно показать, что $a_i \in \mathbb{Z}$ $(i = 0, 1, \ldots, m)$. Будем это делать индукцией по $m = \deg f(t)$.

Если $m = 0$, то из целозначности многочлена $f(t)$ следует, что $f(t) = a_0 \in \mathbb{Z}$. Предположим, что $m > 0$ и существование и однозначность представления (11.11) (с целыми коэффициентами $a_0, a_1, \ldots, a_m$) доказана для всех целозначных многочленов степени меньшей m. Рассматривая конечные разности обеих частей (11.12) и используя (11.10), мы получаем

$$\Delta^k f(t) = \sum_{i=0}^{m-k} a_{i+k} \binom{t+i+k}{i} \quad (k = 1, 2, \ldots, m).$$

Многочлен $\Delta^k f(t)$ является целозначным, следовательно, $\Delta^m f(t) = a_m \in \mathbb{Z}$. Применяя предположение индукции к многочлену $f(t) - a_m\binom{t+m}{m} = \sum\limits_{i=0}^{m-1} a_i\binom{t+i}{i}$ (степень которого не превосходит $m-1$), мы получим, что $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}$. □

Из предложения 11.3, в частности, следует, что старший коэффициент любого целозначного многочлена $f(t)$ степени m равен $\frac{\Delta^m f(t)}{m!}$, следовательно, $f(t)$ можно представить в виде

$$f(t) = \frac{\Delta^m f(t)}{m!} t^m + o(t^m). \tag{11.13}$$

(Как обычно, $o(t^m)$ обозначает многочлен с рациональными коэффициентами, степень которого не превосходит $m-1$.)

Кроме того, поскольку $\binom{t+i}{i} \in \mathbb{Z}$ для любых $t \in \mathbb{Z}$ и $i \in \mathbb{N}$, из предложения 11.3 вытекает следующий результат.

11.4. Следствие. *Пусть $f(t)$ — целозначный многочлен. Тогда $f(s) \in \mathbb{Z}$ для всех $s \in \mathbb{Z}$ (не только достаточно больших).*

11.5. Предложение. *Пусть $f(t) = a_m t^m + a_{m-1}t^{m-1} + \cdots + a_1 t + a_0$ — целозначный многочлен степени m и $s_0 \in \mathbb{Z}$. Тогда существует целозначный многочлен $g(t)$ со следующими свойствами:*

(1) $g(s) = f(s_0+1) + f(s_0+2) + \cdots + f(s)$ *для всех* $s \in \mathbb{Z}$, $s > s_0$;
(2) $\deg g(t) = m+1$;
(3) *старший коэффициент многочлена $g(t)$ равен* $\frac{1}{m+1}a_m$.

Доказательство. По предложению 11.3 $f(t)$ можно представить в виде $f(t) = \sum\limits_{i=0}^{m} b_i \binom{t+i}{i}$, где $b_0, b_1, \ldots, b_m \in \mathbb{Z}$, и легко видеть, что $b_m = a_m \cdot m!$. Следовательно,

$$f(s_0+1) + f(s_0+2) + \cdots + f(s) = \sum_{i=0}^{m} b_i \sum_{k=0}^{s-s_0-1} \binom{s_0+1+i+k}{i}$$

для всех $s \in \mathbb{Z}$, $s > s_0$. Воспользовавшись соотношением (11.4), можно заменить внутреннюю сумму в правой части последнего уравнения на $\binom{s+i+1}{i+1} - \binom{s_0+i+1}{i+1}$, следовательно,

$$\begin{aligned}\sum_{j=1}^{s-s_0} f(s_0+j) &= \sum_{i=0}^{m} b_i \left[\binom{s+i+1}{i+1} - \binom{s_0+i+1}{i+1}\right] \\ &= \sum_{i=0}^{m} b_i \binom{s+i+1}{i+1} - A,\end{aligned}$$

где $A = \sum\limits_{i=0}^{m} b_i \binom{s_0+i+1}{i+1} \in \mathbb{Z}$. Таким образом, целозначный многочлен $g(t) = \sum\limits_{i=0}^{m} b_i \binom{t+i+1}{i+1} - A$ удовлетворяет всем условиям (1)–(3) (степень этого многочлена равна $m+1$, и коэффициент при t^{m+1} равен коэффициенту при t^{m+1} в многочлене $b_m \binom{t+m+1}{m+1}$, т. е. числу $\frac{b_m}{(m+1)!} = \frac{1}{m+1}a_m$). Предложение доказано. □

В заключение этого параграфа мы дадим решение некоторых комбинаторных задач, тесно связанных с задачей вычисления дифференциальных и разностных размерностных многочленов.

Для любых целых чисел m и r ($m > 0$, $r \geqslant 0$), пусть $\mu^+(m,r)$ обозначает число решений уравнения

$$x_1 + x_2 + \cdots + x_m = r \tag{11.14}$$

в положительных целых числах x_i. Пусть $\mu(m,r)$ обозначает число решений уравнения (11.14) в неотрицательных целых числах x_i, и $\bar{\mu}(m,r)$ — число решений в целых числах x_i уравнения

$$|x_1| + |x_2| + \cdots + |x_m| = r. \tag{11.15}$$

11.6. Предложение. *В обозначениях, введенных выше,*

$$\mu^+(m,r) = \binom{r-1}{m-1}, \tag{11.16}$$

$$\mu(m,r) = \binom{m+r-1}{m-1}, \tag{11.17}$$

$$\bar{\mu}(m,r) = \sum_{i=1}^{m} 2^i \binom{m}{i}\binom{r-1}{i-1}. \tag{11.18}$$

Доказательство. Прежде всего докажем равенство (11.17). Для этого поставим в соответствие каждому решению $(x_1,\ldots,x_m) \in \mathbb{N}^m$ уравнения (11.14) упорядоченное множество из r нулей и $(m-1)$ единиц, построенное следующим образом: берем x_1 нулей, затем одну единицу, затем x_2 нулей и одну 1 и т. д. После последней единицы берем x_m нулей. Легко видеть, что построенное соответствие взаимно однозначно и $\mu(m,r)$ равно числу описанных выше множеств. С другой стороны, это число равно числу всех $(m-1)$-элементных подмножеств множества $\{1,2,\ldots,m+r-1\}$: подмножество $\{i_1,\ldots,i_{m-1}\}$ $(1 \leqslant i_1,\ldots,i_{m-1} \leqslant m+r-1)$ соответствует упорядоченному множеству нулей и единиц, в котором единицы находятся на местах $i_1,\ldots,i_{m-1}$. Следовательно, $\mu(m,r) = \binom{m+r-1}{m-1}$.

Любое решение $(x_1,\ldots,x_m)$ уравнения (11.14) в положительных целых числах соответствует решению $(x'_1,\ldots,x'_m) \in \mathbb{N}^m$ уравнения $x_1 + \cdots + x_m = r - m$, где $x'_i = x_i - 1$ $(1 \leqslant i \leqslant m)$. Обратно, каждое решение $(x'_1,\ldots,x'_m) \in \mathbb{N}^m$ последнего уравнения соответствует решению в положительных целых числах $(x'_1+1,\ldots,x'_m+1)$ уравнения (11.14). Следовательно,

$$\mu^+(m,r) = \mu(m,r-m) = \binom{r-m+m-1}{m-1} = \binom{r-1}{m-1}.$$

(Заметим, что (11.16) выполняется также при $r < m$, так как $\binom{k}{l} = 0$ для $k,l \in \mathbb{N},\ k < l$.)

Для доказательства равенства (11.18) заметим, что число m-наборов $(x_1,\dots,x_m)\in\mathbb{N}^m$, у которых $x_1+\dots+x_m=r$ и все координаты кроме $x_{k_1},\dots,x_{k_i}$ $(1\leqslant i\leqslant m)$ нулевые, равно $\mu^+(i,r)=\binom{r-1}{i-1}$. Значит, число элементов $(x_1,\dots,x_m)\in\mathbb{N}^m$, у которых $|x_1|+\dots+|x_m|=r$ и все координаты кроме $x_{k_1},\dots,x_{k_i}$ нулевые, равно $2^i\binom{r-1}{i-1}$. Таким образом, существует $\binom{m}{i}2^i\binom{r-1}{i-1}$ элементов $(x_1,\dots,x_m)\in\mathbb{Z}^m$, таких что $|x_1|+|x_2|+\dots+|x_m|=r$ и ровно i координат вектора $(x_1,\dots,x_m)$ отличны от нуля $(i=1,2,\dots,m)$. Следовательно, $\bar\mu(m,r)=\sum\limits_{i=1}^{m}2^i\binom{m}{i}\binom{r-1}{i-1}$. Предложение доказано. □

11.7. Предложение. *Пусть* $\bar u=(u_1,\dots,u_m)$, $\bar v=(v_1,\dots,v_m)\in\mathbb{N}^m$, $u_i\leqslant v_i$ $(i=1,\dots,m)$. *Обозначим через* $C_{mr}(\bar u,\bar v)$ $(m,r\in\mathbb{N},\ m\geqslant 1)$ *число решений* $(x_1,\dots,x_m)\in\mathbb{N}^m$ *уравнения* (11.14), *таких, что* $u_i\leqslant x_i\leqslant v_i$ $(i=1,\dots,m)$, *и пусть* $R=u_1+\dots+u_m$, $d_i=v_i-u_i+1$ $(1\leqslant i\leqslant m)$. *Тогда*

$$C_{mr}(\bar u,\bar v)=\binom{m+r-R-1}{m-1}+\sum_{k=1}^{m}(-1)^k\sum_{\substack{1\leqslant j_1<\dots<j_k\leqslant m\\ d_{j_1}+\dots+d_{j_k}\leqslant r-R}}\binom{m+r-R-d_{j_1}-\dots-d_{j_k}-1}{m-1}. \tag{11.19}$$

Доказательство. Из определения $C_{mr}(\bar u,\bar v)$ следует, что это число равно коэффициенту при t^r в многочлене

$$P(t)=t^R(1+t+\dots+t^{d_1-1})(1+t+\dots+t^{d_2-1})\dots(1+t+\dots+t^{d_m-1}).$$

Действительно, каждое решение $(x_1,\dots,x_m)\in\mathbb{N}^m$ $(u_i\leqslant x_i\leqslant v_i$ при $i=1,\dots,m)$ уравнения (11.14) находится во взаимно однозначном соответствии с мономом t^r (с коэффициентом 1), полученным разложением многочлена $P(t)$, если в i-х скобках мы возьмем множитель $t^{x_i-u_i}$ $(i=1,\dots,m)$. Следовательно, число таких мономов равно $C_{mr}(\bar u,\bar v)$.

Поскольку $1+t+\dots+t^{d_i-1}=(1-t)^{-1}(1-t^{d_i})$ $(1\leqslant i\leqslant m)$, имеем $P(t)=t^R(1-t)^{-m}\prod_{j=1}^{m}(1-t^{d_j})$. Кроме того, так как $(1-t)^{-1}=\sum\limits_{i=0}^{\infty}t^i$ в кольце формальных степенных рядов $\mathbb{Q}[[t]]$ (это

равенство является непосредственным следствием очевидного соотношения $(1-t)\sum\limits_{i=0}^{\infty} t^i = 1$), то

$$(1-t)^{-m} = (1+t+t^2+\dots)(1+t+t^2+\dots)\dots(1+t+t^2+\dots) = \sum_{l=0}^{\infty} C_l t^l,$$

где (в соответствии с вышесказанным) коэффициент C_l равен числу решений $(x_1,\dots,x_m) \in \mathbb{N}^m$ уравнения $x_1+\dots+x_m = l$. Следовательно, (см. предложение 11.6), $C_l = \binom{m+l-1}{m-1}$, так что $(1-t)^{-m} = \sum\limits_{l=0}^{\infty}\binom{m+l-1}{m-1}t^l$. Это соотношение показывает, что коэффициент при t^r в многочлене

$$P(t) = t^R\left\{\sum_{l=0}^{\infty}\binom{m+l-1}{m-1}t^l\right\}\prod_{j=1}^{m}(1-t^{d_j})$$

$$= \left\{\sum_{l=R}^{\infty}\binom{m+l-R-1}{m-1}t^l\right\}\cdot\left\{1+\sum_{k=1}^{m}(-1)^k\sum_{1\leqslant j_1<\dots<j_k\leqslant m} t^{d_{j_1}+\dots+d_{j_k}}\right\}$$

равен

$$\binom{m+r-R-1}{m-1} + \sum_{k=1}^{m}(-1)^k \sum_{\substack{1\leqslant j_1<\dots<j_k\leqslant m\\ d_{j_1}+\dots+d_{j_k}\leqslant r-R}} \binom{m+r-R-d_{j_1}-\dots-d_{j_k}-1}{m-1}$$

□

Обозначим через $\rho(m,r)$ и $\bar{\rho}(m,r)$ соответственно число решений $(x_1,\dots,x_m)\in\mathbb{N}^m$ неравенства

$$x_1+\dots+x_m \leqslant r \tag{11.20}$$

и число решений $(x_1,\dots,x_m)\in\mathbb{Z}^m$ неравенства

$$|x_1|+\dots+|x_m| \leqslant r, \tag{11.21}$$

$(m,r\in\mathbb{N};\ m>0)$.

11.8. Предложение. *Во введенных выше обозначениях*

$$\rho(m,r)=\binom{r+m}{m}, \tag{11.22}$$

$$\bar\rho(m,r)=\sum_{i=0}^{m}2^i\binom{m}{i}\binom{r}{i}=\sum_{i=0}^{m}\binom{m}{i}\binom{r+i}{m}$$

$$=\sum_{i=0}^{m}(-1)^{m-i}2^i\binom{m}{i}\binom{r+i}{i}. \tag{11.23}$$

Доказательство. Поскольку

$$\rho(m,r)=\sum_{k=0}^{r}\mu(m,k)=\sum_{k=0}^{r}\binom{m+k-1}{m-1}=\sum_{k=0}^{r}\binom{m+k-1}{k},$$

получаем (применяя (11.5) при $t=m-1$, $n=r$), что $\rho(m,r)=$ $=\binom{m-1+r+1}{r}=\binom{r+m}{m}$.

Чтобы доказать (11.23), воспользуемся формулой (11.18):

$$\bar\rho(m,r)=\sum_{k=0}^{r}\bar\mu(m,k)=\sum_{k=0}^{r}\sum_{i=0}^{m}2^i\binom{m}{i}\binom{k-1}{i-1}$$

$$=\sum_{i=0}^{m}2^i\binom{m}{i}\sum_{k=0}^{r}\binom{k-1}{i-1}.$$

Так как $\binom{k-1}{i-1}=0$ при $k<i$, имеем

$$\sum_{k=0}^{r}\binom{k-1}{i-1}=\sum_{k=i}^{r}\binom{k-1}{i-1}=\sum_{q=0}^{r-i}\binom{q+i-1}{i-1}$$

$$=\sum_{q=0}^{r-i}\binom{i-1+q}{q}=\binom{i-1+r-i+1}{r-i}=\binom{r}{i}$$

(см. (11.5)). Таким образом, $\bar\rho(m,r)=\sum\limits_{i=0}^{m}2^i\binom{m}{i}\binom{r}{i}$, и остальные равенства в (11.23) немедленно следуют из (11.7) и (11.8). Предложение доказано. □

12. Размерностные многочлены подмножеств в $\mathbb{N}^m$. Размерностный многочлен матрицы

Пусть $(\omega_1\leqslant_1),\dots,(\omega_m\leqslant_m)$ — упорядоченные множества. Их прямое произведение $P=\prod\limits_{i=1}^{m}\omega_i$ можно упорядочить различными

способами. В основном мы будем рассматривать два отношения порядка на множестве P: порядок произведения $\leqslant$, в котором неравенство $(a_1,\dots,a_m) \leqslant (b_1,\dots,b_m)$ выполняется тогда и только тогда, когда $a_i \leqslant_i b_i$ для всех $i = 1,\dots,m$, и лексикографический порядок $\prec$, который определяется следующими условиями: $(a_1,\dots,a_m) \prec \prec (b_1,\dots,b_m)$ в P, если существует индекс k, такой, что $a_1 = b_1,\dots,a_{k-1} = b_{k-1}$, но $a_k \neq b_k$, $a_k \leqslant_k b_k$. Легко видеть, что если каждое множество ω_i $(i = 1,\dots,m)$ вполне упорядочено относительно порядка $\leqslant_i$, то множество $P = \prod_{i=1}^{m} \omega_i$ является вполне упорядоченным относительно лексикографического порядка (в общем случае, P не является даже линейно упорядоченным относительно порядка произведения).

Мы будем рассматривать порядок произведения $\leqslant$ и лексикографический порядок $\prec$ на множестве $\mathbb{N}^m$ всех m-мерных векторов с неотрицательными целыми координатами, а также на множествах вида $\mathbb{N}^m \times \mathbb{N}_k$ $(m \in \mathbb{N})$, где $\mathbb{N}_k = \{1,2,\dots,k\}$ для любого $k \in \mathbb{Z}$, $k \geqslant 1$. Множества $\mathbb{N}$ и $\mathbb{N}_k$ всегда рассматриваются с естественным порядком, относительно которого они, очевидно, вполне упорядочены. Этот естественный порядок мы будем обозначать тем же символом $\leqslant$, который используется для обозначения порядка произведения, если это не ведет к неоднозначности толкования.

12.1. Лемма.

(1) *Любое бесконечное подмножество множества* $\mathbb{N}^m \times \mathbb{N}_k$ $(m,k \in \mathbb{N},\ k \geqslant 1)$ *содержит бесконечную последовательность, строго возрастающую относительно порядка произведения, проекции всех элементов которой на* $\mathbb{N}_k$ *равны между собой.*

(2) *Существует упорядочение* $\leqslant_0$ *множества* $\mathbb{N}^m \times \mathbb{N}_k$, *относительно которого это множество является вполне упорядоченным, удовлетворяющее следующим двум условиям:*

(a) $(i_1,\dots,i_m,j) \leqslant_0 (i_1+e_1,\dots,i_m+e_m,j)$ *для всех*

$$i_1,\dots,i_m,e_1,\dots,e_m \in \mathbb{N}, \quad j \in \mathbb{N}_k;$$

(b) *если* $(i_1,\dots,i_m,j) \leqslant_0 (i'_1,\dots,i'_m,j')$, *то*

$$(i_1+e_1,\dots,i_m+e_m,j) \leqslant_0 (i'_1+e_1,\dots,i'_m+e_m,j')$$

для всех $i_1,\dots,i_m,i'_1,\dots,i'_m,e_1,\dots,e_m \in \mathbb{N}$, $j,j' \in \mathbb{N}_k$.

(3) *Множество $\mathbb{N}^m \times \mathbb{N}_k$ является вполне упорядоченным относительно любого линейного порядка, удовлетворяющего условию 2a.*

Доказательство. Легко видеть, что если E — бесконечное подмножество множества $\mathbb{N}^m \times \mathbb{N}_k$, то существует бесконечное подмножество $E_1 \subseteq E$, проекции всех элементов $e \in E_1$ которого на $\mathbb{N}_k$ равны между собой. Значит, для доказательства первого утверждения леммы достаточно показать, что любое бесконечное подмножество в $\mathbb{N}^m$ содержит бесконечную последовательность, строго возрастающую относительно порядка произведения. Пусть F — бесконечное подмножество множества $\mathbb{N}^m$. Если множество первых координат элементов множества F бесконечно, то существует бесконечное подмножество $G \subseteq F$, первые координаты любых двух различных элементов которого различны. Значит, существует бесконечная последовательность $G_1 \subseteq G$, такая, что первые координаты элементов из G_1 образуют строго возрастающую последовательность в $\mathbb{N}$. Если же множество первых координат элементов из F конечно, то существует бесконечное подмножество $F' \subset F$, все элементы которого имеют одну и ту же первую координату. В обоих случаях существует бесконечная подпоследовательность $F_1 \subseteq F$, состоящая из различных элементов множества F, первые координаты которых образуют неубывающую последовательность в $\mathbb{N}$. Аналогично, из F_1 можно выбрать бесконечную подпоследовательность F_2, вторые координаты элементов которой образуют неубывающую последовательность в $\mathbb{N}$ и т. д. В результате мы получим бесконечную последовательность F_m элементов из $\mathbb{N}^m$, которая строго возрастает относительно порядка произведения. Таким образом, первое утверждение леммы доказано.

Рассмотрим порядок $\leqslant_0$ на множестве $\mathbb{N}^m \times \mathbb{N}_k$, такой, что

$$(i_1, \dots, i_m, j) <_0 (i'_1, \dots, i'_m, j')$$

тогда и только тогда, когда

$$\Big(\sum_{\nu=1}^{m} i_\nu, j, i_1, \dots, i_m\Big) \prec \Big(\sum_{\nu=1}^{m} i'_\nu, j', i'_1, \dots, i'_m\Big)$$

("$\prec$" обозначает лексикографический порядок на $\mathbb{N} \times \mathbb{N}_k \times \mathbb{N}^m$) для любых элементов $(i_1, \dots, i_m, j)$, $(i'_1, \dots, i'_m, j') \in \mathbb{N}^m \times \mathbb{N}_k$. Множество $\mathbb{N}^m \times \mathbb{N}_k$ вполне упорядочено относительно этого порядка (поскольку множество $\mathbb{N} \times \mathbb{N}_k \times \mathbb{N}^m$ вполне упорядочено относительно лексикографического порядка), и условия 2a и 2b, очевидно, выполнены.

Докажем последнее утверждение леммы. Пусть $\leqslant_0$ — линейный порядок на множестве $\mathbb{N}^m \times \mathbb{N}_k$, удовлетворяющий условию 2а, и пусть F — бесконечное подмножество множества $\mathbb{N}^m \times \mathbb{N}_k$. По первому утверждению леммы, существует бесконечная подпоследовательность $F_1 \subseteq F$, строго возрастающая относительно порядка произведения и такая, что проекции на $\mathbb{N}_k$ всех ее элементов равны между собой. Покажем, что F_1 также строго возрастает относительно порядка $\leqslant_0$. Действительно, если $f' = (i_1, \ldots, i_m, j)$, $f'' = (i'_1, \ldots, i'_m, j) \in F_1$ и $f' \neq f''$, $i_1 \leqslant i'_1, \ldots, i_m \leqslant i'_m$, то $f' \leqslant_0 f'' = (i_1 + (i'_1 - i_1), \ldots, i_m + (i'_m - i_m), j)$, поскольку порядок $\leqslant_0$ удовлетворяет условию 2а. Таким образом, любая строго убывающая (относительно порядка $\leqslant_0$) последовательность элементов из $\mathbb{N}^m \times \mathbb{N}_k$ конечна (иначе, как мы видели, она содержит строго возрастающую последовательность, что невозможно для убывающей последовательности), так что множество $\mathbb{N}^m \times \mathbb{N}_k$ вполне упорядочено. Лемма доказана. □

Пусть $m \in \mathbb{Z}$, $m \geqslant 1$ и U — подмножество множества $\mathbb{N}^m$. Для любого $s \in \mathbb{N}$ обозначим $U(s)$ множество элементов $\mathbf{u} = (u_1, \ldots, u_m)$ из U, для которых выполнено неравенство $\sum\limits_{i=1}^{m} u_i \leqslant s$.

Если $E \subseteq \mathbb{N}^m$, то V_E будет обозначать множество всех элементов $\mathbf{v} \in \mathbb{N}^m$, которые не превосходят ни одного элемента из E относительно порядка произведения $\leqslant$ на $\mathbb{N}^m$. (В дальнейшем, если противное не оговорено явно, все сравнения элементов из $\mathbb{N}^m$ рассматриваются относительно порядка произведения.) Таким образом, включение $\mathbf{v} \in V_E$ эквивалентно утверждению, что неравенство $\mathbf{e} \leqslant \mathbf{v}$ не выполняется ни для какого $\mathbf{e} \in E$.

В дальнейшем h_U обозначает функцию $\mathbb{N} \to \mathbb{N}$, такую, что $h_U(s) = \operatorname{Card} U(s)$ для любого $s \in \mathbb{N}$.

12.2. Лемма. *Пусть $U \subseteq \mathbb{N}^m$ и $U_{\mathbf{a}}$ — результат параллельного сдвига множества U на вектор $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$, т. е. $U_{\mathbf{a}} = \{\mathbf{a} + \mathbf{u} \mid \mathbf{u} \in U\} \subseteq \mathbb{Z}^m$. Предположим также, что $U_{\mathbf{a}} \subseteq \mathbb{N}^m$. Тогда для любого $s \in \mathbb{Z}$ имеем $h_U(s) = h_{U_{\mathbf{a}}}(s + |\mathbf{a}|)$, где $|\mathbf{a}| = \sum\limits_{i=1}^{m} a_i$.*

Доказательство. Очевидно, параллельный сдвиг на вектор $\mathbf{a}$, отображающий точку $\mathbf{u} \in U(s)$ на точку $\hat{\mathbf{u}} \in U_{\mathbf{a}}(s + |\mathbf{a}|)$, является биективным отображением множеств $U(s) \to U_{\mathbf{a}}(s + |\mathbf{a}|)$. Следовательно,

$$h_U(s) = \operatorname{Card} U(s) = \operatorname{Card} U_{\mathbf{a}}(s + |\mathbf{a}|) = h_{U_{\mathbf{a}}}(s + |\mathbf{a}|).$$

□

12.3. Лемма. *Пусть $K \subseteq \mathbb{Z}^m$ и $L = \{\mathbf{x} \in \mathbb{N}^m \mid \mathbf{x}$ не превосходит ни одной точки из K относительно порядка произведения на $\mathbb{Z}^m\}$. Тогда существует подмножество $H \subseteq \mathbb{N}^m$, такое, что $h_{V_H}(s) = h_L(s)$ для всех $s \in \mathbb{Z}$.*

Доказательство. Для любой точки $\mathbf{a} = (a_1, \ldots, a_m) \in K$ положим $f(\mathbf{a}) = (j_1, \ldots, j_m)$, где $j_i = \max(0, a_i)$, $i = 1, \ldots, m$. Пусть $H = \cup_{\mathbf{a} \in K} f(\mathbf{a})$. Тогда $H \subseteq \mathbb{N}^m$ является требуемым множеством. Действительно, $\mathbf{x} \in \mathbb{N}^m \setminus L$ тогда и только тогда, когда $\mathbf{x} \in \mathbb{N}^m$ и $\mathbf{x}$ больше или равен некоторой $\mathbf{a} \in K$, что эквивалентно неравенству $\mathbf{x} \geqslant f(\mathbf{a})$, $\mathbf{a} \in K$. □

Для любого данного подмножества $E \subseteq \mathbb{N}^m$ и для любого элемента $\mathbf{e} = (e_1, \ldots, e_m) \in \mathbb{N}^m$ пусть $E_1 = E \cup \mathbf{e}$ и $v(s) = h_{V_E}(s) - h_{V_{E_1}}(s)$ для любого $s \in \mathbb{Z}$. Ясно, что $v(s) = h_U(s)$, где U — множество элементов $\mathbf{v} \in V_E$, таких, что $\mathbf{v} \geqslant \mathbf{e}$. Применяя лемму 12.2 к U и $-\mathbf{e}$, видим, что $v(s) = h_{U_{-\mathbf{e}}}(s - |\mathbf{e}|)$. Далее, обозначая $K \subseteq \mathbb{Z}^m$ результат параллельного сдвига E на вектор $-\mathbf{e}$ и применяя лемму 12.2, получаем, что L совпадает с $U_{-\mathbf{e}}$. Таким образом, $h_{U_{-\mathbf{e}}}(s) = h_{V_H}(s)$, где множество H задается следующим условием:
$\mathbf{x} = (x_1, \ldots, x_m) \in H$ тогда и только тогда, когда существует элемент $\mathbf{r} = (r_1, \ldots, r_m) \in E$, такой, что $x_j = \max(0, r_j - e_j)$, $j = 1, \ldots, m$. Таким образом, мы доказали следующую формулу:

$$h_{V_E}(s) = h_{V_{(E \cup \mathbf{e})}}(s) + h_{V_H}(s - |\mathbf{e}|) \tag{12.1}$$

для всех $s \in \mathbb{Z}$.

Отметим, что в формуле (12.1) множество E, а следовательно, и H, может быть пустым.

12.4. Лемма. *Пусть $E \subseteq \mathbb{N}^m$ $(m > 1)$, и $1 \leqslant i \leqslant m$. Предположим, что E содержит элемент, i-я координата которого равна 1, а все остальные равны 0. Пусть $\tilde{E}$ обозначает множество всех элементов $e = (e_1, \ldots, e_{m-1}) \in \mathbb{N}^{m-1}$, таких, что $(e_1, \ldots, e_{i-1}, 0, e_i, \ldots, e_{m-1}) \in E$. Тогда $h_{V_E}(s) = h_{V_{\tilde{E}}}(s)$ для всех $s \in \mathbb{Z}$.*

Доказательство. Отображение $\varphi : V_{\tilde{E}}(s) \mapsto V_E(s)$, такое, что

$$\varphi(v_1, \ldots, v_{m-1}) = (v_1, \ldots, v_{i-1}, 0, \ldots, v_{m-1})$$

является взаимно однозначным отображением множества $V_{\tilde{E}}(s)$ на множество всех элементов $\mathbf{v} = (v_1, \ldots, v_m) \in V_E(s)$ с нулевой i-ой координатой, т. е. на множество $V_E(s)$. □

12.5. Теорема. *Для любого множества $E \subseteq \mathbb{N}^m$ $(m \geqslant 1)$ справедливы следующие утверждения:*

(1) *существует целозначный многочлен $\omega_E(t)$, такой, что $\omega_E(s) = \operatorname{Card} V_E(s)$ для всех достаточно больших $s \in \mathbb{N}$;*
(2) $\deg \omega_E \leqslant m$, *причем* $\deg \omega_E = m$ *тогда и только тогда, когда* $E = \emptyset$ *(в этом случае* $\omega_E(t) = \binom{t+m}{m}$*);*
(3) $\omega_E(t) \equiv 0$ *тогда и только тогда, когда* $(0, \ldots, 0) \in E$.

Доказательство. (1) Очевидно, что если F — множество всех минимальных элементов множества E, то $V_F = V_E$, так что мы можем (и будем) предполагать, что E конечно и его элементы попарно несравнимы. Пусть $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$, где $\mathbf{e}_i = (e_{i1}, \ldots, e_{im})$ $(i = 1, \ldots, r)$ и пусть $|E| = \sum\limits_{i=1}^{r} \sum\limits_{j=1}^{m} e_{ij}$. Доказательство будем вести индукцией по $|E|$. Если $|E| = 0$, то либо $E = \emptyset$, либо E состоит из единственного элемента $(0, \ldots, 0)$. В первом случае $V_E = \mathbb{N}^m$ и из (11.22) следует, что $\operatorname{Card} V_E(s) = \rho(m, s) = \binom{m+s}{m}$. Во втором случае (когда $(0, \ldots, 0) \in E$), $V_E = \emptyset$, следовательно, $\operatorname{Card} V_E(s) = 0$ для любого $s \in \mathbb{N}$, так что можно положить $\omega_E(t) \equiv 0$. Таким образом, утверждение (1) доказано при $|E| = 0$.

Более того, если $m = 1$, то E содержит только одну точку e, так что $\omega_E(t) \equiv e$ является требуемым многочленом.

Пусть $|E| > 0$ и $m > 1$. Тогда существует отличный от $(0, \ldots, 0)$ элемент $\mathbf{e} = (e_1, \ldots, e_m) \in E$. Пусть $e_i > 0$, для некоторого $1 \leqslant i \leqslant m$, и $\mathbf{r}$ — элемент множества $\mathbb{N}^m$, i-я координата которого равна 1 и все остальные равны 0. Применяя соотношение (12.1) к E и $\mathbf{r}$, получаем

$$h_{V_E}(s) = h_{V_{(E \cup \mathbf{r})}}(s) + h_{V_H}(s-1),$$

для некоторого $H \subseteq \mathbb{N}^m$ такого, что $|H| < |E|$.

По лемме 12.4 $h_{V_{(E \cup \mathbf{r})}}(s) = h_{V_{\tilde{E}}}(s)$, где $\tilde{E} \subset \mathbb{N}^{m-1}$, $|\tilde{E}| < |E|$. Согласно индуктивному предположению можно считать, что существуют целозначные многочлены $\omega_1(t)$ и $\omega_2(t)$ такие, что $h_{V_{(E \cup \mathbf{r})}}(s) = \omega_1(s)$ и $h_{V_H}(s) = \omega_2(s)$ для всех достаточно больших $s \in \mathbb{N}$. Поэтому целозначный многочлен

$$\omega_E(t) = \omega_1(t) + \omega_2(t-1)$$

удовлетворяет условиям первого утверждения леммы.

(2) Как мы уже видели, если $E = \emptyset$, то $\omega_E(t) = \binom{t+m}{m}$, $\deg \omega_E = m$. Значит, чтобы доказать второе утверждение теоремы, достаточно доказать, что $\deg \omega_E < m$, если $E \neq \emptyset$. Формула (12.1), примененная в

случае пустого множества E и произвольного вектора $\mathbf{e}$, показывает, что

$$\omega_{\mathbf{e}}(s) = \omega_{\emptyset}(s) - \omega_{\emptyset}(s - |\mathbf{e}|) = \binom{s+m}{m} - \binom{s+m-|\mathbf{e}|}{m},$$

т. е. $\omega_{\mathbf{e}}(t)$ является многочленом степени $m-1$. Остается отметить, что добавление новых элементов в множество E может только уменьшить значения $\omega(s)$, а, следовательно, не может увеличить степень многочлена $\omega_{\mathbf{e}}(t)$.

(3) Как мы уже видели, $\omega_E \equiv 0$, если $(0,\dots,0) \in E$. С другой стороны, если $\omega_E \equiv 0$, то $V_E(s) = \emptyset$ для всех достаточно больших $s \in \mathbb{N}$, следовательно, $V_E = \emptyset$. □

12.6. Определение. Многочлен $\omega_E(t)$, существование которого доказано в теореме 12.5, называется *многочленом Гильберта* подмножества $E \subseteq \mathbb{N}^m$.

12.7. Замечание. Из рассуждений, приведенных в начале доказательства теоремы 12.5, следует, что размерностный многочлен множества $E \subseteq \mathbb{N}^m$ равен размерностному многочлену конечного множества F, состоящего из всех минимальных элементов множества E. Поэтому, чтобы уметь находить размерностные многочлены подмножеств множества $\mathbb{N}^m$, достаточно найти метод, вычисляющий размерностные многочлены конечных подмножеств $F \subseteq \mathbb{N}^m$, элементы которых попарно несравнимы.

Поэтому в дальнейшем мы всегда будем иметь дело с конечными множествами $E = \{\mathbf{e}_1,\dots,\mathbf{e}_n\} \subseteq \mathbb{N}^m$ и записывать элементы этих множеств в виде матрицы размера $n \times m$ со строками $\mathbf{e}_1,\dots,\mathbf{e}_n$. Эту матрицу будем обозначать той же буквой E. Под размерностным многочленом $n \times m$-матрицы E мы будем понимать размерностный многочлен множества строк матрицы E (рассматриваемого как подмножество множества $\mathbb{N}^m$). В следующей теореме мы формулируем уже доказанные свойства размерностных многочленов подмножеств множества $\mathbb{N}^m$ в форме свойств размерностных многочленов матриц. Все элементы рассматриваемых матриц и векторов принадлежат $\mathbb{N}$.

12.8. Теорема. *Предположим, что $E = (e_{ij})$ — $n \times m$-матрица и $\mathbf{e} = (e_1,\dots,e_m)$ — вектор. Тогда*

(1) *имеет место равенство*

$$\omega_E(s) = \omega_{E \cup \mathbf{e}}(s) + \omega_H(s - |\mathbf{e}|), \tag{12.2}$$

где $E \cup \mathbf{e}$ *— матрица, полученная присоединением строки* $\mathbf{e}$ *к матрице* E, $H = (h_{ij})$ *—* $n \times m$*-матрица с элементами* $h_{ij} = \max(e_{ij} - e_j, 0)$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, *и* $|\mathbf{e}| = \sum_{k=1}^{m} e_k$;

(2) *если* $n \geqslant 1$, *то*

$$\omega_E(s) = \omega_{E \setminus \mathbf{e}_n}(s) - \omega_H(s - |\mathbf{e}_n|), \tag{12.3}$$

где $\mathbf{e}_n = (e_{n1}, \ldots, e_{nm})$, *и* $H = (h_{ij})$ *— это* $(n-1) \times m$*-матрица, такая, что* $h_{ij} = \max(e_{ij} - e_{nj}, 0)$;

(3) *размерностный многочлен матрицы* E *не меняется при перестановке строк;*

(4) *размерностный многочлен матрицы* E *не меняется при перестановке столбцов матрицы* E;

(5) *если* $e_{pj} \geqslant e_{qj}$ *при* $j = 1, \ldots, m$, *то* $\omega_E = \omega_{E_1}$, *где матрица* E_1 *получена из* E *удалением* p*-й строки (такую строку мы называем лишней);*

(6) $\omega_E(s) \equiv 0$ *тогда и только тогда, когда* E *содержит нулевую строку (в этом случае полагаем* $\deg \omega_E = -1$*);*

(7) *если* E *непусто, т. е. содержит хотя бы одну строку, то* $\deg \omega_E < m$; *размерностный многочлен "пустой" матрицы равен* $\binom{t+m}{m}$;

(8) *если* E *содержит строку* $(1, 0, \ldots, 0)$, *то* $\omega_E = \omega_{E_1}$, *где* $E_1 \subseteq \mathbb{N}^{m-1}$ *— матрица, полученная из* E *удалением сначала строк, первая координата которых больше 0, а затем первого столбца (состоящего из нулей). В частности, если* E *содержит строку* $(1, 0, \ldots, 0)$ *и в первом столбце имеется нулевой элемент, то* $\deg \omega_E < m - 1$;

(9) *если* $n > 1$ *и* $\mathbf{r} = (r_1, \ldots, r_m)$, *где* $r_j = \min_{i=1}^{n} e_{ij}$ $(1 \leqslant j \leqslant m)$, *то*

$$\omega_E(s) = \binom{s+m}{m} - \binom{s+m-|\mathbf{r}|}{m} + \omega_H(s - |\mathbf{r}|),$$

где H *—* $n \times m$*-матрица, полученная вычитанием вектора* $(r_1, \ldots, r_m)$ *из каждой строки матрицы* E *(в частности, каждый столбец матрицы* H *содержит 0).*

Фиксируем $n \times m$-матрицу E со строками $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Для вычисления $\omega_E(t)$ можно применить соотношение (12.3), выбирая строки матрицы E случайным образом; эта процедура приводит к комбинаторной формуле (12.4), дающей явное выражение для $\omega_E(t)$.

Для более точной формулировки введем некоторые обозначения. Пусть $\mathbf{f}_1 = (f_{11}, \ldots, f_{1m}), \ldots, \mathbf{f}_q = (f_{q1}, \ldots, f_{qm})$ элементы множества

$\mathbb{N}^m$. Тогда элемент $\mathbf{f} = (f_1, \dots, f_m) \in \mathbb{N}^m$, где $f_j = \max_{1 \leqslant i \leqslant q}\{f_{ij}\}$ $(1 \leqslant j \leqslant m)$ называется *наименьшим общим кратным* элементов $\mathbf{f}_1, \dots, \mathbf{f}_q$ и обозначается $\mathrm{НОК}(\mathbf{f}_1, \dots, \mathbf{f}_q)$. Для любых $l, n \in \mathbb{N}$, таких, что $n \geqslant 1$, $0 \leqslant l \leqslant n$, обозначим через $A(l, n)$ множество всех l-элементных подмножеств множества $\mathbb{N}_n = \{1, \dots, n\}$, и для любого $\xi \in A(l, n)$ положим $E_\xi = \{\mathbf{e}_j \mid j \in \xi\}$. Далее, обозначим $\mathbf{e}_\xi$ наименьшее общее кратное элементов множества E_ξ (как и прежде, элементы множества $\mathbb{N}^m$ сравниваются относительно порядка произведения "$\leqslant$", если противное не оговорено явно). Если $\xi = \emptyset$, то $\mathbf{e}_\xi = (0, \dots, 0)$; если $\xi \neq \emptyset$, то, очевидно, $\mathbf{e}_\xi = (e_{\xi 1}, \dots, e_{\xi m})$, где $e_{\xi i} = \max_{j \in \xi}\{e_{ji}\}$ $(i = 1, \dots, m)$. Пусть $|\mathbf{e}_\xi| = \sum\limits_{i=1}^{m} e_{\xi i}$.

12.9. Предложение. *В обозначениях, введенных выше, следующее соотношение имеет место*

$$\omega_E(t) = \sum_{l=0}^{n} (-1)^l \sum_{\xi \in A(l,n)} \binom{t + m - |\mathbf{e}_\xi|}{m}. \tag{12.4}$$

Доказательство. Воспользуемся индукцией по n. Случай $n = 0$ следует из теоремы 12.8.

Если $n > 0$, то по формуле (12.3) имеем

$$\omega_E(t) = \omega_{E_1}(t) - \omega_H(t - r),$$

где E_1 обозначает $(n-1) \times m$-матрицу, полученную из E удалением последней строки, $r = \sum\limits_{k=1}^{m} e_{nk}$, и $H = (h_{ij})$, где $h_{ij} = \max(e_{ij} - e_{nj}, 0)$, $i = 1, \dots, n-1$, $j = 1, \dots, m$. По предположению индукции

$$\omega_{E_1}(t) = \sum_{l=0}^{n-1} (-1)^l \sum_{\xi \in A(l,n-1)} \binom{t + m - |\mathbf{e}_\xi|}{m}$$

и

$$\omega_H(t - r) = \sum_{l=0}^{n-1} (-1)^l \sum_{\xi \in A(l,n-1)} \binom{t + m - |g_\xi|}{m},$$

где

$$\begin{aligned} |g_\xi| &= \sum_{k=1}^{m} \max_{i \in \xi} h_{ik} + r = \sum_{k=1}^{m} \left(\max_{i \in \xi} \max(e_{ik} - e_{nk}, 0) + e_{nk} \right) \\ &= \sum_{k=1}^{m} \max_{i \in \xi} (e_{ik}, e_{nk}) = |\mathbf{e}_{\xi \cup n}|. \end{aligned}$$

следовательно,

$$\begin{aligned}\omega_E(t) &= \sum_{l=0}^{n-1}(-1)^l \sum_{\xi\in A(l,n-1)} \binom{t+m-|\mathbf{e}_\xi|}{m} \\ &\quad + \sum_{l=0}^{n}(-1)^l \sum_{\xi\in A(l-1,n-1)} \binom{t+m-|\mathbf{e}_{\xi\cup n}|}{m} \\ &= \sum_{l=0}^{n}(-1)^l \sum_{\xi\in A(l,n)} \binom{t+m-|\mathbf{e}_\xi|}{m}. \qquad \square\end{aligned}$$

Предложение 12.9, в частности, означает, что многочлен Гильберта множества E представляется в виде

$$\omega_E(t) = \sum_{l=0}^{n}(-1)^l \sum_{\xi\in A(l,n)} \binom{t+m-\sum_{k=1}^{m} e_{\xi k}}{m}. \tag{12.5}$$

13. Алгоритмы вычисления размерностных многочленов

В предыдущем параграфе (см. замечание 12.7) мы отмечали, что размерностный многочлен любого множества $F \subseteq \mathbb{N}^m$ равен размерностному многочлену, ассоциированному с множеством всех минимальных элементов множества F. Значит, достаточно уметь вычислять размерностные многочлены только для конечных множеств $F \subseteq \mathbb{N}^m$ (более того, можно предполагать, что элементы множества F попарно несравнимы относительно порядка произведения).

Пусть $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ обозначает $n\times m$-матрицу над $\mathbb{N}$, т. е. матрицу с n строками и m столбцами, элементы которой — неотрицательные целые числа. Рассматривая строки матрицы E как элементы множества $\mathbb{N}^m$ и обозначая i-ю строку $(e_{i1},\ldots,e_{im})$ через $\mathbf{e}_i$ $(1\leqslant i\leqslant n)$, мы получим подмножество $\tilde{E}=\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}\subseteq\mathbb{N}^m$, ассоциированное с E. Напомним, что размерностный многочлен $n\times m$-матрицы E в точности совпадает с размерностным многочленом множества $\tilde{E}$ и называется многочленом Гильберта матрицы E.

Пусть $\omega_E(t)$ — размерностный многочлен $n\times m$-матрицы E над $\mathbb{N}$. По определению $\omega_E(s) = \operatorname{Card} V_E(s)$ для всех достаточно больших $s\in\mathbb{N}$, где V_E обозначает множество всех элементов из $\mathbb{N}^m\setminus\tilde{E}$, которые не превосходят ни одного элемента из $\tilde{E}$ относительно порядка произведения, так что $v\in V_E$ если и только если неравенство $\mathbf{e}_i\leqslant v$ не выполняется ни для одного $\mathbf{e}_i$ $(1\leqslant i\leqslant n)$.

Как было отмечено, для того, чтобы уметь вычислять размерностный многочлен любого подмножества в $\mathbb{N}^m$, достаточно уметь

вычислять его для любой $n\times m$-матрицы E над $\mathbb{N}$. Один из методов вычисления основан на формуле (12.4).

Пусть $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ обозначает $n\times m$-матрицу над $\mathbb{N}$. Воспользуемся следующими обозначениями, введенными в параграфе 12:

$$\mathbf{e}_\xi = \begin{cases} (0,\dots,0) & \text{если } \xi = \emptyset,\\ (e_1 = \max_{i\in\xi}\{e_{i1}\},\dots,e_m = \max_{i\in\xi}\{e_{im}\}) & \text{если } \xi \neq \emptyset \end{cases}$$

для любого подмножества $\xi \subseteq \mathbb{N}_n$ и $|\mathbf{e}_\xi| = \sum\limits_{j=1}^{m} e_j$. По предложению 12.9 (см. (12.4)) мы можем записать

$$\omega_E(t) = \binom{t+m}{m} + \sum_{l=1}^{n}(-1)^l \sum_{\xi\in A(l,n)} \binom{t+m-|\mathbf{e}_\xi|}{m},$$

где $A(l,n)$ $(1 \leqslant l \leqslant n)$ обозначает множество всех l-элементных подмножеств множества $\mathbb{N}_n = \{1,\dots,n\}$.

Пользуясь выписанной формулой, можно предложить следующий алгоритм вычисления размерностного многочлена $\omega_E(t)$, ассоциированного с $n\times m$-матрицей E.

А9. Алгоритм (E, n, m, ω).
Дано: $n \in \mathbb{N}$; $m \in \mathbb{N}$; $n\times m$-матрица E.
Надо: $\omega_E(t)$ — многочлен Гильберта матрицы E.
Переменные: IB — вектор типа $true/false$ с индексами $1..n$;
$\mathbf{v} = (v_1,\dots,v_m)$ — вектор типа $\mathbb{N}$ с индексами $1..m$;
S_1 — переменная типа ± 1;
S_2 — переменная типа $\mathbb{N}$.
Начало
$\omega(t) := \binom{t+m}{m}$
цикл для каждого вектора IB
  $\mathbf{v} := (0,\dots,0)$
  $S_1 := 1$
  цикл для j **от** 1 **до** n
    если $IB(j)$ **то**
      $\mathbf{v} := \text{НОК}\,(\mathbf{v}, \mathbf{e}_j)$
      $S_1 := -S_1$
    конец если
    $S_2 := v_1 + \dots + v_m$
    $\omega(t) := \omega(t) + S_1\binom{t+m-S_2}{m}$
  конец цикла
конец цикла
Конец

Легко видеть, что асимптотическая сложность алгоритма **A**9 имеет порядок $n \times 2^n$, где n — число строк матрицы E (по теореме 12.8 мы можем считать, что строки попарно несравнимы относительно порядка произведения на $\mathbb{N}^m$).

Мора и Мёллер модифицировали алгоритм вычисления многочлена Гильберта [**27**]. Их алгоритм основан на следующих соображениях. Легко видеть, что в формуле (12.5) может выполняться равенство $\mathbf{e}_\xi = \mathbf{e}_\theta$ для двух различных подмножеств ξ и θ множества $\mathbb{N}_n$, таких, что $\operatorname{Card}\xi$ и $\operatorname{Card}\theta$ являются четным и нечетным числами соответственно (мы пользуемся обозначениями предложения 12.9). Тогда соответствующие слагаемые в формуле (12.5) сократятся. Более того, можно сгруппировать все слагаемые, соответствующие одному и тому же элементу $\tau \in \mathbb{N}^m$.

Пусть $T = T(E)$ — множество всех элементов $\tau \in \mathbb{N}^m$, которые равны, по крайней мере, одному из элементов $\mathbf{e}_\xi$, где $\xi \subseteq \mathbb{N}_n$. Тогда из формулы (12.4) следует, что

$$\omega_E(t) = \sum_{\tau\in T}\sum_{k=0}^{n}(-1)^k \sum_{\{\xi\in A(k,n)\mid \mathbf{e}_\xi=\tau\}} \binom{t+m-|\tau|}{m} = \sum_{\tau\in T}\mu_\tau\binom{t+m-|\tau|}{m}, \quad (13.1)$$

где $|\tau|$ обозначает сумму всех координат вектора τ, и

$$\mu_\tau = \sum_{k=0}^{n}\sum_{\substack{\xi\in A(k,n)\\ \mathbf{e}_\xi=\tau}}(-1)^k. \quad (13.2)$$

Очевидно, если матрица E_1 получена присоединением строки $\mathbf{e} = (e_1, \ldots, e_m)$ к матрице E, $T_1 = T(E_1)$ и $\{\mu'_\tau \mid \tau \in T_1\}$ — множество коэффициентов (13.2) в соотношении (13.1) для многочлена $\omega_{E_1}(t)$, так что

$$\mu'_\tau = \sum_{k=0}^{n+1}\sum_{\substack{\xi\in A(k,n+1)\\ \mathbf{e}_\xi=\tau}}(-1)^k$$

для каждого $\tau \in T_1$, то

$$\mu'_\tau = \begin{cases} \mu_\tau - \sum_{\{\mathbf{u}\in T\mid \mathrm{HOK}(\mathbf{u},\mathbf{e})=\tau\}}\mu_{\mathbf{u}} & \text{если } \tau \in T \\ -\sum_{\{\mathbf{u}\in T\mid \mathrm{HOK}(\mathbf{u},\mathbf{e})=\tau\}}\mu_{\mathbf{u}} & \text{если } \tau \in T_1 \setminus T \end{cases} \quad (13.3)$$

Таким образом, вычисление многочлена $\omega_E(t)$, т. е. вычисление коэффициентов μ_τ ($\tau \in T$), в (13.1) может быть основано на формуле (13.3), если мы начнем с пустой матрицы (число строк которой равно нулю и многочлен Гильберта которой равен $\binom{t+m}{m}$) и последовательно будем присоединять строки матрицы E, вычисляя множество T и коэффициенты μ_τ ($\tau \in T$) на каждом шаге (см. алгоритм **А**10).

А10. Алгоритм (E, n, m, ω).
Дано: $n \in \mathbb{N}$; $m \in \mathbb{N}$; $n \times m$-матрица E.
Надо: $\omega_E(t)$ — многочлен Гильберта матрицы E.
Переменные: T, T_1 — множества типа
{вектор типа $\mathbb{N}$ с индексами $1..m$};
μ, μ_1 — векторы типа $\mathbb{Z}$ с индексами из T, T_1.

Начало
$\omega := 0$
$T := \{(0, \ldots, 0)\}$
$\mu(0, \ldots, 0) := 1$
цикл для i **от** 1 **до** n
  $T_1 := T$
  цикл для каждого $\mathbf{u} \in T_1$
    $\mu_1(\mathbf{u}) := \mu(\mathbf{u})$
  конец цикла
  цикл для каждого $\mathbf{u} \in T_1$
    $\tau :=$ НОК $(\mathbf{u}, \mathbf{e}_i)$, $\mathbf{e}_i$ — i-я строка матрицы E
    если $\tau \in T$ **то**
      $\mu(\tau) := \mu(\tau) - \mu_1(\mathbf{u})$
    иначе $T := T \cup \tau$; $\mu(\tau) := -\mu_1(\mathbf{u})$
    конец если
  конец цикла
конец цикла
цикл для каждого $\mathbf{u} \in T$
  $\omega(t) := \omega(t) + \mu(\mathbf{u})\binom{t+m-|\mathbf{u}|}{m}$
конец цикла
Конец

Поскольку на k-м шаге ($1 \leqslant k \leqslant n$) алгоритма каждый элемент $\mathbf{u} \in T_1$ является наименьшим общим кратным некоторого подмножества множества $\{\mathbf{e}_1, \ldots, \mathbf{e}_{k-1}\}$ (т. е. $\mathbf{u} = \mathbf{e}_\xi$ для некоторого $\xi \subseteq \mathbb{N}_{k-1}$), существует не более $(k-1)$ различных возможностей для выбора каждой координаты вектора $\mathbf{u}$, следовательно, на k-м

шаге ($1 \leqslant k \leqslant n$) множество T_1 содержит не более $(k-1)^m$ элементов. Вычисление всех элементов $\tau = \mathrm{НОК}\,(\mathbf{u}, \mathbf{e}_k)$ требует не более $m(k-1)^m$ сравнений, и можно предполагать (используя достаточно эффективный метод сортировки), что число проверок на принадлежность $\tau \in T$ не превосходит $k^m \log k$ для всех достаточно больших $k \in \mathbb{N}$. Таким образом, асимптотическая сложность (по n) алгоритма **A**10 не превосходит $m \sum\limits_{k=2}^{n} [(k-1)^m + k^m \log k]$. Поскольку $m \sum\limits_{k=2}^{n} [(k-1)^m + k^m \log k] < 2m \sum\limits_{k=2}^{n} k^m \log k$, асимптотическая сложность имеет порядок $n^{m+1} \log n$.

Следующие алгоритмы вычисления размерностного многочлена произвольной $n \times m$-матрицы E сводят эту задачу к аналогичной задаче для матрицы с числом строк меньшим, чем в E. По одному из этих алгоритмов (см. ниже алгоритм **A**11) можно вычислить коэффициенты μ_τ в (13.1) размерностного многочлена $\omega_E(t)$, что дает выражение для размерностного многочлена. Для обоснования этого алгоритма нам нужны некоторые свойства коэффициентов μ_τ, которые сформулированы ниже в леммах 13.1–13.5, 13.7 и 13.9. Последняя из этих лемм устанавливает соотношения, на которых основан алгоритм вычисления μ_τ.

Чтобы подчеркнуть зависимость коэффициентов μ_τ от матрицы E, будем обозначать эти коэффициенты $\mu_\tau(E)$ и продолжим это обозначение на случай произвольного вектора $\tau \in \mathbb{N}^m$, полагая

$$\mu_\tau(E) = \begin{cases} \mu_\tau, & \text{если } \tau \in T \\ 0, & \text{если } \tau \in \mathbb{N}^m \setminus T. \end{cases}$$

(Напомним, что $T = T(E)$ — множество всех элементов $\tau \in \mathbb{N}^m$, таких, что каждый τ равен либо $(0, \ldots, 0)$, либо наименьшему общему кратному некоторых строк матрицы E; элементы множества T будем называть *допустимыми элементами* или *допустимыми векторами* матрицы E.)

13.1. Лемма. *Пусть дана $n \times m$-матрица $E = (e_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$. Предположим, что элемент $\tau = (\tau_1, \ldots, \tau_m) \in \mathbb{N}^m$ мажорирует все строки этой матрицы, т. е. τ больше любой строки матрицы E или равен ей (относительно порядка произведений на $\mathbb{N}^m$). Тогда $\mu_\tau(E) = \mu_{(1,\ldots,1)}(H)$, где $H = (h_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ — матрица с элементами*

$$h_{ij} = \begin{cases} 1, & \textit{если } e_{ij} = \tau_j, \\ 0, & \textit{если } e_{ij} \neq \tau_j, \end{cases} \quad (i = 1, \ldots, n).$$

Доказательство. Пусть $\xi = \{i_1, \dots, i_k\} \in A(k,n)$ $(1 \leqslant k \leqslant n)$, $\mathbf{e}_\xi = \text{НОК}\{\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_k}\}$ и $\mathbf{h}_\xi = \text{НОК}\{\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_k}\}$ ($\mathbf{e}_i$ и $\mathbf{h}_i$ обозначают i-е строки матриц E и H соответственно). Покажем, что равенство $\mathbf{e}_\xi = \tau$ эквивалентно равенству $\mathbf{h}_\xi = (1, \dots, 1)$. Действительно, если $\mathbf{e}_\xi = \tau$, то $\tau_j = \max\{e_{i_1 j}, \dots, e_{i_k j}\}$ $(1 \leqslant j \leqslant m)$, так что для каждого $j = 1, \dots, m$ существует индекс $\lambda(j) \in \mathbb{N}_k$, такой, что $h_{i_{\lambda(j)}} = 1$. Таким образом, j-й элемент строки $\mathbf{h}_{i_{\lambda(j)}}$ равен 1, следовательно, $\mathbf{h}_\xi = \text{НОК}\{\mathbf{h}_{i_1}, \dots, \mathbf{h}_{i_k}\} = (1, \dots, 1)$. Обратно, если $\mathbf{h}_\xi = (1, \dots, 1)$, то для каждого $j = 1, \dots, m$ существует число $\nu = \nu(j) \in \mathbb{N}_k$, такое, что $h_{i_\nu j} = \max_{i \in \xi}\{h_{ij}\} = 1$, т. е. $e_{i_\nu j} = \tau_j$. Поэтому, $\mathbf{e}_\xi \geqslant \tau$, следовательно, $\mathbf{e}_\xi = \tau$ (так как элемент τ больше любой строки матрицы E или равен ей). Таким образом,

$$\mu_\tau = \sum_{k=0}^{n} \sum_{\substack{\xi \in A(k,n) \\ \mathbf{e}_\xi = \tau}} (-1)^k = \sum_{k=0}^{n} \sum_{\substack{\xi \in A(k,n) \\ \mathbf{h}_\xi = (1,\dots,1)}} (-1)^k = \mu_{(1,\dots,1)}(H). \qquad \square$$

Рассмотрим свойства размерностных многочленов матриц, состоящих из 0 и 1 (такова, например, матрица H в лемме 13.1). Для краткости будем писать $\mu_1(E)$ вместо $\mu_{(1,\dots,1)}(E)$, где E — $n \times m$-матрица и $(1, \dots, 1) \in \mathbb{N}^m$.

13.2. Лемма. *Пусть E — $n \times m$-матрица, состоящая из 0 и 1, и $\omega_E(t)$ — ее многочлен Гильберта. Тогда $\mu_1(E) = (-1)^m \omega_E(-1)$.*

Доказательство. По (12.4) имеем

$$\omega_E(t) = \sum_{\tau \in T} \mu_\tau \binom{t + m - |\tau|}{m}, \tag{13.4}$$

и, очевидно, каждая координата любого вектора $\tau = (\tau_1, \dots, \tau_m) \in$ $\in T = T(E)$ равна либо 0, либо 1. Если $\tau \neq (1, \dots, 1)$, то $0 \leqslant |\tau| = \sum_{i=1}^{m} \tau_i < m$. В этом случае многочлен $\binom{t+m-|\tau|}{m}$ обращается в нуль при $t = -1$, следовательно,

$$\begin{aligned} \omega_E(-1) &= \mu_1(E) \left.\binom{t + m - |\tau|}{m}\right|_{t=-1} \\ &= \mu_1(E) \left.\frac{t(t-1)\dots(t-m+1)}{m!}\right|_{t=-1} \\ &= (-1)^m \mu_1(E). \end{aligned}$$

$\square$

Из леммы 13.2 следует, что

$$\mu_1(E) = (-1)^m \omega_E(-1), \tag{13.5}$$

где $\omega_E(t)$ — многочлен Гильберта матрицы E. Если

$$\omega_E(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i} \quad (a_0, a_1, \ldots, a_m \in \mathbb{Z}),$$

то $\omega_E(-1) = a_0$, так что $\mu_1(E)$ равно свободному члену многочлена Гильберта $\omega_E(t)$.

13.3. Лемма. *Пусть E — $n \times m$-матрица, состоящая из 0 и 1. Тогда*

(1) *если E содержит нулевую строку, то $\mu_1(E) = 0$;*
(2) *если E содержит нулевой столбец, то $\mu_1(E) = 0$;*
(3) *значение $\mu_1(E)$ инвариантно относительно перестановки строк (или столбцов) матрицы E;*
(4) *если E состоит из одной строки $(1, \ldots, 1)$, то $\mu_1(E) = -1$;*
(5) *если первая строка матрицы E равна $(1, 0, \ldots, 0)$ и первые элементы остальных строк равны 0, то $\mu_1(E) = -\mu_1(H)$, где матрица H получена из E удалением первой строки и первого столбца.*

Доказательство. Все утверждения леммы следуют из (13.5) и из доказанных выше свойств размерностного многочлена матрицы E.

(1) Если E содержит нулевую строку, то $\omega_E(t) \equiv 0$ (см. теорему 12.8(6). Применяя лемму 13.2, получаем $\mu_1(E) = 0$.

(2) Если каждый элемент ν-го столбца матрицы E равен нулю $(1 \leqslant \nu \leqslant m)$, то из формулы (13.2) следует, что $\mu_1(E) = 0$ (действительно, в обозначениях формулы (13.2) ν-ая координата любого вектора $\mathbf{e}_\xi$ $(\xi \subseteq \mathbb{N}_m)$ равна нулю, так что $\mathbf{e}_\xi \neq (1, \ldots, 1)$ ни для какого подмножества $\xi \subseteq \mathbb{N}_m$).

(3) Очевидно, что перестановка строк (или столбцов) матрицы E не меняет значения $\omega_E(t)$, а, значит, и значения $\mu_1(E) = (-1)^m \omega_E(-1)$ (см. утверждения (3) и (4) теоремы 12.8).

(4) Пусть E состоит из одной строки $\mathbf{e} = (1, \ldots, 1)$. Поскольку

$$\begin{aligned} V_{\mathbf{e}}(s) &= \operatorname{Card} \mathbb{N}^m(s) \\ &\quad - \operatorname{Card}\{(1+u_1, \ldots, 1+u_m) \mid (u_1, \ldots, u_m) \in \mathbb{N}^m(s-m)\} \\ &= \binom{s+m}{m} - \binom{s}{m} \end{aligned}$$

для всех достаточно больших $s \in \mathbb{N}$, имеем

$$\omega_E(t) = \binom{t+m}{m} - \binom{t}{m} = \frac{(t+1)\dots(t+m)}{m!} - \frac{t(t-1)\dots(t-m+1)}{m!}.$$

Значит, $\mu_1(E) = (-1)^m \omega_E(-1) = (-1)^m (-1)^{m+1} = -1$.

(5) По теореме 12.8(8) имеем $\omega_E(t) \equiv \omega_H(t)$, следовательно, $\mu_1(E) = (-1)^m \omega_E(-1) = -(-1)^{m-1} \omega_H(-1) = -\mu_1(H)$. □

Пусть $E = (e_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ — $n \times m$-матрица над $\mathbb{N}$, $\tilde{E} = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ — множество строк матрицы E и $\mathbf{e} = (e_1, \dots, e_m)$ — элемент множества $\mathbb{N}^m$. Пусть $E \cup \mathbf{e}$ обозначает $(n+1) \times m$-матрицу, полученную присоединением строки $\mathbf{e}$ к матрице E (без потери общности можно предполагать, что $\mathbf{e}$ является $(n+1)$-й строкой матрицы $E \cup \mathbf{e}$). Следующая лемма устанавливает связь между размерностными многочленами матриц E и $E \cup \mathbf{e}$. Как и выше, $|E|$ обозначает сумму $\sum\limits_{i=1}^{n} \sum\limits_{j=1}^{m} e_{ij}$ всех элементов матрицы E (в частности, $|\mathbf{e}|$ обозначает сумму всех координат элемента $\mathbf{e} \in \mathbb{N}^m$).

13.4. Лемма. *Пусть E является $n \times m$-матрицей ($n, m \in \mathbb{N}$; $m > 1$, $n \geqslant 1$), состоящей из нулей и единиц. Если первый столбец матрицы E состоит только из нулей, а матрица E_1 получена из E удалением этого нулевого столбца, то $\omega_E(-2) = -\omega_{E_1}(-1)$.*

Доказательство. Применяя формулу (12.2) к матрице E и вектору $\mathbf{e} = (1, 0, \dots, 0)$, получим $\omega_E(t) = \omega_{E \cup \mathbf{e}}(t) + \omega_H(t-1)$, где $H = (h_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ — матрица с элементами $h_{ij} = \max\{e_{ij} - e_j, 0\}$ ($e_1 = 1$, $e_2 = 0, \dots, e_m = 0$ суть координаты вектора $\mathbf{e}$). Очевидно, $H = E$ и $\omega_{E \cup \mathbf{e}}(t) = \omega_{E_1}(t)$ (см. теорему 12.8(8)), так что $\omega_E(t) = \omega_{E_1}(t) + \omega_E(t-1)$ и, в частности, $\omega_{E_1}(-1) + \omega_E(-2) = \omega_E(-1)$. Поскольку E содержит нулевой столбец, из леммы 13.3(2) следует, что $\omega_E(-1) = (-1)^m \mu_1(E) = 0$, значит, $\omega_E(-2) = -\omega_{E_1}(-1)$. □

13.5. Лемма. *Пусть $E = (e_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ ($n, m \in \mathbb{N}$; $m > 1$, $n \geqslant 1$) является $n \times m$-матрицей состоящей из нулей и единиц. Предположим, что $e_{j1} = 1$ для $j = 1, \dots, r$ и $e_{j1} = 0$ для $j = r+1, \dots, n$ ($1 \leqslant r \leqslant n$). Тогда $\mu_1(E) = \mu_1(E_1) - \mu_1(E_2)$, где матрица E_1 получена из E удалением первого столбца, а E_2 получена из E_1 удалением r первых строк.*

Доказательство. Применяя (12.2) к E и $\mathbf{e}=(1,0,\dots,0)$, получаем $\omega_E(t)=\omega_{E\cup\mathbf{e}}(t)+\omega_H(t-1)$, где $H=(h_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$-матрица с элементами $h_{ij}=\max\{e_{ij}-e_j,0\}=\begin{cases}0, & \text{если } j=1,\\ e_{ij}, & \text{если } j\neq 1.\end{cases}$ По теореме 12.8(8) $\omega_{E\cup\mathbf{e}}(t)=\omega_{E_2}(t)$, следовательно, $\omega_E(t)=\omega_{E_2}(t)+\omega_H(t-1)$. Далее, пользуясь леммой 13.4, можно написать $\omega_H(-2)=-\omega_{E_1}(-1)$, значит, $\omega_E(-1)=\omega_{E_2}(-1)-\omega_{E_1}(-1)$. Теперь, по лемме 13.2 имеем

$$\mu_1(E)=(-1)^m\omega_E(-1)=(-1)^m\omega_{E_2}(-1)+(-1)^{m-1}\omega_{E_1}(-1)$$
$$=\mu_1(E_1)-\mu_1(E_2).\quad\square$$

13.6. Следствие. *Пусть $E=(e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ $(m,n\in\mathbb{N},\ m>1)$ — $n\times m$-матрица, состоящая из 0 и 1. Предположим, что существуют $p,q\in\mathbb{N}_m$, такие, что $e_{ip}\geqslant e_{iq}$ для всех $i=1,\dots,n$. Тогда $\mu_1(E)=\mu_1(E_1)$, где E_1 получена из E удалением p-го столбца.*

Доказательство. Поскольку размерностный многочлен матрицы E инвариантен относительно перестановок строк (или столбцов) матрицы E, значение $\mu_1(E)=(-1)^m\omega_E(-1)$ также обладает этим свойством. Поэтому, без потери общности, можно считать, что $p=1$ и существует $r\in\mathbb{N}_{n-1}$, такое, что $e_{j1}=1$ для $j=1,\dots,r$, и $e_{j1}=0$ для $j=r+1,\dots,n$. По лемме 13.5, $\mu_1(E)=\mu_1(E_1)-\mu_1(E_2)$, где E_2 получена из E удалением первого столбца и r первых строк (поскольку $0\leqslant e_{iq}\leqslant e_{i1}=0$ для $i=r+1,\dots,n$, каждый элемент q-го столбца матрицы E_2 равен нулю). Следовательно, $\mu_1(E_2)=0$ (см. лемму 13.3(2)), так что $\mu_1(E)=\mu_1(E_1)$. $\square$

13.7. Лемма. *Пусть $E=(e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ $(m,n\in\mathbb{N},\ m>1)$ — $n\times m$-матрица, состоящая из 0 и 1. Предположим, что E содержит строку $\mathbf{e}=(e_1,\dots,e_m)$, такую, что $e_i=1$ для $1\leqslant i\leqslant r$ и $e_i=0$ для $r<i\leqslant m$ $(r\in\mathbb{N}_{m-1})$. Тогда $\mu_1(E)=\mu_1(E\setminus\mathbf{e})-\mu_1(E_1)$, где матрица $E\setminus\mathbf{e}$ получена удалением строки $\mathbf{e}$ из матрицы E, а $(n-1)\times(m-r)$-матрица E_1 получена из матрицы $E\setminus\mathbf{e}$ удалением r первых столбцов.*

Доказательство. Применяя формулу (12.3) к матрице E и строке $\mathbf{e}=(1,\dots,1,0,\dots,0)$, получаем $\omega_E(t)=\omega_{E\setminus\mathbf{e}}(t)-\omega_{\tilde{E}_1}(t-r)$, где матрица $\tilde{E}_1$ получена из E_1 присоединением слева r нулевых

столбцов. Теперь из (12.2) видно, что $\omega_{\tilde{E}_1}(t) = \omega_{\tilde{E}_1\cup\mathbf{e}}(t) + \omega_{\tilde{E}_1}(t-r)$, следовательно,

$$\omega_E(-1) = \omega_{E\setminus\mathbf{e}}(-1) - \omega_{\tilde{E}_1}(-1-r) = \omega_{E\setminus\mathbf{e}}(-1) + \omega_{\tilde{E}_1\cup\mathbf{e}}(-1) - \omega_{\tilde{E}_1}(-1).$$

Поскольку $\tilde{E}_1$ содержит нулевой столбец, из пункта 2 леммы 13.3 следует, что $\mu_1(\tilde{E}_1) = 0$, значит,

$$\omega_{\tilde{E}_1}(-1) = (-1)^m \mu_1(\tilde{E}_1) = 0$$

(см. лемму 13.2) и

$$\begin{aligned}\mu_1(E) &= (-1)^m \omega_E(-1) = (-1)^m \omega_{E\setminus\mathbf{e}}(-1) + (-1)^m \omega_{\tilde{E}_1\cup\mathbf{e}}(-1)\\ &= \mu_1(E\setminus\mathbf{e}) + \mu_1(\tilde{E}_1\cup\mathbf{e}).\end{aligned}$$

Поскольку каждый из первых $(r-1)$ столбцов матрицы $\tilde{E}_1\cup\mathbf{e}$ мажорирует r-й столбец этой матрицы, из следствия 13.6 вытекает, что $\mu_1(\tilde{E}_1\cup\mathbf{e}) = \mu_1(\mathbf{0}E_1\cup(1,0,\ldots,0))$, где $\mathbf{0}E_1$ — матрица, полученная присоединением слева нулевого столбца к E_1. Применяя теперь п. 5 леммы 13.3, получаем $\mu_1(\mathbf{0}E_1\cup(1,0,\ldots,0)) = -\mu_1(E_1)$, откуда следует требуемое соотношение $\mu_1(E) = \mu_1(E\setminus\mathbf{e}) - \mu_1(E_1)$. □

Пусть $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$-матрица. По теореме 12.8 п. 5, удаление "лишних" строк матрицы E не меняет размерностный многочлен этой матрицы, значит, не меняет и значение $\mu_1(E)$. Кроме того, если любой элемент матрицы E равен либо 0, либо 1, то из следствия 13.6 вытекает, что удаление "лишних" столбцов матрицы E не меняет значения $\mu_1(E)$ (p-й столбец матрицы $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ $(1\leqslant p\leqslant m)$ называется "лишним", если существует число $q\in\mathbb{N}_m$, такое, что $q\neq p$ и $e_{ip}\geqslant e_{iq}$ для всех $i = 1,\ldots,n$).

Таким образом, в ходе вычисления $\mu_1(E)$ (где E — $n\times m$-матрица, состоящая из 0 и 1) мы можем прежде всего отбросить "лишние" строки и столбцы (по п. 5 леммы 13.3, эти вычисления сопровождаются соответствующими изменениями знака $\mu_1(E)$), а затем отбросить строки и столбцы, удовлетворяющие соотношениям леммы 13.5. Затем мы можем выбрать одну из следующих альтернатив: воспользоваться леммой 13.5 для вычисления $\mu_1(E_1)$ (где E_1 — матрица, полученная из E с помощью описанного выше процесса сокращения) или вычислить $\mu_1(E_1)$, воспользовавшись леммой 13.7, т. е. "раскладывая" E_1 по строкам и столбцам соответственно. Очевидно, что если число строк матрицы E_1 больше числа ее столбцов, то предпочтительнее "движение по столбцам" с помощью леммы 13.5, в противном случае для вычисления $\mu_1(E_1)$ целесообразно воспользоваться леммой 13.7.

13.8. Пример. Найдем значение $\mu_1(E)$ для матрицы

$$E = \begin{pmatrix} 0&0&1&1 \\ 0&1&0&1 \\ 0&1&1&0 \\ 1&0&0&1 \\ 1&0&1&0 \\ 1&1&0&0 \end{pmatrix}.$$

Применяя лемму 13.5, получаем $\mu_1(E) = \mu_1(E_1) - \mu_1(E_2)$, где $E_1 = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix}$, $E_2 = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \end{pmatrix}$. Легко видеть, что три первых строки матрицы E_1 являются "лишними", поэтому $\mu_1(E_1) = \mu_1\left(\begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix}\right) = -1$ (см. п. 5 леммы 13.3). Применяя еще раз лемму 13.5, получаем (в силу утверждений леммы 13.3), что $\mu_1(E_2) = \mu_1\left(\begin{pmatrix} 1&1 \\ 0&1 \\ 1&0 \end{pmatrix}\right) - \mu_1((1,1)) = 1+1 = 2$. Следовательно, $\mu_1(E) = \mu_1(E_1) - \mu_1(E_2) = -3$.

Другой метод вычисления $\mu_1(E)$ основан на лемме 13.7:

$$\begin{aligned} \mu_1(E) &= \mu_1\left(\begin{pmatrix} 0&1&0&1 \\ 0&1&1&0 \\ 1&0&0&1 \\ 1&0&1&0 \\ 1&1&0&0 \end{pmatrix}\right) - \mu_1\left(\begin{pmatrix} 0&1 \\ 0&1 \\ 1&0 \\ 1&0 \\ 1&1 \end{pmatrix}\right) \\ &= \mu_1\left(\begin{pmatrix} 0&1&1&0 \\ 1&0&0&1 \\ 1&0&1&0 \\ 1&1&0&0 \end{pmatrix}\right) - \mu_1\left(\begin{pmatrix} 0&1 \\ 1&0 \\ 1&0 \end{pmatrix}\right) - 1 \\ &= \mu_1\left(\begin{pmatrix} 1&0&0&1 \\ 1&0&1&0 \\ 1&1&0&0 \end{pmatrix}\right) - \mu_1\left(\begin{pmatrix} 1&1 \\ 1&0 \\ 1&0 \end{pmatrix}\right) - 2 \\ &= \mu_1\left(\begin{pmatrix} 1&0&1&0 \\ 1&1&0&0 \end{pmatrix}\right) - \mu_1\left(\begin{pmatrix} 0&1 \\ 1&0 \end{pmatrix}\right) - 2 = -3. \end{aligned}$$

В качестве следствия леммы 13.7 получаем следующее утверждение, на котором основан алгоритм вычисления размерностного многочлена матрицы (см. ниже алгоритм **A**11).

13.9. Лемма. *Пусть* $E = (e_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ *— $n\times m$-матрица над* $\mathbb{N}$ *и* $\tau = (\tau_1, \ldots, \tau_m) \in T = T(E)$ *(как и выше, $T(E)$ обозначает множество всех допустимых векторов матрицы E, т. е. множество всех элементов $\tau \in \mathbb{N}^m$, равных либо $(0, \ldots, 0)$, либо наименьшему общему кратному некоторых строк матрицы E). Пусть K — матрица, состоящая из всех тех строк матрицы E, которые мажорируются вектором τ (для определенности предположим, что строки матрицы K располагаются в том же порядке, в каком они расположены в матрице E). Кроме того, пусть $\mathbf{k} = (k_1, \ldots, k_m)$ — одна из строк матрицы K и $K \setminus \mathbf{k}$ — матрица, полученная удалением строки $\mathbf{k}$ из K. Тогда для любого подмножества $J = \{i_1, \ldots, i_l\}$ множества $\mathbb{N}_m$, такого, что*

$i_1 < \cdots < i_l$ $(1 \leqslant l \leqslant m)$, *имеем*

$$\mu_\tau(K, m) = \mu_\tau(K \setminus \mathbf{k}, m) - \mu_{\tau'}(K \setminus \mathbf{k}, J), \tag{13.6}$$

где $\mu_\tau(K, m)$, $\mu_\tau(K \setminus \mathbf{k}, m)$ *суть соответственно коэффициенты* μ_τ, *определенные формулой* (13.2) *для матриц* K *и* $K \setminus \mathbf{k}$, *а* $\mu_{\tau'}(K \setminus \mathbf{k}, J)$ — *аналогичные коэффициенты для вектора* $\tau' = (\tau_{i_1}, \ldots, \tau_{i_l}) \in \mathbb{N}^l$ *(вместо* τ*) и для* $(n-1)\times(m-l)$*-матрицы, полученной из* E *удалением столбцов с индексами* $j \in \mathbb{N}_m \setminus J$.

Доказательство. Без потери общности можно предположить, что $\mathbf{k}$ — первая строка матрицы K. Из леммы 13.1 следует, что $\mu_\tau(K, m) = \mu_1(H)$, где $H = (h_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ — $n \times m$-матрица с элементами $h_{ij} = \begin{cases} 1, & \text{если } e_{ij} = \tau_j, \\ 0, & \text{если } e_{ij} \neq \tau_j, \end{cases}$ $(i = 1, \ldots, n)$. Аналогично, $\mu_\tau(K \setminus \mathbf{k}, m) = \mu_1(H_1)$ и $\mu_{\tau'}(K \setminus \mathbf{k}, J) = \mu_1(H_2)$, где матрица H_1 получена из H отбрасыванием первой строки, а H_2 получена из H_1 отбрасыванием столбцов с индексами $i_1, \ldots, i_l$. Применяя теперь лемму 13.7, получаем соотношение $\mu_1(H) = \mu_1(H_1) - \mu_1(H_2)$, из которого следует требуемое утверждение. □

Вычисление коэффициентов μ_τ $(\tau \in T = T(E))$ в (13.4) для размерностного многочлена произвольной $n \times m$-матрицы E (а, значит, и вычисление самого размерностного многочлена) может быть выполнено по следующей схеме: сначала применяем (13.6) к матрице E (формируя матрицу K тех строк матрицы E, которые мажорируются вектором τ. Ясно, что коэффициенты μ_τ для матриц K и E совпадают). Затем вычисляем значения $\mu_\tau(K \setminus \mathbf{k}, m)$ и $\mu_{\tau'}(K \setminus \mathbf{k}, J)$, снова применяя (13.6) и т. д., пока не получим "пустые" матрицы (т. е. матрицы с нулевым числом строк).

А11. Алгоритм (E, n, m, T, μ).

Дано: $m \in \mathbb{N}$, $n \in \mathbb{N}$; E — $n \times m$-матрица

Надо: T — множество допустимых векторов матрицы E;
μ — вектор типа $\mathbb{Z}$ с индексами из T.

Переменные: J — множество типа $1..m$;
K — множество типа {вектор типа $\mathbb{N}$ с индексами $1..m$}.

Начало

сформировать множество T допустимых векторов

цикл для каждого $\tau \in T$

$\mu_\tau := 0$

$J := \{1, \ldots, m\}$

$K := \{\mathbf{e}_i \mid \mathbf{e}_i \leqslant \tau\}$ где $\mathbf{e}_i$ — строка матрицы E
$v_\tau := 1$
NEXTINDEX (J, K, v_τ, μ_τ)
конец цикла
Конец

Алгоритм NEXTINDEX (J, K, v_τ, μ_τ)

Дано: J — множество типа $1..m$
K — множество типа {вектор типа $\mathbb{N}$ с индексами $1..m$}.
v_τ — элемент типа ± 1
Надо: μ_τ — вектор типа $\mathbb{N}$ с индексами из T.
Глобальные переменные: $m \in \mathbb{N}$;
τ — вектор типа $\mathbb{N}$ с индексами $1..m$.
Начало
цикл для каждой строки $\mathbf{k} = \{k_1, \ldots, k_m\}$ матрицы K, такой, что $k_{i_1} = \tau_{i_1}$, где i_1 — первый элемент множества J
$K := K \setminus \mathbf{k}$
$v_\tau := -v_\tau$
$J' := \{j \in J \mid k_j = \tau_j\}$
$J = J \setminus J'$
выбор
$K = \emptyset \& J = \emptyset \implies \mu_\tau := \mu_\tau + v_\tau$
$K \neq \emptyset \& J \neq \emptyset \implies$ NEXTINDEX(J, K, v_τ, μ_τ)
конец выбора
$J := J \cup J'$
конец цикла
Конец

Чтобы оценить асимптотическую сложность алгоритма **A**11 для достаточно больших $n \in \mathbb{N}$, заметим, прежде всего, что при фиксированном векторе $\tau = (\tau_1, \ldots, \tau_m) \in T$ построение $K = K(\tau)$ требует не более mn сравнений чисел (на этом шаге мы запоминаем все пары $(k, j) \in \mathbb{N}_n \times \mathbb{N}_m$, для которых $e_{kj} = \tau_j$). Далее, выполнение элементарных операций для всех вызовов алгоритма NEXTINDEX (для фиксированного τ) требует не более $h_1 h_2 \ldots h_m$ сравнений, где $h_\nu = h_\nu(\tau)$ $(1 \leqslant \nu \leqslant m)$ обозначает число строк $\mathbf{k} = (k_1, \ldots, k_m)$ матрицы $K(\tau)$, таких, что $k_\nu = \tau_\nu$ для всех $\nu = 1, \ldots, m$. Легко видеть, что общее число операций для всех вызовов алгоритма NEXTINDEX (с точностью до постоянного множителя это число равно $\sum_{\tau \in T} h_1(\tau) \ldots h_m(\tau)$) не превосходит $\mathrm{Card}\{(a_1, \ldots, a_m) \in \mathbb{N}^m \mid$ для каждого $\nu \in \mathbb{N}_m$ существует $i = i(\nu) \in \mathbb{N}_n$, такое, что $a_\nu = e_{i\nu}\}$,

и это не превосходит n^m. Поэтому для достаточно больших $n \in \mathbb{N}$ асимптотическая сложность алгоритма **A**11 имеет порядок n^{m+1}.

Другой способ вычисления размерностного многочлена $\omega_E(t)$ для $n\times m$-матрицы E состоит в следующем. Для $n < m$ можно вычислять многочлен $\omega_E(t)$, пользуясь алгоритмом **A**9. Пусть $n \geqslant m$. В этом случае применяем к E соотношение (12.3), в котором $\mathbf{e}$ — строка с максимальным значением элемента в первом столбце матрицы E. (Тривиальные случаи: если $E = (0)$, то $\omega_E = 0$; если $n = 1$, применяем алгоритм **A**9.) Легко видеть, что число нулевых столбцов в матрице H (см. (12.3)) больше, чем в матрице E, и число строк в каждой из матриц $E \setminus \mathbf{e}$, K меньше чем в E. Затем применяем описанную процедуру к матрице $E \setminus \mathbf{e}$ и т. д., пока не получим матрицу, размерностный многочлен которой можно вычислить по алгоритму **A**9. В результате этого процесса мы получаем представление требуемого многочлена $\omega_E(t)$ в виде линейной комбинации многочленов $\omega_{\mathbf{e}}, \omega_{H_1}, \ldots, \omega_{H_{n-1}}$ (со сдвинутыми аргументами), таких, что каждая матрица H_i имеет ровно i строк и число ее нулевых столбцов на один больше, чем в E. Многочлен $\omega_{\mathbf{e}}$ и некоторые из многочленов ω_{H_i} вычисляются по алгоритму **A**9 (в тех случаях, когда этот алгоритм нужно применять в соответствии с вышеприведенными рассуждениями). Для вычисления остальных многочленов ω_{H_i} снова применяем соотношение (12.3) и продолжаем в том же духе. Заметим, что если первый столбец в матрице E нулевой и $m > 1$, то число операций в вычислении ω_E по предлагаемой схеме совпадает с числом операций при вычислении размерностного многочлена $n \times (m-1)$-матрицы. Кроме того, если E — $n\times 1$-матрица, то все ее строки кроме той, которая содержит элемент $\min_{1\leqslant i\leqslant n}\{e_{i1}\}$, являются лишними, так что вычисление размерностного многочлена по формуле $\omega_E = \min_{1\leqslant i\leqslant n}\{e_{i1}\}$ требует $(n-1)$ операцию. Таким образом, если $f(n,m)$ обозначает число элементарных операций (сложение, сравнение или умножение) необходимых для вычисления размерностного многочлена $\omega_E(t)$ матрицы E размера $n\times m$, то $f(n,m) \leqslant (n-1) + f(n-1,m) + f(n-1,m-1)$. Поскольку $f(n,1) = n-1$, имеем

$$\begin{aligned} f(n,2) &\leqslant 2(n-1) + f(n-1,2) \\ &\leqslant 2((n-1)+(n-2)) + f(n-2,2) \leqslant \ldots \\ &\leqslant 2((n-1)+(n-2)+\cdots+1) = \frac{n(n-1)}{2}\cdot 2 \leqslant n^2; \end{aligned}$$

$$f(n,3) \leqslant n^2 + (n-1)^2 + \cdots + 1 \leqslant n^3;$$

$$\vdots$$

$$f(n,k) \leqslant n^{k-1} + (n-1)^{k-1} + \cdots + 1 \leqslant n^k$$

и т. д. Поэтому алгоритм вычисления размерностного многочлена, основанный на приведенной схеме (см. алгоритм **А**12), имеет асимптотическую сложность $O(n^m)$.

А12. Алгоритм (E, n, m, ω).

Дано: $n \in \mathbb{N}$; $m \in \mathbb{N}$; $n \times m$-матрица E.

Надо: $\omega(t) = \omega_E(t)$ — многочлен Гильберта матрицы E.

Пер.: $h \in \mathbb{N}$
J — множество элементов типа $1..m$;
$\mathbf{e}$ — вектор типа $\mathbb{N}$ с индексами $1..m$;
F — матрица типа $\mathbb{N}$, число столбцов которой не более m, а число строк — не более n.

Начало
$h := n$
$F := E$
если $h \leqslant m$ **то**
    Алгоритм **А**9(E, n, m, ω)
иначе
    $J := \{$ненулевые столбцы $F\}$
    если $J = \emptyset$ **то** $\omega(t) := 0$
    иначе если $\operatorname{Card} J = 1$ **то**
        $c :=$ минимальный элемент столбца $j \in J$
        $\omega := \binom{t+m}{m} - \binom{t+m-c}{m}$
    иначе
        $j := \{$первый элемент множества $J\}$
        $\mathbf{e} := \{$первая строка матрицы F с минимальным элементом в j-м столбце$\}$
        $F := F \setminus \mathbf{e}$
        Алгоритм **А**12 $(F, h-1, m, \omega)$
        $v(t) := \omega(t)$
        $F := \{\mathbf{f} \dot{-} \mathbf{e} \mid \mathbf{f}$ — строка матрицы F, $\mathbf{f} \neq \mathbf{e}\}$
        Алгоритм **А**12 $(F, h-1, m, \omega)$
        $\omega(t) := v(t) - \omega(t - |\mathbf{e}|)$
    конец если
конец если
Конец

Символ $\dot{-}$, которым мы пользуемся в алгоритме **A**12, обозначает следующую операцию на векторах:

$$(a_1, \ldots, a_m)\dot{-}(b_1, \ldots, b_m) = (c_1, \ldots, c_m),$$

где $c_i = \max(a_i - b_i, 0)$ для всех $i = 1, \ldots, m$. При этом, если $m > 2$, то e_i $(1 \leqslant i \leqslant m)$ обозначает i-ю координату элемента $\mathbf{e} \in \mathbb{N}^m$.

В заключение этого параграфа рассмотрим алгоритм вычисления размерностного многочлена, асимптотическая сложность которого меньше асимптотической сложности алгоритмов **A**9, **A**10, **A**11 и **A**12. Кроме того, представим алгоритм вычисления старшего коэффициента размерностного многочлена.

Пусть $\mathbb{Q}[t]$ — кольцо многочленов над полем рациональных чисел. Для каждого $s \in \mathbb{N}$ пусть Δ_s и Δ^{-1} обозначают операторы, действующие на $\mathbb{Q}[t]$ следующим образом:

$$\Delta_s(f(t)) = f(t) - f(t-s) \tag{13.7}$$

и если

$$f(t) = \sum_{i \in \mathbb{N}} a_i \binom{t+i}{i}$$

$(a_i \in \mathbb{Q})$ для всех $i \in \mathbb{N}$, то

$$\Delta^{-1} f(t) = \sum_{i \in \mathbb{N}} a_i \binom{t+1+i}{i+1}. \tag{13.7'}$$

Отметим, что операторы Δ_s и Δ^{-1} $(s \in \mathbb{N})$, удовлетворяют следующему тождеству:

$$\Delta_s \Delta^{-1} f(t) = f(t) + f(t-1) + \cdots + f(t-s+1). \tag{13.8}$$

В частности,

$$\Delta_1 \Delta^{-1} = \mathrm{id}_{\mathbb{Q}[t]}.$$

Действительно, пусть

$$f(t) = \sum_{i \in \mathbb{N}} a_i \binom{t+i}{i}$$

$a_i \in \mathbb{Q}$ для всех $i \in \mathbb{N}$, и $a_i = 0$ для почти всех $i \in \mathbb{N}$ и пусть $s \in \mathbb{N}$. По (11.4) имеем

$$\Delta_s \Delta^{-1} f(t) = \sum_{i \in \mathbb{N}} a_i \left[\binom{t+i+1}{i+1} - \binom{t+i+1-s}{i+1} \right]$$

$$= \sum_{i\in\mathbb{N}} a_i \sum_{r=0}^{s-1} \binom{t+i+1-s+r}{i} = \sum_{i\in\mathbb{N}} a_i \sum_{r=0}^{s-1} \binom{t+i-r}{i}$$

$$= \sum_{r=0}^{s-1} \sum_{i\in\mathbb{N}} a_i \binom{t+i-r}{i} = \sum_{r=0}^{s-1} f(t-r).$$

13.10. Лемма. *Пусть* $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$*-матрица над* $\mathbb{N}$, $k \in \mathbb{N}_m$ *и* $a = \min_{i=1}^{n}\{e_{ik} \mid e_{ik} \neq 0\}$. *Через* E_1 *обозначим матрицу, полученную из* E *удалением* k*-го столбца и всех строк с ненулевым элементом в* k*-м столбце. Далее, пусть* $H = (h_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$*-матрица с элементами*

$$h_{ij} = \begin{cases} \max(e_{ik}-a, 0), & \text{если } j = k \\ e_{ij}, & \text{если } j \neq k \end{cases} \quad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m).$$

Тогда

$$\omega_E(t) = \Delta_a \Delta^{-1} \omega_{E_1}(t) + \omega_H(t-a), \tag{13.9}$$

где $\omega_E(t)$, $\omega_H(t)$ *и* $\omega_{E_1}(t)$ — *размерностные многочлены матриц* E, H *и* E_1 *соответственно.*

В частности, если $E = \begin{pmatrix} k & 0\ldots 0 \\ 0 & \\ \vdots & E_1 \\ 0 & \end{pmatrix}$, *где* $e_{11} = k$, *а все остальные элементы первого столбца и первой строки равны нулю, то* $\omega_E(t) = \Delta_k \cdot \Delta^{-1}\omega_{E_1}(t)$.

Доказательство. Применяя формулу (12.2) к матрице E и вектору $(0,\ldots,0,a,0,\ldots,0)$ (a — k-я координата этого вектора), получаем

$$\omega_E(t) = \omega_{E\cup(0,\ldots,0,a,0,\ldots,0)}(t) + \omega_H(t-a).$$

Теперь применим (12.2) к матрице $E \cup (0,\ldots,0,a,0,\ldots,0)$ и вектору $(0,\ldots,0,1,0,\ldots,0)$ (где 1 стоит на k-м месте). По теореме 12.8(8) получим

$$\omega_{E\cup(0,\ldots,0,a,0,\ldots,0)}(t) = \omega_{E_1}(t) + \omega_{E\cup(0,\ldots,0,a-1,0,\ldots,0)}(t-1).$$

Повторяя эту операцию a раз, получим равенство

$$\omega_{E\cup(0,\ldots,0,a,0,\ldots,0)}(t) = \omega_{E_1}(t) + \omega_{E_1}(t-1) + \cdots + \omega_{E_1}(t-(a-1)),$$

откуда следует (13.9) (см. (13.8)). □

Теперь можно предложить следующую схему вычисления размерностного многочлена $\omega_E(t)$ матрицы $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$, основанную на формуле (13.9). Сначала, выбрав вектор $(a, 0, \ldots, 0) \in \mathbb{N}^m$, где $a = \min_{1\leqslant i\leqslant n}\{e_{i1} \mid e_{i1} \neq 0\}$, и применив лемму 13.10, сведем нашу задачу к вычислению размерностного многочлена матрицы E_1 с $(m-1)$ столбцом и размерностного многочлена матрицы $H = (h_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$, такой, что $0 \leqslant h_{i1} < e_{i1}$ $(1 \leqslant i \leqslant n)$. Для определения $\omega_H(t)$ применим формулу (13.9) (с матрицей H вместо E) и продолжим процесс до тех пор, пока не получим представление $\omega_E(t)$ в виде суммы размерностных многочленов матриц с $(m-1)$ столбцом и размерностного многочлена $\omega_{H_1}(t)$, где H_1 — $n\times m$-матрица с нулевым первым столбцом. Для вычисления $\omega_{H_1}(t)$ применяем описанную процедуру ко второму столбцу и т. д.

13.11. Пример. Вычислим многочлен Гильберта $\omega_E(t)$ матрицы $E = \begin{pmatrix} 2 & 0 & 0\\ 0 & 2 & 0\end{pmatrix}$.

Сначала находим $a = 2$. Применяя (13.9), получаем

$$\omega_E(t) = \Delta_2\Delta^{-1}\omega_{E_1}(t) + \omega_H(t-2),$$

где $E_1 = (2, 0)$ и $H = \begin{pmatrix} 0 & 0 & 0\\ 0 & 2 & 0\end{pmatrix}$. Ясно, что $\omega_H(t) = 0$ (см. теорему 12.8(6)) и $\omega_{E_1}(t) = \binom{t+2}{2} - \binom{t+2-2}{2}$, следовательно, (см. (13.8))

$$\begin{aligned}\omega_E(t) &= \Delta_2\Delta^{-1}\omega_{E_1}(t) = \omega_{E_1}(t) + \omega_{E_1}(t-1)\\ &= \binom{t+2}{2} - \binom{t}{2} + \binom{t+1}{2} - \binom{t-1}{2} = 4t.\end{aligned}$$

Заметим, что вычисление многочлена Гильберта $\omega_E(t)$ по одному из алгоритмов **A**9, **A**10, **A**11 или **A**12 приводит к представлению этого многочлена в виде $\omega_E(t) = \binom{t+3}{3} - 2\binom{t+3-2}{3} + \binom{t+3-4}{3}$. Однако, применяя лемму 13.10, мы получаем многочлен $\omega_E(t)$ в виде суммы многочленов вида $a_k\binom{t+i}{k}$ $(i \in \mathbb{Z},\ k \in \mathbb{N},\ a_k \in \mathbb{Z})$. Максимальная степень этих многочленов меньше степени многочленов, фигурирующих в подобном представлении для $\omega_E(t)$, когда $\omega_E(t)$ вычисляется по одному из алгоритмов **A**9, **A**10, **A**11 или **A**12.

Следующая лемма дает возможность оценивать степень многочлена Гильберта и вычислять его старший коэффициент, не вычисляя многочлен Гильберта полностью.

13.12. Лемма. *Пусть* $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$*-матрица над* $\mathbb{N}$ *и* $\tau\leqslant m$ *— неотрицательное целое число. Тогда* $\deg\omega_E(t)<\tau$ *если и только если для любого подмножества* I*, состоящего из* $m-\tau$ *элементов множества* $\{1,\dots,m\}$*, существует строка* e_I *матрицы* E*, такая, что все элементы этой строки, стоящие в столбцах с индексами из* I*, равны нулю. В частности,* $\omega_E(t)=\mathrm{const}$ *тогда и только тогда, когда* E *содержит диагональную подматрицу.*

Доказательство леммы проводится индукцией по сумме элементов матрицы E и оставляется читателю в качестве упражнения.

Матрицу E над $\mathbb{N}$ назовем *нормализованной*, если каждый столбец матрицы E содержит нуль. Ниже будет показано, что если E — нормализованная $n\times m$-матрица, то алгоритм вычисления размерностного многочлена $\omega_E(t)$, основанный на лемме 13.10, требует меньшего числа операций, чем для произвольной $n\times m$-матрицы. В то же время, для сведения задачи вычисления размерностного многочлена произвольной $n\times m$-матрицы над $\mathbb{N}$ к аналогичной задаче для нормализованной $n\times m$-матрицы можно воспользоваться теоремой 12.8(9).

13.13. Лемма. *Пусть* $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$*-матрица над* $\mathbb{N}$ *и предположим, что* $\deg\omega_E = 0$.

(1) *Если* $e_{1j}=0$ *при* $j=2,\dots,m$ *и* $e_{i1}=0$ *при* $i=2,\dots,n$*, то* $\omega_E = e_{11}\omega_{E_1}$*, где* $(n-1)\times(m-1)$*-матрица* E_1 *получена из* E *удалением первой строки и первого столбца.*

(2) *Если матрица* H *получена из* E *посредством обнуления первого столбца, то* $\omega_H = 0$.

(3) *Если* $a=\min_{1\leqslant i\leqslant n}\{e_{i1}|e_{i1}\neq 0\}$*, то*

$$\omega_E = a\omega_{E_1} + \omega_{E_2}, \tag{13.10}$$

где матрица E_1 *получена из* E *удалением первого столбца и всех строк, содержащих ненулевые элементы в первом столбце, а* $E_2 = (e'_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$*, где*

$$e'_{ij} = \begin{cases} e_{ij}, & \text{если}\quad 2\leqslant j\leqslant m,\\ \max\{e_{i1}-a,0\}, & \text{если}\quad j=1\end{cases}\quad (i=1,\dots,n).$$

Доказательство. (1) Если $e_{11}=0$, то в E имеется нулевая строка, следовательно, $\omega_E=0$ (см. теорему 12.8(6)). Если $e_{11}>0$, то

применяя (12.2) к E и $\mathbf{e} = (1, 0, \ldots, 0) \in \mathbb{N}^m$, получаем

$$\omega_E = \omega_{E \cup \mathbf{e}} + \omega_H = \omega_{E_1} + \omega_H, \text{ где } H = \begin{pmatrix} e_{11} - 1 & 0 \ldots 0 \\ 0 & \\ \vdots & E_1 \\ 0 & \end{pmatrix}.$$

Таким образом, индукция по e_{11} дает требуемый результат.

(2) Лемма 13.12 утверждает, что E содержит строку, в которой ненулевой может быть только первая координата. Значит H содержит нулевую строку, следовательно, $\omega_H = 0$.

(3) Соотношение (13.10) следует из (12.2), записанного для E и $(a, 0, \ldots, 0) \in \mathbb{N}^m$. □

Пользуясь леммой 13.13, можно предложить следующий метод вычисления многочлена Гильберта ω_E матрицы E в случае, когда $\deg \omega_E = 0$: применить соотношение (13.10) к ω_E (где a — минимальный ненулевой элемент в первом столбце матрицы E), затем выписать аналогичное представление для E_2 и т. д. После конечного числа таких шагов получим представление многочлена ω_E в виде суммы многочленов Гильберта матриц $F_1, \ldots, F_r$ ($r \in \mathbb{N}$, $r \geqslant 1$) с $(m-1)$ столбцами и многочлена Гильберта ω_H, где элементы матрицы $H = (h_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ равны

$$h_{ij} = \begin{cases} e_{ij}, & \text{если } 1 \leqslant i \leqslant n,\ 2 \leqslant j \leqslant m \\ 0, & \text{если } 1 \leqslant i \leqslant n,\ j = 1, \end{cases}$$

так что $\omega_H = 0$ (см. лемму 13.13(2)). Применяя описанную процедуру к каждой из матриц $F_1, \ldots, F_r$, мы сводим вычисление многочлена ω_E к вычислению многочленов Гильберта для некоторых матриц с $(m-2)$ столбцами и т. д., пока не получим матрицы, состоящие из единственного столбца. Как мы знаем, многочлен Гильберта такой матрицы совпадает с ее минимальным элементом.

В общем случае (без условия $\deg \omega_E = 0$) вычисление размерностного многочлена $\omega_E(t)$ для $n \times m$-матрицы $E = (e_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ по описанной схеме (используя (13.9) вместо (13.10)) можно свести к вычислению размерностных многочленов матриц, число столбцов в которых меньше m, и размерностных многочленов некоторых $n \times m$-матриц с нулевым первым столбцом. Более точно: если первый столбец матрицы E содержит ненулевые элементы, то мы полагаем $a = \min_{1 \leqslant i \leqslant n} \{e_{i1} | e_{i1} \neq 0\}$ и применяем (13.9). Затем применяем то

же самое соотношение к H (см. лемму 13.10) и т. д. В результате получим разложение многочлена $\omega_E(t)$ в сумму многочленов вида $\omega_{E_i}(t-a_i)$, где $a_i \in \mathbb{N}$ и E_i — либо матрица, число столбцов в которой меньше m, либо $n\times m$-матрица с нулевым первым столбцом. Для вычисления размерностных многочленов матриц второго типа применяем описанный метод ко второму столбцу и т. д., пока не получим представление многочлена $\omega_E(t)$ в виде суммы размерностных многочленов матриц, число столбцов в которых меньше m, и размерностных многочленов матриц с не более чем двумя ненулевыми столбцами. Размерностный многочлен матрицы последнего типа может быть найден с помощью следующего утверждения.

13.14. Лемма. *Пусть*

$$E = \begin{pmatrix} e_{11} & e_{12} & 0 & \dots & 0 \\ e_{21} & e_{22} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & 0 & \dots & 0 \end{pmatrix}$$

— нормализованная $n\times m$-матрица над $\mathbb{N}$ ($m \geqslant 2$). Предположим, что $0 = e_{11} < e_{21} < \dots < e_{n1}$ и $e_{12} > e_{22} > \dots > e_{n2} = 0$. Тогда

$$\omega_E(t) = \sum_{i=1}^{n-1} \Delta_{(e_{i+1,1}-e_{i1})}\Delta^{-1}\omega_{\mathbf{e}_i}(t-e_{i1}), \tag{13.11}$$

где $\mathbf{e}_i = (e_{i2}, 0, \dots, 0) \in \mathbb{N}^{m-1}$ $(i = 1, \dots, n-1)$.

Доказательство. Воспользуемся индукцией по n. Случай $n = 1$ тривиален. Пусть $n > 1$, и предположим, что утверждение леммы доказано для всех матриц, число строк которых меньше n. Для доказательства соотношения (13.11) для $n\times m$-матрицы $E = (e_{ij})_{\substack{1\leqslant i\leqslant n,\\ 1\leqslant j\leqslant m}}$, у которой $e_{ij} = 0$ $(1 \leqslant i \leqslant n,\ 3 \leqslant j \leqslant m)$, прежде всего заметим, что если $a = \min_{1\leqslant i\leqslant n}(e_{i1} \mid e_{i1} \neq 0) = e_{21}$, то

$$\omega_E(t) = \Delta_a\Delta^{-1}\omega_{E_1}(t) + \omega_H(t-a),$$

где $E_1 = (e_{12}, 0, \dots, 0) \in \mathbb{N}^{m-1}$ и $H = \begin{pmatrix} 0 & e_{12} & 0 & \dots & 0 \\ 0 & e_{22} & 0 & \dots & 0 \\ e_{31}-e_{21} & e_{32} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{n1}-e_{21} & e_{n2} & 0 & \dots & 0 \end{pmatrix}$

(см. лемму 13.10). Первая строка матрицы H является лишней, следовательно, $\omega_H = \omega_{H_1}$, где $H_1 = \begin{pmatrix} 0 & e_{22} & 0 & \dots & 0 \\ e_{31}-e_{21} & e_{32} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{n1}-e_{21} & e_{n2} & 0 & \dots & 0 \end{pmatrix}$. По предположению индукции имеем

$$\omega_H(t) = \omega_{H_1} = \sum_{i=2}^{n-1} \Delta_{(e_{i+1,1}-e_{i1})}\Delta^{-1}\omega_{\mathbf{e}_i}(t-e_{i1}),$$

следовательно,

$$\begin{aligned}\omega_E(t) &= \Delta_{e_{21}}\Delta^{-1}\omega_{E_1}(t) + \sum_{i=2}^{n-1} \Delta_{(e_{i+1,1}-e_{i1})}\Delta^{-1}\omega_{\mathbf{e}_i}(t-e_{i1}) \\ &= \sum_{i=1}^{n-1}\Delta_{(e_{i+1,1}-e_{i1})}\Delta^{-1}\omega_{\mathbf{e}_i}(t-e_{i1}). \qquad \square\end{aligned}$$

13.15. Следствие. *Пусть* $E = \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \\ \vdots & \vdots \\ e_{n1} & e_{n2} \end{pmatrix}$ — $n\times 2$-*матрица над* $\mathbb{N}$, *такая, что* $0 = e_{11} < e_{21} < \dots < e_{n1}$, $e_{12} > e_{22} > \dots > e_{n2} = 0$. *Тогда*

$$\omega_E(t) = \sum_{i=1}^{n-1}(e_{i+1,1}-e_{i1})e_{i2}. \tag{13.12}$$

А13. Алгоритм (E, n, m, ω).

Дано: $n \in \mathbb{N}$; $m \in \mathbb{N}$; $n\times m$-матрица E.

Надо: $\omega_E(t)$ — многочлен Гильберта матрицы E.

Переменные: P_0, P_1 — многочлены;
N_S — текущее значение первой координаты;
N_R — следующее значение первой координаты;
E_0 — последовательность $(m-1)$-мерных векторов.

Начало
$\omega(t) := 0$
если $n = 0$ **то** $\omega(t) := \binom{t+m}{m}$
иначе $\mathbf{v} := (v_1, \dots, v_m)$, где $v_j = \min_{1\leqslant i\leqslant n}\{e_{ij}\}$ $(j = 1, \dots, m)$
$E := (e_{ij} - v_j)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$
$K :=$ {индексы ненулевых столбцов матрицы E}

выбор

$\operatorname{Card} K = 2$, $K = \{j, p\}$ $\Longrightarrow$ сортировать строки по возрастанию j-го столбца

удалить лишние строки

$\omega := \omega(t) + \sum\limits_{i=1}^{n-1} \Delta_{(e_{i+1,j} - e_{ij})} \Delta^{-1} \omega_{\mathbf{e}_i}(t - e_{ij})$,

где $\mathbf{e}_i = (e_{ip}, 0, \ldots, 0) \in \mathbb{N}^{m-1}$

$\operatorname{Card} K > 2 \Rightarrow$ взять $k \in K$

переставить k-й столбец с первым

$N_S := 0$

$E_0 := \emptyset$

цикл для каждого ненулевого e_{i1} в возрастающем порядке

$N_R := e_{i1}$

E_0: добавить последовательность строк

$\{(e_{j2}, \ldots, e_{jm}) | e_{j1} = N_S\}$

$N_0 :=$ число векторов в E_0

Алгоритм **A**13 $(E_0, N_0, m-1, P_0(t))$

$P_0(t) := \Delta_{(N_R - N_S)} \Delta^{-1} P_0(t)$

$\omega(t) := \omega(t) + P_0(t - N_S)$

$N_S := N_R$

конец цикла

E: обнулить первый столбец

Алгоритм **A**13 $(E, n, m, P_1(t))$

$\omega(t) := \omega(t) + P_1(t - N_S)$

конец выбора

$\omega(t) := \omega(t - |\mathbf{v}|) + \binom{t+m}{m} - \binom{t+m-|\mathbf{v}|}{m}$

конец если

Конец

Приведенный здесь алгоритм **A**13 вычисления многочлена Гильберта $\omega_E(t)$ для $n \times m$-матрицы E основан на данной выше схеме. В соответствии с ней, воспользуемся (13.8), чтобы представить многочлен $\omega_E(t)$ в виде суммы многочленов Гильберта матриц, которые содержат менее m столбцов, и многочлена Гильберта $n \times m$-матрицы E', содержащей не более двух ненулевых столбцов (без потери общности можно считать, что ненулевыми являются два первых столбца матрицы E'). Многочлен $\omega_{E'}(t)$ вычисляется с помощью соотношения (13.10). Сначала переупорядочим строки так, чтобы элементы первого столбца удовлетворяли условию леммы 13.14 (такое переупорядочение требует $\sim n \log n$ элементарных операций). Тогда видно, что если второй ненулевой столбец не упорядочен в обратном порядке, то матрица E' содержит лишние строки (в точности те строки

$\mathbf{e}_i$ $(1 \leqslant i \leqslant n)$, в которых $e_{12} \geqslant e_{j2}$ для некоторого $j \in \mathbb{N},\ 1 \leqslant j < i)$. Таким образом, получаем следующую оценку числа $f(n,m)$ элементарных операций, которые требуются для вычисления многочлена Гильберта $\omega_E(t)$ для $n \times m$-матрицы E с помощью алгоритма **A**13:

$$\begin{aligned} f(n,m) &\leqslant n\log n + f(n,m-1) + \sum_{i=1}^{k} f(b_i, m-1) \\ &\leqslant n\log n + nf(n,m-1) \end{aligned}$$

где $1 \leqslant k < n;\ b_1, \ldots, b_k \in \mathbb{N};\ 1 \leqslant b_i \leqslant n\ (i = 1, \ldots, k)$. Следовательно, алгоритм **A**13 имеет асимптотическую сложность $\sim n^{m-1}\log n$ при $m \geqslant 2$ (если $m = 1$, то асимптотическая сложность $\sim n$).

13.16. Пример. Вычислим многочлен Гильберта матрицы

$$E = \begin{pmatrix} 1 & 0 & 0 & 1 \\ r-2 & 0 & 1 & 0 \\ r-3 & 0 & 2 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ i & 0 & r-i-1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & r-2 & 0 \\ 0 & 1 & 0 & r-2 \end{pmatrix}$$

$(r \in \mathbb{N},\ r \geqslant 3)$ при помощи алгоритма **A**13. В процессе вычислений последовательно применяем (13.8), начиная с последнего столбца матрицы E. Прежде всего запишем

$$\omega_E(t) = \Delta_1\Delta^{-1}\omega_{E_1}(t) + \omega_H(t-1) = \omega_{E_1}(t) + \omega_H(t-1),$$

где $E_1 = \begin{pmatrix} r-2 & 0 & 1 \\ r-3 & 0 & 2 \\ \vdots & \vdots & \vdots \\ 1 & 0 & r-2 \end{pmatrix}$, $H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ r-2 & 0 & 1 & 0 \\ r-3 & 0 & 2 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ i & 0 & r-i-1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & r-2 & 0 \\ 0 & 1 & 0 & r-3 \end{pmatrix}$. По теореме 12.8(8) имеем

$$\begin{aligned} \omega_H(t-1) = \omega_{(1,0,r-3)}(t-1) &= \binom{t-1+3}{3} - \binom{t-1+3-(r-2)}{3} \\ &= \binom{t+2}{3} - \binom{t+4-r}{3}. \end{aligned}$$

Применяя (12.2) к E_1 и $(1,0,1)$, получаем $\omega_{E_1}(t) = \omega_{(1,0,1)}(t) + {}$ $+\omega_{H_1}(t-2)$, где $H_1 = \begin{pmatrix} r-3 & 0 & 0 \\ r-4 & 0 & 1 \\ \vdots & \vdots & \vdots \\ 1 & 0 & r-4 \\ 0 & 0 & r-3 \end{pmatrix}$, так что из формулы (13.10)

следует, что

$$\begin{aligned}\omega_{H_1}(t-2) &= \sum_{i=1}^{r-3} \Delta_1\Delta^{-1}\omega_{(r-2-i,0)}(t-2-(i-1)) \\ &= \sum_{i=1}^{r-3} \omega_{(r-2-i,0)}(t-i-1) \\ &= \sum_{i=1}^{r-3} \left[\binom{t-i-1+2}{2} - \binom{t-i-1+2-(r-2-i)}{2}\right] \\ &= \sum_{i=1}^{r-3} \left[\binom{t-i+1}{2} - \binom{t+3-r}{2}\right] \\ &= \frac{(r-3)(r-2)}{2}t - \frac{(r-2)(r-3)(2r-5)}{6}.\end{aligned}$$

Поэтому,

$$\begin{aligned}\omega_{E_1}(t) &= \binom{t+3}{3} - \binom{t+3-2}{3} + \frac{(r-3)(r-2)}{2}t - \frac{(r-2)(r-3)(2r-5)}{6} \\ &= (t+1)^2 + \frac{(r-3)(r-2)}{2}t - \frac{(r-2)(r-3)(2r-5)}{6},\end{aligned}$$

следовательно,

$$\begin{aligned}\omega_E(t) &= \binom{t+2}{3} - \binom{t+4-r}{3} + (t+1)^2 \\ &\quad + \frac{(r-3)(r-2)}{2}t - \frac{(r-2)(r-3)(2r-5)}{6} \\ &= \frac{r}{2}t^2 + \frac{r+2}{2}t - \frac{r^3-6r^2+11r-12}{6}.\end{aligned}$$

Рассмотрим задачу вычисления старшего коэффициента многочлена Гильберта. Пусть $E = (e_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ — $n\times m$-матрица над $\mathbb{N}$ и

$$\omega_E(t) = \sum_{i=0}^{m} a_i(E)\binom{t+i}{i} \tag{13.13}$$

— ее многочлен Гильберта. Тогда по теореме 12.8(7) имеем

$$a_m(E) = \begin{cases} 1, & \text{если матрица } E \text{ пустая } (n=0) \\ 0, & \text{в противном случае.}\end{cases}$$

Из теоремы 12.8(9) и леммы 13.12 легко следует, что

$$a_{m-1}(E) = \begin{cases} 0, & \text{если матрица } E \text{ пустая,} \\ \sum_{j=1}^{m} \min_{1\leqslant i\leqslant n}\{e_{ij}\}, & \text{в противном случае.} \end{cases}$$

Вычисление коэффициента $a_{m-2}(E)$ (при $m \geqslant 2$) может основываться на следующем утверждении.

13.17. Лемма. *Пусть* $E = (e_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ — $n\times m$*-матрица над* $\mathbb{N}$*, такая, что* $m > 1$ *и первый столбец матрицы* E *нулевой. Пусть* $\omega_E(t) = \sum\limits_{i=0}^{\tau} a_i(E)\binom{t+i}{i}$ — *многочлен Гильберта матрицы* E *и* $0 < \deg\omega_E \leqslant \tau$ ($\tau \in \mathbb{N}_m$). *Далее, пусть* E_1 — $n\times(m-1)$*-матрица, полученная из* E *удалением первого (нулевого) столбца. Тогда* $\deg\omega_{E_1} \leqslant \tau - 1$ *и* $a_\tau(E) = a_{\tau-1}(E_1)$.

Доказательство. Применяя (12.2) к E и $(1, 0, \ldots, 0) \in \mathbb{N}^m$, получим, что $\omega_E(t) = \omega_{E_1}(t) + \omega_E(t-1)$. Значит, если

$$\omega_E(t) = \sum_{i=0}^{\tau} a_i(E)\binom{t+i}{i},$$

то

$$\begin{aligned}\omega_{E_1}(t) &= \sum_{i=0}^{\tau} a_i(E_1)\binom{t+i}{i} = \sum_{i=0}^{\tau} a_i(E)\left[\binom{t+i}{i} - \binom{t+i-1}{i}\right] \\ &= \sum_{i=0}^{\tau-1} a_{i+1}(E)\binom{t+i}{i},\end{aligned}$$

следовательно, $\deg\omega_{E_1} \leqslant \tau - 1$ и $a_i(E_1) = a_{i+1}(E)$ для всех $i = 0, 1, \ldots, \tau-1$. В частности, $a_\tau(E) = a_{\tau-1}(E_1)$. □

Отметим, что если для $n\times m$-матрицы $E = (e_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ степень многочлена Гильберта $\omega_E(t) = \sum\limits_{i=0}^{m} a_i(E)\binom{t+i}{i}$ меньше или равна τ ($\tau \in \mathbb{N}$, $0 \leqslant \tau \leqslant m$), то

$$a_\tau(E) = a_\tau(E_1) + a_\tau(E_2), \tag{13.14}$$

где $a = \min_{1\leqslant i\leqslant n}\{e_{i1} | e_{i1} \neq 0\}$, матрица E_1 получена из E удалением первого столбца и всех строк с нулем в первом столбце, а $E_2 = (e'_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ — $n\times m$-матрица с элементами

$$e'_{ij} = \begin{cases} e_{ij}, & \text{если } j \neq 1 \\ \max\{e_{i1} - a, 0\}, & \text{если } j = 1 \end{cases} \quad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m).$$

(Соотношение (13.14) легко может быть установлено применением (12.2) к E и $(a,0,\dots,0)\in\mathbb{N}^m$.)

Прежде чем вычислять коэффициент $a_{m-2}(E)$ многочлена Гильберта (13.13), заметим, что, без потери общности, можно предполагать, что $\deg\omega_E\leqslant m-2$. Действительно, применяя (12.2) к E и $\mathbf{e}=\big(\min\limits_{1\leqslant i\leqslant n}\{e_{i1}\},\dots,\min\limits_{1\leqslant i\leqslant n}\{e_{im}\}\big)$, получаем, что

$$\omega_E(t)=\binom{t+m}{m}-\binom{t+m-|\mathbf{e}|}{m}+\omega_{E'}(t-|\mathbf{e}|),$$

где $E'=(e'_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}$ — матрица с элементами $e'_{ij}=e_{ij}-\min_{1\leqslant i\leqslant n}\{e_{ij}\}$ $(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m)$. Пользуясь (11.4), можно переписать последнее представление $\omega_E(t)$ в виде

$$\begin{aligned}\omega_E(t)&=\sum_{i=0}^{|\mathbf{e}|-1}\binom{t+m-1-i}{m-1}+\omega_{E'}(t-|\mathbf{e}|)\\&=|\mathbf{e}|\binom{t+m-1}{m-1}-\sum_{i=1}^{|\mathbf{e}|-1}\left[\binom{t+m-1}{m-1}-\binom{t+m-1-i}{m-1}\right]+\omega_{E'}(t-|\mathbf{e}|)\\&=|\mathbf{e}|\binom{t+m-1}{m-1}-\sum_{i=1}^{|\mathbf{e}|-1}\sum_{k=0}^{i-1}\binom{t+m-1-i+k}{m-2}+\omega_{E'}(t-|\mathbf{e}|)\\&=|\mathbf{e}|\binom{t+m-1}{m-1}-\frac{|\mathbf{e}|(|\mathbf{e}|-1)}{2}\binom{t+m-2}{m-2}+o(t^{m-2})+\omega_{E'}(t-|\mathbf{e}|).\end{aligned}$$

Поскольку $\deg\omega_{E'}\leqslant m-2$ (см. лемму 13.12), имеем $a_{m-2}(E)=$ $=a_{m-2}(E')-\frac{|\mathbf{e}|(|\mathbf{e}|-1)}{2}$, следовательно, можно вместо $a_{m-2}(E)$ вычислять $a_{m-2}(E')$, поэтому в дальнейших рассуждениях предполагаем, что $\deg\omega_{E'}\leqslant m-2$ и $\omega_E(t)=\sum\limits_{i=0}^{m-2}a_i(E)\binom{t+i}{i}$, где $a_i(E)\in\mathbb{Z}$ $(i=0,1,\dots,m-2)$. Кроме того, предполагаем, что E содержит не более двух ненулевых столбцов (следует отметить, что если в E имеется единственный ненулевой столбец, то многочлен Гильберта $\omega_E(t)$ совпадает с минимальным элементом этого столбца). Предполагая, что первый столбец матрицы E ненулевой, упорядочим его элементы и применим (13.14) при $\tau=m-2$. Поскольку число столбцов в E_1 (см. (13.14)) равно $(m-1)$, вычисление $a_\tau(E_1)$ можно свести к выбору минимальных элементов в столбцах матрицы E_1 (см. теорему 12.8(3)). Легко видеть, что такой выбор требует $(m-1)b_1$ элементарных операций, где b_1 — число строк матрицы E_1.

Применяя (13.14) к E_2, сводим вычисление $a_\tau(E_2)$ (в правой части формулы (13.14)) к вычислению коэффициента $a_2(E_{21})$ многочлена Гильберта некоторой матрицы E_2, содержащей $(m-1)$ столбец (эта матрица получена добавлением некоторых дополнительных строк к E_1). Чтобы вычислить $a_\tau(E_{21})$, нужно не более $(m-1)b_2$ элементарных операций (здесь b_2 обозначает число строк матрицы E_{21}). Продолжаем применять (13.14), пока не получим матрицу с нулевым первым столбцом. По лемме 13.17 такой столбец можно отбросить, затем применяем (13.14) к новой матрице и т. д.

Асимптотическая сложность $g(n,m)$ описанного алгоритма не превосходит

$$\begin{aligned} n\log n + \sum_{\substack{i=1\\ b_i\in\mathbb{N}\\ b_1+\dots+b_k=n}}^{k} b_i m + g(n,m-1) \\ \leqslant 2n\log n + n(m+m-1) + g(n,m-2) \leqslant \dots \\ \leqslant (m-1)n\log n + n(m+(m-1)+\dots+2) + g(n,1) \\ = (m-1)n\log n + n\binom{m+1}{2} \sim mn\log n. \end{aligned}$$

A14. Алгоритм (E,n,m,a_{m-2}).
Дано: $n\in\mathbb{N}$; $m\in\mathbb{N}$; $n\times m$-матрица E, такая, что $\deg\omega_E \leqslant m-2$
Надо: $a_{m-2}(E)$.

Начало
$a_{m-2} := 0$
$r :=$ число нулевых столбцов матрицы E
$m := m - r$
E : удалить нулевые столбцы
сортировать строки по возрастанию элементов первого столбца
$N_S := 0$
$i := 1$
$E_0 := \emptyset$
цикл пока $i < n$
  цикл пока $e_{i1} = N_S$ и $i \leqslant n$
    $E_0 := E_0 \cup (e_{i2},\dots,e_{im})$
    $i := i+1$
  конец цикла
  $N_R := e_{i1}$
  a $:= (a_1,\dots,a_{m-1})$, где a_i — минимальный элемент i-го столбца матрицы, состоящей из векторов из E_0

$E_0 := \mathbf{a}$
$a_{m-2} := a_{m-2} + |\mathbf{a}|(N_R - N_S)$
$N_S := N_R$
конец цикла
E : удалить первый столбец
алгоритм $\mathbf{A}14(E, n, m-1, b)$
$a_{m-2} := a_{m-2} + b$
Конец

Теперь, пользуясь алгоритмом **A**14 и формулой (13.14), можно найти старший коэффициент многочлена Гильберта для любой матрицы. Сложность $f_k(n,m)$ вычисления этого коэффициента для матрицы E, такой, что $\deg \omega_E = m-k$ $(1 \leqslant k \leqslant m)$, не превосходит

$$n\log n + \sum_{i=1}^{n} f_{k-1}(i, m-1) + f_k(n, m-1) \leqslant n\log n + nf_{k-1}(n, m-1) + f_k(n, m-1),$$

при использовании приведенного ниже алгоритма **A**15. Таким образом, $f_3(n,m) \sim \binom{m}{2} n^2 \log n$ и, в общем случае,

$$f_k(n,m) \sim \binom{m}{k-1} n^{k-1} \log n \quad (k = 3, \ldots, m).$$

A15. Алгоритм (E, n, m, k, a_{m-k}).
Дано: $n \in \mathbb{N}$, $m \in \mathbb{N}$, $k \in \mathbb{N}$, $k \geqslant 2$, $m \geqslant k$;
$n \times m$-матрица E, такая, что $\deg \omega_E \leqslant m-k$
Надо: $a_{m-k}(E)$.

Начало
$a_{m-k} := 0$
$r :=$ число нулевых столбцов матрицы E
$m := m - r$
E : удалить нулевые столбцы
сортировать строки по возрастанию элементов первого столбца
$N_S := 0$
$i := 1$
$E_0 := \emptyset$
цикл пока $i < n$
  цикл пока $e_{i1} = N_S$ и $i \leqslant n$
    $E_0 := E_0 \cup (e_{i2}, \ldots, e_{im})$
    $i := i + 1$
  конец цикла

$N_R := e_{i1}$
a $:= (a_1, \ldots, a_{m-1})$, где a_i — минимальный элемент i-го столбца матрицы, состоящей из векторов из E_0
$E_0 := \mathbf{a}$
$a_{m-2} := a_{m-2} + |\mathbf{a}|(N_R - N_S)$
$N_S := N_R$
конец цикла
E : удалить первый столбец
алгоритм $\mathbf{A}14(E, n, m-1, b)$
$a_{m-2} := a_{m-2} + b$
если $k = 2$**, то** алгоритм $\mathbf{A}14(E, n, m, a_{m-2})$
иначе E : удалить нулевые столбцы
$m :=$ число столбцов матрицы E
$N_S := 0$
$E_0 := \emptyset$
цикл для каждого ненулевого e_{i1} в порядке возрастания
$N_R := e_{i1}$
E_0 : добавить последовательность строк
$\{(e_{j2}, \ldots, e_{jm}) \mid e_{j1} = N_S\}$
$N_0 :=$ число векторов в E_0
алгоритм $\mathbf{A}15(E_0, N_0, m-1, k-1, P)$
$a_{m-k} := a_{m-k} + (N_R - N_S)P$
$N_S := N_R$
конец цикла
E : удалить первый столбец
алгоритм $\mathbf{A}15\ (E, n, m-1, k-1, P)$
$a_{m-k} := a_{m-k} + P$
конец если
Конец

Завершая изложение теории размерностных многочленов, следует упомянуть размерностные многочлены от многих переменных, теория которых была заложена в статье [**19**] и подробно изложена в монографии [**20**].

Глава 5

Факторизация многочленов

14. Алгоритмы Кронекера

Алгоритм Кронекера находит для данного многочлена $f(x) \in \mathbb{Z}[x]$ многочлен $f_1(x) \in \mathbb{Z}[x]$, такой, что $f_1(x) | f(x)$, или доказывает, что такого многочлена нет. Алгоритм Кронекера основан на следующих соображениях:

- если степень многочлена f равна n, то степень хотя бы одного множителя f_1 многочлена f не превосходит $[n/2]$;
- значения как f, так и f_1 в целых точках — целые числа, причем $f_1(i)$ делит $f(i)$ для любого целого i;
- при фиксированном i, если $f(i) \neq 0$, то $f_1(i)$ может принимать только конечное множество значений, состоящее из делителей числа $f(i)$;
- коэффициенты многочлена f_1 однозначно восстанавливаются по его значениям в $[n/2] + 1$ точке.

Таким образом, для f_1 получается конечное число возможностей; непосредственным делением проверяем, получили ли делитель многочлена f.

Перепишем алгоритм Кронекера в соответствии со сделанными выше замечаниями.

А16. Алгоритм (Кронекера).

Дано: $f \in \mathbb{Z}[x]$;

Надо: $g \in \mathbb{Z}[x]$;
успех $\in \mathcal{L}$ // "да", если множитель найден.

Обозначения:

$n == f$.степень
$m == g$.степень
$f(i), \quad i \in \mathbb{Z} ==$ значение многочлена f в точке i.

Переменные:

M — множество элементов типа целое
U — множество 'динамических' векторов элементов типа $\mathbb{Z}$

Начало
успех := “нет”
цикл для i **от** 0 **до** $[n/2]$ **пока** не успех
    // проверка, что среди целых чисел от 0 до $[\frac{n}{2}]$ нет корней $f(x)$
    если $f(i) = 0$, **то**
        успех := “да”
        $g := x - i$
        $m := 1$
    конец если
конец цикла
если не успех, **то**
    $U :=$ множество делителей числа $f(0)$
    цикл для i **от** 1 **до** $[n/2]$ **пока** не успех
            // поиск множителя степени i
        $M :=$ множество делителей числа $f(i)$
        $U := U \times M$ // прямое произведение
        цикл для каждого u из U **пока** не успех
            построить многочлен g степени i, такой, что
            $g(j) = u(j)$ для $j = 0..i$
            если f делится на g, **то**
                успех := “да”
                $m := i$
            конец если
        конец цикла
    конец цикла
конец если
Конец

14.1. Замечание. Достаточно научиться разлагать на множители многочлены со старшим коэффициентом, равным 1. Действительно, если старший коэффициент равен a, то домножив на a^{n-1} и сделав замену $x = y/a$, сводим задачу к этому случаю. После ее решения остается сделать обратную замену и сократить на общий множитель a^{n-1}. Однако этот метод обычно оказывается неэффективным: из-за увеличения коэффициентов ухудшаются различные оценки и скорость работы алгоритмов. Поэтому в большинстве работающих алгоритмов таких преобразований не производится.

Другое решение задачи факторизации “за конечное число шагов” следует из того, что коэффициенты делителя — целые числа и их абсолютная величина ограничена сверху некоторой функцией

от коэффициентов многочлена f. В параграфе 7 мы нашли некоторые оценки для этих коэффициентов. Они еще понадобятся нам в дальнейшем.

Задача разложения на неприводимые множители "за конечное число шагов" многочленов от нескольких переменных с "классической" точки зрения решена также примерно сто лет назад. Соответствующий алгоритм также носит имя Кронекера и для некоторых областей коэффициентов (например, для поля комплексных чисел $\mathbb{C}$) остается единственным известным алгоритмом решения этой задачи. Для многочленов с коэффициентами из кольца целых чисел, или из кольца алгебраических чисел, или из конечного поля и некоторых других получены в последнее время новые, более быстрые алгоритмы. Общая схема этих алгоритмов достаточно близка к соответствующим алгоритмам факторизации одномерных многочленов, хотя некоторые отличия весьма существенны. Изложение современных алгоритмов факторизации многомерных многочленов не входит в число вопросов, освещаемых в данном пособии. Читателю, интересующемуся этой задачей, следует обратиться к специальной литературе.

Ниже излагаем многомерный алгоритм Кронекера для задачи, поставленной следующим образом.

Пусть D — область целостности с однозначным разложением на множители, $f(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$. Требуется разложить f на неприводимые множители.

14.1. Многомерный алгоритм Кронекера.

А17. Алгоритм (Кронекера_многомерный).
Дано: $f \in \mathbb{Z}[x_1, \ldots, x_n]$
Надо: G — разложение
Переменные:
многочлен $\bar{f} \in \mathbb{Z}[y]$,
разложение $\bar{G}$ многочлена $\bar{f}$
множество M элементов типа $\mathbb{Z}$

Идея реализации: Редуцировать задачу к одномерному случаю, путем введения новой неизвестной и заменой всех переменных достаточно высокими степенями этой неизвестной. Факторизовать получившийся многочлен. Выполнить обратную подстановку, пробным делением убедиться, получено ли желаемое разложение.

Начало
выбрать целое d большее, чем степени отдельных переменных в f
заменить все переменные степенями новой неизвестной y:

$$\bar{f}(y) := S_d(f) = f(y, y^d, \ldots, y^{d^{n-1}}).$$

разложить $\bar{f}(y)$ на неприводимые множители, т. е.

$$\bar{f}(y) = \bar{g}_1(y) \ldots \bar{g}_s(y), \qquad g_i(y) \in \mathbb{Z}[y], \quad 1 \leqslant i \leqslant s.$$

G.число_множителей $:= 1$
$m := 1$
$M := \{1, \ldots, s\}$
цикл пока $m \leqslant [s/2]$
  цикл для каждого подмножества $\{i_1, \ldots, i_m\} \subset M$ **пока** $m \leqslant [\frac{s}{2}]$
    $g_{i_1,\ldots,i_m}(x_1, \ldots, x_n) := S_d^{-1}(\bar{g}_{i_1}(y)\bar{g}_{i_2}(y) \ldots \bar{g}_{i_m}(y))$
    если f делится на g **то**
      G.множитель[G.число_множителей] $:= g$
      G.число_множителей $:= G$.число_множителей $+ 1$
      $f := f/g$
      $s := s - m$
      M.удалить$\{i_1, i_2, \ldots, i_m\}$
    конец если
  конец цикла
  $m := m + 1$
конец цикла
G.множитель[G.число_множителей] $:= f$
Конец

В этом алгоритме обратное преобразование S_d^{-1} определяется на одночленах по формуле

$$S_d^{-1}\left(y^{b_1 + db_2 + \cdots + d^{v-1}b_v}\right) = x_1^{b_1} \ldots x_v^{b_v}$$

($0 \leqslant b_i < d$ для $1 \leqslant i \leqslant v$, $v \in \mathbb{Z}$), далее S_d^{-1} распространяется по линейности.

15. Разложение на множители, свободные от квадратов

Разложение многочлена на множители начнем с приведения его к некоторому каноническому виду. Прежде всего найдем НОД его коэффициентов, эта величина называется содержанием многочлена f и обозначается $\mathrm{cont}(f)$. Далее разложим многочлен f на *свободные от квадратов* множители, т. е. на такие множители, которые

являются произведениями взаимно простых неприводимых многочленов в первой степени. Это можно сделать путем дифференцирования исходного многочлена и нахождения общих делителей многочлена и его производной. Свободный от квадратов многочлен, содержание которого равно 1, назовем *примитивным*.

В принятых нами обозначениях алгоритм факторизации многочлена f принимает следующий вид.

А18. Алгоритм (факторизовать_многочлен).
Дано: $f \in \mathbb{Z}[x]$
Надо: $\mathrm{cont}(f)$ — содержание многочлена f
U — разложение
Переменные: G — разложение на свободные от квадратов
V — разложение текущего многочлена из G
Обозначения: $s == G$.число_множителей
$g == G$.множители
$u == U$.множители
$v == V$.множители

Начало
u.начать работу
вычислить $\mathrm{cont}(f)$
$f(x) := f(x)/\mathrm{cont}(f)$
разложить_на_свободные_от_квадратов (f, G)

$$f(x) = g_1(x)g_2^2(x)\dots g_s^s(x),$$

цикл для i **от 1 до** s
факторизовать примитивный, свободный от квадратов (g_i, v)
u.добавить v^i
конец цикла
Конец

Вычисление содержания многочлена сводится к вычислению наибольшего общего делителя целых чисел. Поскольку мы предполагаем коэффициенты не слишком большими, вполне достаточно ограничиться алгоритмом Евклида нахождения НОД.

Разложение примитивного (без нетривиальных общих делителей коэффициентов) многочлена на свободные от квадратов множители осуществляется следующим образом.

А19. Алгоритм (разложить_на_свободные_от_квадратов).
Дано: $f(x) \in \mathbb{Z}[x]$; $\mathrm{cont}(f) = 1$
Надо: G — разложение

Переменные: $h,\ c,\ d \in \mathbb{Z}[x]$
$k \in \mathbb{N}$
Обозначения: $s == G.$число_множителей
$g == G.$множители

Начало
$h(x) := \text{НОД}(f(x), f'(x))$, где $f'(x) = df(x)/dx$
$c(x) := f(x)/h(x)$
$d(x) := (df(x)/dx)/h(x) - dc(x)/dx$
$k := 1$
цикл пока $c(x) \neq 1$
$g_k(x) := \text{НОД}(c(x), d(x))$
$c(x) := c(x)/g_k(x)$
$d(x) := d(x)/g_k(x) - dc(x)/dx$
$k := k + 1$
конец цикла
$s := k - 1$
Конец

Для доказательства корректности этого алгоритма предположим, что $f = \prod\limits_{i=1}^{s} g_i^i$, где g_i свободны от квадратов и взаимно просты. Тогда $h = \prod\limits_{i=2}^{s} g_i^{i-1}$, до начала цикла

$$c(x) = \prod_{i=1}^{s} g_i,$$
$$\frac{f'}{h} = \sum_{i=1}^{s}\left(ig_i' \prod_{j=1, j\neq i}^{s} g_j \right),$$
$$d = \sum_{i=1}^{s}\left((i-1)g_i' \prod_{j=1, j\neq i}^{s} g_j \right).$$

В теле цикла выполняется присваивание многочленам $c(x)$ и $d(x)$ значений

$$c(x) = \prod_{i=k+1}^{s} g_i, \qquad d = \sum_{i=k+2}^{s}\left((i-k-1)g_i' \cdot \prod_{j=k+1, j\neq i}^{s} g_j \right).$$

15.1. Упражнение. Построить аналог алгоритма **A**19 для многочленов с коэффициентами из поля F_p.

Алгоритмы разложения на неприводимые множители примитивного свободного от квадратов многочлена с целыми коэффициентами составляют главное содержание данной главы.

Современные алгоритмы разложения примитивного свободного от квадратов многочлена $f(x) \in \mathbb{Z}(x)$ на неприводимые множители основаны на следующих соображениях. Кольцо целых чисел $\mathbb{Z}$ вкладывается в полное нормированное поле $\mathbb{K}$. Предполагается, что мы умеем раскладывать на множители многочлены из кольца $\mathbb{K}[x]$, т. е. для любого наперед заданного числа $\varepsilon > 0$ можем вычислить с абсолютной точностью ε коэффициенты всех неприводимых делителей данного многочлена (предполагается некоторая нормировка делителей, например, равенство единице старшего коэффициента). Каждому неприводимому в $\mathbb{K}[x]$ делителю $h(x)$ многочлена $f(x)$ соответствует однозначно определенный неприводимый в $\mathbb{Z}[x]$ делитель $g(x)$ многочлена $f(x)$, который делится на $h(x)$ (более точно, $g(x)$ представляет собой произведение нескольких неприводимых в $\mathbb{K}[x]$ делителей многочлена $f(x)$, если, конечно, сам $h(x)$ не принадлежит $\mathbb{Q}[x]$). Для нахождения неприводимого в $\mathbb{Z}[x]$ делителя многочлена $f(x)$ либо используют перебор произведений различных подмножеств неприводимых в $\mathbb{K}[x]$ делителей многочлена $f(x)$, либо для восстановления $g(x)$ по $h(x)$ пользуются следующим методом. Ограничивают возможную степень многочлена $g(x)$ положительным числом m; выделяют свободный $\mathbb{Z}$-модуль ранга $m+1$ в модуле многочленов с целыми коэффициентами степени не выше m, в котором должен находиться искомый многочлен $g(x)$, в частности, выделенный модуль может совпадать со всем множеством многочленов степени не выше m, вкладывают этот модуль в евклидово пространство над полем $\mathbb{Q}$ так, чтобы многочлену $g(x)$ соответствовал кратчайший вектор в выделенном модуле, называемом обычно *решеткой*, и находят этот кратчайший вектор.

15.1. Выделение линейных множителей. Прежде чем переходить к общим алгоритмам разложения многочленов на неприводимые множители, рассмотрим случай, когда у многочлена имеются линейные множители. Нахождение линейных множителей осуществляется значительно проще, чем в общем случае нахождение неприводимых множителей. В большинстве систем компьютерной алгебры, прежде чем применять общие методы факторизации, у многочлена выделяются линейные множители.

Нахождение линейных множителей основано на теореме Безу, которая утверждает, что если рациональное число m/n, где m — целое, n — натуральное, $\text{НОД}(m, n) = 1$, является корнем многочлена

с целыми коэффициентами, то n делит старший коэффициент этого многочлена, а m делит его свободный член. Кроме того, между рациональными корнями многочлена и его линейными множителями существует взаимно однозначное соответствие: m/n является корнем многочлена $f(x) \in \mathbb{Z}[x]$ тогда и только тогда, когда $f(x)$ делится на $nx - m$ (предполагается, что m и n взаимно простые числа).

А20. Алгоритм (рациональные_корни).
Дано: $f(x) \in \mathbb{Z}[x]$
Надо: M — стек элементов типа $\mathbb{Q}$ (рациональные корни $f(x)$)
$g(x)$ — делитель максимальной степени многочлена $f(x)$, не имеющий рациональных корней.

Начало
M.начать работу
$a := f$.старший коэффициент
$b := f$.свободный член
$g(x) := f(x)$
цикл для всех (p, q), где $p \in \mathbb{N}$, $q \in \mathbb{Z}$, $p|a$, $q|b$, НОД$(p, q) = 1$
    $r :=$ остаток от деления $g(x)$ на $px - q$
        // т. е. $g(x) = (px - q) \cdot h(x) + r$
    если $r = 0$, **то**
        M.добавить q/p
        $g(x) := h(x)$
    конец если
конец цикла
Конец

15.2. Организация перебора. Простейший случай:

цикл для p **от** 1 **до** a таких, что $p|a$
    цикл для q **от** 1 **до** b таких, что $q|b$ & НОД$(p, q) = 1$,
        цикл для $j = -1; 1$
            $r :=$ остаток от деления $g(x)$ на $px - jq$
                // т. е. $g(x) = (px - jq) * h(x) + r$
            если r=0, **то**
                M.добавить q/p
                $g(x) := h(x)$
            конец если
        конец цикла
    конец цикла
конец цикла

15.3. Перебор с предварительным разложением старшего коэффициента и свободного члена на простые множители. Мы предполагаем, что количество простых чисел, на которые делятся a или b, невелико (не превосходит $NDEL$). Эти числа располагаются в массиве del, соответствующие показатели степеней — в $pow1$ и $pow2$. Числа p и q задаются векторами $curr1$ и $curr2$, которые содержат показатели степеней простых делителей чисел p и q соответственно.

$curr1 := 0$
$p := 0$
M.начать работу
конец_p_перебора := “нет”
цикл пока не конец_p_перебора
    $q := 1$
    $curr2 := 0$
    конец_q_перебора := “нет”
    цикл пока не конец_q_перебора
        ДЕЛЕНИЕ $(g, p, q,$ успех$)$
        если успех, **то**
            M.добавить q/p
            цикл для i **от 1 до** $NDEL$
                $pow1_i := pow1_i - curr1_i$
                $pow2_i := pow2_i - curr2_i$
            конец цикла
        конец если
        если $q > 0$ **то**
            $q := -q$
        иначе $NEXTQ$
        конец если
    конец цикла
    $NEXTP$
конец цикла

А21. Алгоритм NEXTP.
Начало
конец_p_перебора := “да”
цикл для i **от** 1 **до** $NDEL$ **пока** конец_p_перебора
    если $curr1_i < pow1_i$ **то**
        $curr1_i := curr1_i + 1$
        конец_p_перебора := “нет”

иначе $curr1_i := 0$
конец если
конец цикла
$p := 1$
если не конец_p_перебора, **то**
цикл для i **от** 1 **до** $NDEL$
$p := p \cdot del_i^{curr1_i}$
конец цикла
конец если
Конец

А22. Алгоритм NEXTQ.
Начало
конец_q_перебора := “да”
цикл для i **от** 1 **до** $NDEL$ **пока** конец_q_перебора
если $(curr2_i < pow2_i)\&(pow1_i = 0)$ **то**
$curr2_i := curr2_i + 1$
конец_q_перебора := “нет”
иначе $curr2_i := 0$
конец если
конец цикла
$q := 1$
если не конец_q_перебора, **то**
цикл для i **от** 1 **до** $NDEL$
$q := q \cdot del_i^{curr2_i}$
конец цикла
конец если
Конец

16. Факторизация, основанная на переборе неприводимых сомножителей в $K[x]$

16.1. Общая схема. Рассмотрим вложение кольца целых чисел $\mathbb{Z}$ в поле комплексных чисел $\mathbb{C}$. Основная теорема алгебры утверждает, что в кольце $\mathbb{C}[x]$ всякий полином разлагается на линейные множители. Можно считать, что это разложение имеет вид

$$f(x) = a \cdot (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

где a — старший коэффициент полинома f, а $\alpha_1, \dots, \alpha_n$ — его корни. Если f_1 — делитель полинома f в кольце $\mathbb{Z}[x]$, то в $\mathbb{C}[x]$ имеет место разложение

$$f_1(x) = b \cdot (x - \alpha_{i_1}) \dots (x - \alpha_{i_k}),$$

где b — целое число, делящее a, а $\{i_1, \ldots, i_k\}$ — подмножество множества индексов $\{1, \ldots, n\}$. С другой стороны, если полином $f_1(x) = a \cdot (x - \alpha_{i_1}) \ldots (x - \alpha_{i_k})$ принадлежит $\mathbb{Z}[x]$, то полином $f_1(x)/\operatorname{cont}(f_1(x))$ также принадлежит $\mathbb{Z}[x]$ и делит $f(x)$. Таким образом можно предложить следующий метод факторизации полинома $f(x) \in \mathbb{Z}[x]$.

А23. Алгоритм (Факторизовать перебором комплексных корней).
Начало
Найти все комплексные корни $\alpha_1, \ldots, \alpha_n$ полинома f
$I := \{1, \ldots, n\}$
цикл для каждого подмножества $\{i_1, \ldots, i_k\} \subset I$
  если $g(x) = a \cdot (x - \alpha_{i_1}) \ldots (x - \alpha_{i_k})$ принадлежит $\mathbb{Z}[x]$ **то**
    запомнить множитель $g(x) := g(x)/\operatorname{cont}(g(x))$
    $f(x) := f(x)/g(x)$
    $I := I \setminus \{i_1, \ldots, i_k\}$
  конец если
конец цикла
Конец

Если цикл по подмножествам индексов организован так, что вначале рассматриваются множества, состоящие из одного элемента, затем — из двух и т. д., то выделяемый на очередном шаге множитель будет неприводимым и задача факторизации будет полностью решена.

К сожалению, описанный подход не является решением задачи факторизации даже с "классической" точки зрения, поскольку в общем случае мы не можем "за конечное число шагов" найти даже один корень полинома. Однако мы можем находить корни полинома с любой наперед заданной точностью. При этом возникает другая проблема. Если корни полинома вычислены приближенно, то мы не можем проверить, принадлежит ли полином $g(x)$ кольцу $\mathbb{Z}[x]$.

Однако, если точность выбрана достаточно высокой, то эту проверку мы можем заменить двумя шагами: округлить коэффициенты полинома $g(x)$ до ближайшего целого, и проверить, делит ли получившийся полином исходный полином $f(x)$. Получаем:

А24. Алгоритм (с учетом точности вычислений).
Начало
Определить требуемую точность вычислений ε
Найти все комплексные корни $\alpha_1, \ldots, \alpha_n$ полинома f с точностью ε
$I := \{1, \ldots, n\}$

Цикл для каждого подмножества $\{i_1, \dots, i_k\} \subset I$
    Округлить до ближайшего целого коэффициенты
        полинома $g(x) = a \cdot (x - \alpha_{i_1}) \dots (x - \alpha_{i_k})$
    $g(x) := g(x)/\operatorname{cont}(g(x))$
    если $g(x)$ делит $f(x)$ **то**
        запомнить множитель $g(x)$
        $f(x) := f(x)/g(x)$
        $I := I \setminus \{i_1, \dots, i_s\}$
    конец если
конец цикла
Конец

Для практической реализации данного метода нужно детализировать алгоритмы выбора точности вычислений и нахождения корней полинома.

Выбор точности определяется следующим условием: если

$$g(x) = a \cdot (x - \alpha_{i_1}) \dots (x - \alpha_{i_k}) \in \mathbb{Z}[x]$$

и

$$\tilde{g}(x) = a \cdot (x - \tilde{\alpha}_{i_1}) \dots (x - \tilde{\alpha}_{i_k}),$$

где $|\alpha_i - \tilde{\alpha}_i| < \varepsilon$, то коэффициенты полинома $g(x) - \tilde{g}(x)$ по модулю меньше $1/2$. На основе оценок значений корней эта задача не представляет особой сложности.

16.1. Упражнение. Используя границы для корней многочлена, оценить значение ε.

Для нахождения всех комплексных корней полинома можно воспользоваться комплексным аналогом метода Штурма, позволяющим определить количество корней полинома в заданном прямоугольнике комплексной плоскости [**28**], а далее — методом дихотомии. Однако гораздо чаще для нахождения комплексных корней полинома используются разновидности метода Ньютона. Эти методы разрабатываются в численном анализе, и мы не будем здесь останавливаться на них.

Для сокращения перебора можно воспользоваться тем, что корни исходного полинома (коэффициенты которого предполагаются целыми числами), не являющиеся действительными, распадаются на пары комплексно-сопряженных, при этом комплексно-сопряженные корни относятся к одному и тому же неприводимому над $\mathbb{Z}$ делителю исходного полинома. Это замечание позволяет переписать алгоритм без использования комплексных чисел.

А25. Алгоритм (факторизовать с помощью разложения над $\mathbb{R}$).
Начало
Определить требуемую точность вычислений ε
Найти все неприводимые над $\mathbb{R}$ нормированные делители $h_1, \ldots, h_m$ полинома f с точностью ε
$I := \{1, \ldots, m\}$
цикл для каждого подмножества $\{i_1, \ldots, i_k\} \subset I$
    Округлить коэффициенты полинома $g(x) = a \cdot (h_{i_1} \cdot \cdots \cdot h_{i_k})$
        до ближайшего целого
    $g(x) := g(x)/\operatorname{cont}(g(x))$
    если $g(x)$ делит $f(x)$ **то**
        запомнить множитель $g(x)$
        $f(x) := f(x)/g(x)$
        удалить из множества I подмножество $\{i_1, \ldots, i_k\}$
    конец если
конец цикла
Конец

Проанализируем предлагаемый алгоритм. Он основан на том, что любое действительное число является пределом фундаментальной последовательности рациональных чисел и любая фундаментальная последовательность рациональных чисел сходится к действительному числу. Арифметические операции являются при этом непрерывными. При реальных вычислениях на компьютере мы используем итерационные методы, т. е. строим фундаментальные последовательности, сходящиеся к коэффициентам делителей исходного полинома.

Определение фундаментальной и сходящейся последовательности чисел основано на понятии расстояния между двумя числами. В поле действительных чисел расстояние между двумя числами определяется как абсолютная величина разности этих чисел. Метрики такого типа относятся к так называемым архимедовым метрикам. Поле действительных чисел часто определяют как пополнение поля рациональных чисел по архимедовой метрике, т. е. множество классов эквивалентности фундаментальных последовательностей рациональных чисел; при этом две последовательности считаются эквивалентными, если разность между ними — бесконечно малая величина.

Кроме архимедовой, на поле рациональных чисел имеются более экзотические метрики, так называемые неархимедовы или p-адические. Они используются при решении многих алгебраических и

теоретико-числовых задач. В частности, p-адическая метрика оказывается более полезной, чем архимедова при факторизации полиномов.

Применение ее для решения задач факторизации стало возможным после того, как был получен достаточно эффективный метод разложения полиномов на множители над полем p-адических чисел. Этот метод состоит из двух ключевых алгоритмов: первый из них, алгоритм Берлекэмпа, позволяет достаточно быстро разлагать на множители полиномы с коэффициентами из конечного поля, что соответствует нахождению нулевого приближения разложения в описанном выше алгоритме; второй представляет p-адический аналог метода Ньютона. Математический результат, на котором он основан, носит название леммы Гензеля. Метод факторизации, базирующийся на алгоритме Берлекэмпа и лемме Гензеля, принят во многих системах компьютерной алгебры.

16.2. *p*-адический случай. Формально алгоритм факторизации с использованием поля p-адической метрики совпадает с алгоритмом, приведенным выше для поля $\mathbb{R}$:

А26. Алгоритм. (Факторизовать многочлен с помощью p-адической метрики)

Начало
Выбрать простое число p.
Определить требуемую точность вычислений ε.
Найти все неприводимые над R_p нормированные делители $h_1, \ldots, h_m$
    полинома f с точностью ε
$I := \{1, \ldots, m\}$
цикл для каждого подмножества $\{i_1, \ldots, i_k\} \subset I$
    Округлить коэффициенты полинома $g(x) = a \cdot h_{i_1} \cdot \cdots \cdot h_{i_k}$
        до ближайшего целого
    $g(x) := g(x)/\operatorname{cont}(g(x))$
    если $g(x)$ делит $f(x)$ **то**
        запомнить множитель $g(x)$
        $f(x) := f(x)/g(x)$
        удалить из множества I подмножество $\{i_1, \ldots, i_k\}$
    конец если
конец цикла
Конец

Основные отличия заключаются в следующем.

Добавляется новый шаг алгоритма, заключающийся в выборе простого числа p. На выбор его накладывается два условия: во-первых, при переходе к вычетам по модулю p не должна понизиться степень полинома f, т. е. p не должно делить старший коэффициент полинома f; во-вторых, после перехода к классам по модулю p полином f должен остаться свободным от квадратов, т. е. p не должно делить результант полиномов f и f'.

Отметим, что от выбора простого числа p может зависеть количество множителей в разложении полинома по модулю p. В некоторых системах выполняется разложение исходного полинома по модулю нескольких различных значений p (обычно до пяти значений), из них выбирается такое p, разложение по модулю которого имеет наименьшее количество сомножителей, и разложение продолжается по этому модулю. Это замечание относится только ко временным характеристикам алгоритма и носит вероятностный характер (нет алгоритма, позволяющего проверить, что разложение по какому-то модулю имеет минимальное возможное количество сомножителей).

Далее, вместо рациональных чисел, приближающих вещественные коэффициенты, будут использоваться классы по модулю p^i для натуральных значений i. Требуемая точность вычислений определяется как натуральное число s, так что для факторизации полинома $f(x) \in \mathbb{Z}[x]$ нам нужно разложить на множители этот полином по модулю p^s. Округление коэффициентов полинома до ближайшего целого состоит в том, что представители коэффициентов берутся из симметричной системы вычетов.

Как определить требуемую точность вычислений?

Предположим, что $f(x), g(x) \in \mathbb{Q}[x]$, причем $g(x)$ делит $f(x)$. Предположим, что мы умеем оценивать сверху какой-то величиной B абсолютную величину коэффициентов полинома $g(x)$ в зависимости от коэффициентов исходного полинома $f(x)$ и от старшего коэффициента полинома $g(x)$ и от его степени. Таким образом, ошибок округления при нахождении делителя исходного полинома не будет, если используемая симметричная система содержит значения от $-B$ до $+B$, т. е. , если s удовлетворяет неравенству $p^s > 2B$.

Учитывая предположение, что полином f не имеет линейных делителей, т. е. нужно искать неприводимые делители степени не выше $n-2$, где $n = \deg f$, и максимальное значение старшего коэффициента полинома $g(x)$ равно старшему коэффициенту a исходного полинома, шаг алгоритма

Определить требуемую точность вычислений ε

принимает вид:

Найти наименьшее натуральное s, такое, что $p^s > 2^{n-1}\|f\|$.

Перейдем теперь к рассмотрению основного шага алгоритма:

Найти все неприводимые над R_p нормированные делители $h_1, \ldots, h_m$ полинома f с точностью ε

Детализируем его следующим образом.

Найти нулевое приближение разложения
Оценить необходимую точность вычислений
цикл пока не достигнута требуемая точность
    выполнить шаг итерации
конец цикла

Нулевое приближение разложения $f(x)$ в поле p-адических чисел получается из разложения полинома $f(x)$ в поле вычетов по модулю p. Это разложение выполняется с помощью алгоритма Берлекэмпа.

Итерационный шаг уточнения разложения заключается в переходе от сравнения по модулю p^k к сравнению по модулю $q = p^t$, где $t > k$. Этот переход выполняется с помощью леммы Гензеля. Наиболее часто используется случай $t = 2k$ (квадратичный подъем) или $t = k + 1$ (линейный подъем). При этом в одной и той же системе могут применяться оба метода: сначала квадратичный, а после, когда применение квадратичного метода приведет к слишком большим числам, — линейный. Итерационный процесс заканчивается, когда показатель степени t будет не меньше значения s, определенного выше. В качестве представителей системы вычетов по модулю p^t берется сбалансированная система, т. е. целые числа, не превосходящие по абсолютной величине числа $(p^t - 1)/2$.

Проверка испытуемой комбинации на получение делителя полинома $f(x)$ осуществляется пробным делением.

Отметим, что при переборе возможных комбинаций сомножителей мы можем ограничиться случаем, когда рассматриваемая комбинация содержит не более половины из общего количества неприводимых (над R_p) сомножителей.

С учетом сделанных замечаний алгоритм факторизации принимает вид:

А27. Алгоритм (разложить на неприводимые (f, G)).
Дано: $f(x) \in \mathbb{Z}[x]$
Надо: G — разложение;
Переменные: U — разложение
множество M элементов типа $\mathbb{N}$

Начало
выбрать простое число p
// p не должно делить $\mathrm{lc}(f)$ и результант (f, f')
$B := 2^{m-1}\|f\|$ // оценивается необходимая точность вычислений
$s := [\log_p B] + 1$
$q := p^s$
$f_1(x) := \dfrac{f(x)}{\mathrm{lc}(f)} \pmod q$
$U :=$ нулевое приближение разложения $f_1(x)$
поднять разложение U до разложения по модулю q
// достигается кратным применением леммы Гензеля
$r := U$.число_множителей
$t := 1$
$M := \{1, \ldots, r\}$
цикл пока $t \leqslant [r/2]$
цикл для каждого подмножества $\{i_1, \ldots, i_t\} \subset M$ **пока** $t \leqslant [\frac{r}{2}]$
$g(x) := \mathrm{lc}(f)u_{i_1}(x)u_{i_2}(x)\ldots u_{i_t}(x)$
$g(x) := g(x)/\operatorname{cont}(g)$
если $f(x)$ делится на $g(x)$ **то**
G.добавить $g(x)$
$f(x) := f(x)/g(x)$
$r := r - t$
M.удалить $\{i_1, i_2, \ldots, i_t\}$
конец если
конец цикла
$t := t + 1$
конец цикла
G.добавить $f(x)$
Конец

17. Разложение многочленов на неприводимые множители по модулю p

Этот раздел посвящен детализации предписания “нулевое приближение разложения”. Разделим его на два этапа:

(1) разложить многочлен на неприводимые множители по модулю простого p;
(2) найти добавочные множители v_i.

Результатом первого этапа будет целое r и вектор u элементов типа многочлен с индексом $1..r$.

Результатом второго этапа должен явиться вектор v элементов типа $\mathbb{Z}[x]$ с индексом $1..r$, такой, что

$$\sum_{i=1}^{r} v_i(x) \prod_{\substack{j=1 \\ j\neq i}}^{r} u_j(x) \equiv 1 \pmod{p};$$

при этом на элементы вектора v накладываются условия

$$\deg v_i(x) < \deg u_i(x).$$

Вектор v понадобится нам в предписании "выполнить шаг итерации".

Второй этап не представляет принципиальной трудности. Для его выполнения достаточно разложить рациональную функцию на элементарные дроби, что можно сделать методом неопределенных коэффициентов

$$\frac{1}{\prod\limits_{i=1}^{r} u_i(x)} = \sum_{i=1}^{r} \frac{v_i(x)}{u_i(x)}.$$

Можно также несколько раз воспользоваться расширенным алгоритмом Евклида.

Как и в случае простых чисел, задача разложения многочлена на простые множители безусловно сложнее, чем нахождение НОД, но если выполнять разложение по модулю некоторого простого числа, то оно осуществляется не так сложно, как можно было бы ожидать. Значительно проще найти простые множители произвольного многочлена степени n по модулю 2, чем с помощью любого из известных методов определить сомножители произвольного n-разрядного числа в двоичной системе счисления. Этот удивительный факт — следствие алгоритма разложения, открытого в 1967 году Элвином Р. Берлекэмпом.

Основными результатами, на которых основан алгоритм Берлекэмпа, является малая теорема Ферма и китайская теорема об остатках.

17.1. Теорема (Ферма малая). *Если p — простое число, то для любого $a \in \mathbb{Z}$ выполняется сравнение $a^p \equiv a \pmod{p}$.*

17.2. Замечание. Малая теорема Ферма может использоваться в алгоритмах проверки простоты натуральных чисел, а именно, если $a^n \not\equiv a \pmod{n}$ для некоторого $a \in \mathbb{Z}$, то n — составное число. Существуют однако составные числа n, для которых $a^n \equiv a \pmod{n}$ для любого $a \in \mathbb{Z}$.

17.3. Определение. Составное число n, такое, что сравнение $a^n \equiv a \pmod{n}$ выполняется для любого $a \in \mathbb{Z}$, называется *кармайкловым*.

17.4. Упражнение. Найти несколько первых кармайкловых чисел.

17.5. Теорема (китайская об остатках для целых чисел). *Пусть $p_1, \ldots, p_r$ — попарно взаимно простые целые числа. Для любого набора $a_1, \ldots, a_r$ целых чисел существует целое число c, такое, что $c \equiv a_i \pmod{p_i}$ для любого $i = 1, \ldots, r$. Условием $0 \leqslant c < \prod_{i=1}^{r} p_i$ число c определяется однозначно.*

17.6. Теорема (китайская об остатках для многочленов). *Пусть k — поле и $u_1(x), \ldots, u_r(x)$ — попарно взаимно простые многочлены из $k[x]$. Для любого набора $a_1(x), \ldots, a_r(x)$ многочленов из $k[x]$ существует многочлен $c(x)$, такой, что $c(x) \equiv a_i(x) \pmod{u_i(x)}$ для любого $i = 1, \ldots, r$. Условием $\deg c(x) < \sum_{i=1}^{r} \deg u_i(x)$ многочлен $c(x)$ определяется однозначно.*

17.7. Следствие. *Пусть p — простое число, $u_1(x), \ldots, u_r(x)$ — попарно взаимно простые многочлены из $F_p[x]$. Для любого набора $s_1, \ldots, s_r$ целых чисел существует единственный многочлен $v(x)$, такой, что*

$$\begin{gathered} v(x) \equiv s_i \pmod{u_i(x)}, \qquad 1 \leqslant i \leqslant r, \\ \deg v(x) < \sum_{i=1}^{r} \deg u_i(x). \end{gathered} \tag{17.1}$$

Доказательства малой теоремы Ферма и китайской теоремы об остатках могут быть найдены в большинстве учебников по алгебре и теории чисел и оставляются читателю в качестве упражнения.

Пусть p — простое число. Все рассматриваемые ниже операции с многочленами будут выполняться по модулю p.

Предположим, что задан многочлен $u(x)$, коэффициенты которого выбраны из множества $\{0, 1, \ldots, p-1\}$. Считаем, что многочлен $u(x)$ нормирован, т. е. его старший коэффициент равен 1 и свободен от квадратов, если его рассматривать над полем F_p. Если это условие не выполнено, то можно воспользоваться результатом задачи 15.1.

17.8. Предложение. *Для любого многочлена $v(x) \in F_p[x]$*

$$v(x^p) = [v(x)]^p. \tag{17.2}$$

Доказательство. Для любых многочленов $v_1(x)$ и $v_2(x) \in \mathbb{Z}[x]$ по модулю p выполняются равенства

$$(v_1(x)\cdot v_2(x))^p = (v_1(x))^p \cdot (v_2(x))^p,$$

$$[v_1(x)+v_2(x)]^p = v_1^p + C_p^1 v_1^{p-1} v_2 + \cdots + v_2^p = v_1^p(x) + v_2^p(x),$$

поскольку все биномиальные коэффициенты кратны p (т. е. в F_p обращаются в нуль). Далее, для всякого целого числа a по малой теореме Ферма имеем $a^p \equiv a \pmod p$. Поэтому, если $v(x) = v_m x^m + \cdots + v_0$, то

$$[v(x)]^p = (v_m x^m)^p + \cdots + (v_0)^p = v_m x^{mp} + \cdots + v_1 x^p + v_0 = v(x^p),$$

что и доказывает (17.2). □

Идея Берлекэмпа состоит в том, чтобы для нахождения неприводимых сомножителей $u_1(x), \ldots, u_r(x)$ многочлена $f(x) \in F_p[x]$ воспользоваться теперь китайской теоремой об остатках для многочленов, точнее, следствием 17.7. (Отметим, что сравнение выполняется в кольце многочленов с коэффициентами из конечного поля, т. е. утверждение $g(x) \equiv h(x) \pmod{q(x)}$ означает, что разность $g(x) - h(x)$ в кольце $\mathbb{Z}[x]$ принадлежит идеалу, порожденному элементами $q(x)$ и p.)

Если нам известен многочлен $v(x)$, удовлетворяющий системе сравнений (17.1), то можно получить разложение $f(x)$ на множители, используя тот факт, что если $r \geqslant 2$ и $s_1 \neq s_2$, то НОД$(f(x), v(x) - s_1)$ делится на $u_1(x)$ и не делится на $u_2(x)$.

Поскольку решение системы (17.1) может оказаться полезным для решения интересующей нас задачи разложения многочлена на множители, рассмотрим систему (17.1) более подробно. Прежде всего заметим, что решение $v(x)$ этой системы удовлетворяет условию

$$(v(x))^p \equiv s_j^p \equiv s_j \equiv v(x) \pmod{u_j(x)} \qquad \text{при} \quad 1 \leqslant j \leqslant r,$$

поэтому

$$(v(x))^p \equiv v(x) \pmod{f(x)}, \qquad \deg v < \deg f. \tag{17.3}$$

В поле $F_p = \mathbb{Z}/p\mathbb{Z}$ выполняется разложение

$$x^p - x = (x-0)\cdot(x-1)\cdots(x-(p-1)),$$

доказательство которого восходит еще к Лагранжу (1771 год). Следовательно, любой многочлен $v(x)$ удовлетворяет соотношению

$$(v(x))^p - v(x) = (v(x)-0)(v(x)-1)\cdots(v(x)-(p-1)), \tag{17.4}$$

в котором все операции выполняются по модулю p. Отсюда следует, что если многочлен $v(x)$ удовлетворяет соотношению (17.3), то $f(x)$ делит левую часть равенства (17.4), а следовательно, лю-

бой неприводимый множитель многочлена $f(x)$ должен делить один из p взаимно простых множителей в правой части равенства (17.4). Значит, все решения сравнения (17.3) должны представляться в виде (17.1) при некотором выборе значений $s_1, \ldots, s_r$, т. е. у этого сравнения имеется ровно p^r решений. Таким образом, решения сравнения (17.3) дают нам ключ к отысканию разложения многочлена $f(x)$ на неприводимые множители. Может показаться, что найти все решения сравнения (17.3) еще труднее, чем разложить $f(x)$ на неприводимые множители, однако в действительности это не так, поскольку множество решений сравнений (17.3) замкнуто относительно сложения, следовательно, оно является векторным пространством над полем $F_p = \mathbb{Z}/p\mathbb{Z}$.

Пусть $\deg f(x) = n$; рассмотрим матрицу размера $n \times n$

$$\mathcal{Q} = \begin{bmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n-1,0} & q_{n-1,1} & \cdots & q_{n-1,n-1} \end{bmatrix}$$

элементы которой определяются соотношениями

$$x^{kp} \equiv q_{k,n-1}x^{n-1} + \cdots + q_{k,1}x + q_{k,0} \pmod{f(x)}.$$

Многочлен $v(x) = v_{n-1}x^{n-1} + \cdots + v_0$ является решением сравнения (17.3) тогда и только тогда, когда выполняется векторное равенство

$$(v_0, \ldots, v_{n-1}) \cdot \mathcal{Q} = (v_0, \ldots, v_{n-1}).$$

В самом деле, последнее равенство выполняется тогда и только тогда, когда

$$v(x) = \sum_j v_j x^j = \sum_j \sum_k v_k q_{k,j} x^j \equiv \sum_k v_k x^{kp} = v(x^p) \equiv [v(x)]^p \pmod{f(x)}.$$

Построение матрицы $\mathcal{Q}$ легко можно осуществить следующим образом. Для сравнительно малых p можно воспользоваться таким методом вычисления многочленов $x^k \pmod{f(x)}$. Пусть

$$f(x) = x^n + \cdots + c_1x + c_0;$$

и

$$x^k \equiv a_{k,n-1}x^{n-1} + \cdots + a_{k,1}x + a_{k,0} \pmod{f(x)}.$$

Тогда

$$\begin{aligned} x^{k+1} &\equiv a_{k,n-1}x^n + \cdots + a_{k,1}x^2 + a_{k,0}x \\ &\equiv a_{k,n-1}(-c_{n-1}x^{n-1} - \cdots - c_1x - c_0) + a_{k,n-2}x^{n-1} + \cdots + a_{k,0}x \\ &= a_{k+1,n-1}x^{n-1} + \cdots + a_{k+1,1}x + a_{k+1,0}x, \end{aligned}$$

где $a_{k+1,j} = a_{k,j-1} - a_{k,n-1}c_j$. По определению полагаем $a_{k,-1} = 0$, так что $a_{k+1,0} = -a_{k,n-1}c_0$. Таким образом, алгоритм Берлекэмпа разложения многочлена на неприводимые множители состоит в следующем.

17.1. Алгоритм Берлекэмпа.

А28. Алгоритм (нулевое_приближение_разложения).
Дано: p — простое число,
$f(x) \in \mathbb{Z}[x]$ свободен от квадратов по модулю p
Надо: U — разложение f на неприводимые над полем F_p
Обозначения: $t = U$.число_множителей
$n = f$.степень
$u = U$.множители
$\mathcal{I}$ — единичная $n \times n$-матрица
Переменные: $\mathcal{Q}$ — матрица $(n \times n)$ элементов поля F_p
$m, r \in \mathbb{Z}$
v — вектор элементов типа $F_p[x]$ с индексом $1..r$

Начало
сформировать матрицу $\mathcal{Q}$
базис нуль-пространства матрицы $(n, \mathcal{Q} - \mathcal{I}, r, v)$
$t := 1$
$m := 1$
$u[1](x) := f(x)$
цикл для m **от** 1 **до** r **пока** $t < r$
  цикл для j **от** 2 **до** r **пока** $t < r$
    цикл для s **от** 0 **до** $p-1$ **пока** $t < r$
      $h(x) :=$ НОД$(u[m](x), v[j](x) - s)$
      если $h(x) \neq 1$, **то**
        если $h(x) = u[m](x)$, **то**
          выход из цикла по s
        иначе
          $t := t + 1$
          $u[t](x) := h(x)$
          $u[m](x) := u[m](x)/h(x)$
        конец если
      конец если
    конец цикла
  конец цикла
конец цикла
Конец

Заметим, что для сравнительно небольших p (когда мы можем хранить таблицу обратных элементов для всех элементов поля F_p) сложность алгоритма Берлекэмпа оценивается величиной $O(pn^3)$.

Детализацию этого алгоритма начнем с рассмотрения предписания "базис нуль пространства матрицы $\mathcal{Q}-\mathcal{I}$".

А29. Алгоритм (базис_нуль_пространства_матрицы).

Дано: $\mathcal{Q}$ — матрица
n — размерность матрицы $\mathcal{Q}$

Надо: r — размерность нуль-пространства матрицы $\mathcal{Q}$
v — вектор элементов типа (вектор элементов типа F_p с индексом $0..n-1$) с индексом $1..r$, т.е линейно независимые векторы $v[1],\ldots,v[r]$, такие, что $v[j]\cdot\mathcal{Q}=\vec{0}$ записываем v в виде матрицы с индексами $1..r$, $0..n-1$

Переменные: c — вектор элементов типа $\mathbb{Z}$ с индексом $1..n$
$c[j]\geqslant 0 \iff q_{c[j],j}=-1$,
все остальные элементы этой строки $=0$

Идеи реализации: приведение к треугольному виду операциями со столбцами, т. е. переход от $\mathcal{Q}$ к $\mathcal{Q}\times B$, где B — невырожденная матрица

Начало
$r:=0$
цикл для j **от** 0 **до** $n-1$
    $c[j]:=-1$
конец цикла
цикл для k **от** 0 **до** $n-1$ //поиск зависимости строк
    если $\exists j\colon 0\leqslant j<n$, такое, что $\mathcal{Q}[k,j]\neq 0$ и $c[j]<0$, **то**
        умножить j-ый столбец матрицы $\mathcal{Q}$ на $-1/Q[k,j]$
        цикл для i **от** 0 **до** $j-1$ **и от** $j+1$ **до** $n-1$
            цикл для l **от** 0 **до** $n-1$
                $\mathcal{Q}[l,i]:=\mathcal{Q}[l,i]+\mathcal{Q}[k,i]\cdot\mathcal{Q}[l,j]$
            конец цикла
            $c[j]:=k$
                // эти операции не меняют строк матрицы с
                // номерами $0,1,\ldots,k-1$, т. к. $\mathcal{Q}[s,j]=0$
                // для всех $s<k$
        конец цикла
    иначе // матрица $\mathcal{Q}$ приведена к ступенчатому виду
        $r:=r+1$

```
                    // начинаем нахождение собственных векторов
        цикл для j от 0 до n − 1
            v[r, j] := 0
        конец цикла
        цикл для s от 0 до n − 1
            j := c[s]
            если j ⩾ 0, то v[r, j] := Q[k, s] конец если
        конец цикла
        v[r, k] := 1
    конец если
конец цикла
Конец
```

17.2. Пример вычисления матрицы $\mathcal{Q}$ и нахождения ее нульпространства. Данный пример взят из монографии Кнута [**9**].

Пусть

$$u(x) = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8, \quad p = 13.$$

Непосредственными вычислениями проверяется, что

$$\text{НОД}(u(x), u'(x)) = 1.$$

Значит, $u(x)$ свободен от квадратов. Далее, $x^0 \equiv 1 \pmod{u(x)}$, следовательно, 1-я строка матрицы $\mathcal{Q}$ равна $(1, 0, \ldots, 0)$. Вычислим вторую строку, т. е. $x^{13} \pmod{u(x)}$. Ниже приводятся вычисления.

k	$a_{k,7}$	$a_{k,6}$	$a_{k,5}$	$a_{k,4}$	$a_{k,3}$	$a_{k,2}$	$a_{k,1}$	$a_{k,0}$
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0
2	0	0	0	0	0	1	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	12	0	3	3	5	11	5
9	12	0	3	3	5	11	5	0
10	0	4	3	2	8	0	2	8
11	4	3	2	8	0	2	8	0
12	3	11	8	12	1	2	5	7
13	11	5	12	10	11	7	1	2

Получили вторую строку матрицы $\mathcal{Q}$, записанную в обратном порядке. Продолжая подобным образом, получим остальные строки матрицы $\mathcal{Q}$:

$$\mathcal{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 7 & 11 & 10 & 12 & 5 & 11 \\ 3 & 6 & 4 & 3 & 0 & 4 & 7 & 2 \\ 4 & 3 & 6 & 5 & 1 & 6 & 2 & 3 \\ 2 & 11 & 8 & 8 & 3 & 1 & 3 & 11 \\ 6 & 11 & 8 & 6 & 2 & 7 & 10 & 9 \\ 5 & 11 & 7 & 10 & 0 & 11 & 7 & 12 \\ 3 & 3 & 12 & 5 & 0 & 11 & 9 & 12 \end{bmatrix}$$

Вычитая единичную матрицу, получим

$$\mathcal{Q} - \mathcal{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 7 & 11 & 10 & 12 & 5 & 11 \\ 3 & 6 & 3 & 3 & 0 & 4 & 7 & 2 \\ 4 & 3 & 6 & 4 & 1 & 6 & 2 & 3 \\ 2 & 11 & 8 & 8 & 2 & 1 & 3 & 11 \\ 6 & 11 & 8 & 6 & 2 & 6 & 10 & 9 \\ 5 & 11 & 7 & 10 & 0 & 11 & 6 & 12 \\ 3 & 3 & 12 & 5 & 0 & 11 & 9 & 11 \end{bmatrix}$$

Переходим к нахождению нуль-пространства.

$k = 0$. Первая строка нулевая, таким образом, получаем собственный вектор $v[1] = (1, 0, \ldots, 0)$.

$k = 1$. В качестве допустимого значения j можно взять любое $j \geqslant 1$ (напомним, что нумерация столбцов начинается с 0). Удобно взять $j = 5$, т. к. $a_{15} = 12 \equiv -1 \pmod{13}$. Прибавляя к j-му столбцу 5-ый столбец, умноженный на a_{1j}, $j = 0, 2, 3, 4, 6, 7$, получим

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\ 11 & 6 & 5 & 8 & 1 & 4 & 1 & 7 \\ 3 & 3 & 9 & 5 & 9 & 6 & 6 & 4 \\ 4 & 11 & 2 & 6 & 12 & 1 & 8 & 9 \\ 5 & 11 & 11 & 7 & 10 & 6 & 1 & 10 \\ 1 & 11 & 6 & 1 & 6 & 11 & 9 & 3 \\ 12 & 3 & 11 & 9 & 6 & 11 & 12 & 2 \end{bmatrix}$$

Продолжая таким же образом, получим
$k = 2,\ j = 4$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\ 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\ 8 & 1 & 3 & 11 & 4 & 9 & 10 & 6 \\ 2 & 4 & 7 & 1 & 1 & 5 & 9 & 3 \\ 12 & 3 & 0 & 5 & 3 & 5 & 4 & 5 \\ 0 & 1 & 2 & 5 & 7 & 0 & 3 & 0 \\ 11 & 6 & 7 & 0 & 7 & 0 & 6 & 12 \end{bmatrix}$$

$k = 3,\ j = 1$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\ 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 9 & 9 & 8 & 9 & 11 & 8 & 8 & 5 \\ 1 & 10 & 4 & 11 & 4 & 4 & 0 & 0 \\ 5 & 12 & 12 & 7 & 3 & 4 & 6 & 7 \\ 2 & 7 & 2 & 12 & 9 & 11 & 11 & 2 \end{bmatrix}$$

$k = 4,\ j = 7$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\ 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 \\ 1 & 10 & 4 & 11 & 4 & 4 & 0 & 0 \\ 8 & 2 & 6 & 10 & 11 & 11 & 0 & 9 \\ 1 & 6 & 4 & 11 & 2 & 0 & 0 & 10 \end{bmatrix}$$

$k = 5,\ j = 0$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\ 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 \\ 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 5 & 5 & 0 & 9 \\ 12 & 9 & 0 & 0 & 11 & 9 & 0 & 10 \end{bmatrix}$$

Таким образом, матрица приведена к ступенчатому виду. Для нахождения собственных векторов в качестве свободных параметров выбираем последние две координаты. При этом получаются векторы $v[2] = (0, 5, 5, 0, 9, 5, 1, 0)$ и $v[3] = (0, 9, 11, 9, 10, 12, 0, 1)$.

Им соответствуют многочлены

$$v[2](x) = x^6 + 5x^5 + 9x^4 + 5x^2 + 5x,$$
$$v[3](x) = x^7 + 12x^5 + 10x^4 + 9x^3 + 11x^2 + 9x.$$

Находим НОД$(u(x), v[2](x) - s)$. Получаем

$$\text{НОД}(u(x), v[2](x) - 0) = x^5 + 5x^4 + 9x^3 + 5x + 5,$$
$$\text{НОД}(u(x), v[2](x) - 2) = x^3 + 8x^2 + 4x + 12.$$

При всех s, отличных от 0 и 2, получаем НОД$(u(x), v[2](x) - s) = 1$. Поскольку при приведении матрицы Q к ступенчатому виду мы получили $r = 3$, продолжаем поиск неприводимых множителей. Находим, что при $s = 6$

$$\text{НОД}(v[3](x) - s, x^5 + 5x^4 + 9x^3 + 5x + 5) = x^4 + 2x^3 + 3x^2 + 4x + 6,$$

при s =8,

$$\text{НОД}(v[3](x) - s, x^5 + 5x^4 + 9x^3 + 5x + 5) = x + 3,$$

при остальных значениях s этот НОД равен 1.

Таким образом, мы нашли все три неприводимых сомножителя, на которые исходный многочлен $u(x)$ разлагается в поле вычетов по модулю 13.

18. Лемма Гензеля

Лемма Гензеля в своей классической формулировке, принятой в алгебре и теории чисел, утверждает, что разложение полинома на взаимно простые сомножители, выполненное по модулю простого числа p, можно продолжить до разложения в кольце p-адических чисел. Доказательство ее можно найти, например, в монографии Ван дер Вардена [**4**, с. 549]. Основу доказательства составляет итерационный процесс перехода от сравнения по модулю некоторой степени числа p к сравнению по модулю большей степени p. Показывается, что этот переход можно выполнить за конечное число шагов, вопросам сложности в алгебраическом доказательстве уделяется мало внимания. Нас же в первую очередь интересует алгоритм этого перехода с учетом возможности его практической реализации и оценкой его времени работы.

Начнем с изложения леммы Гензеля в простейшем варианте: линейный подъем для двух сомножителей.

Предположим, что $f(x) \in \mathbb{Z}[x]$ и по модулю некоторой степени $q = p^k$ простого числа p получено разложение $f(x)$ на взаимно простые множители: $f \equiv g_k h_k \pmod q$, где $g_k, h_k \in \mathbb{Z}[x]$. Мы хотим продолжить это сравнение до сравнения по модулю p^{k+1}.

На первом шаге мы должны получить разложение $f \equiv g_1 h_1 \pmod p$, что достигается применением алгоритма Берлекэмпа. Предположим, что мы нашли также полиномы $\tilde g$ и $\tilde h$, такие, что

$$1 \equiv g_1 \tilde g + h_1 \tilde h \pmod p \tag{18.1}$$

Эти полиномы можно найти, применяя в кольце $F_p[x]$ расширенный алгоритм Евклида к полиномам h_1 и g_1. Полиномы $\tilde g$ и $\tilde h$ определены неоднозначно, однозначность получается, если мы потребуем, чтобы их степени были ниже степеней полиномов h_1 и g_1 соответственно. В частности, полиномы $\tilde g$ и $\tilde h$ можно заменить их остатками от деления на h_1 и g_1 в кольце $F_p[x]$

Более того, без потери общности мы можем предполагать, что старшие коэффициенты полиномов h_k равны 1, а старшие коэффициенты полиномов g_k совпадают со старшим коэффициентом полинома f. В дальнейшем мы считаем это условие выполненным, хотя оно может противоречить выбору систем представителей по модулю p^k.

Полиномы $g_{k+1}, h_{k+1} \in \mathbb{Z}[x]$ мы будем искать в виде $g_{k+1} = g_k + \hat g_k p^k$, $h_{k+1} = h_k + \hat h_k p^k$. Сравнения

$$\begin{aligned} f &\equiv g_{k+1} h_{k+1} \\ &\equiv (g_k + \hat g_k p^k)(h_k + \hat h_k p^k) \\ &\equiv g_k h_k + (\hat g_k h_k + \hat h_k g_k) p^k + \hat g_k \hat h_k p^{2k} \pmod{p^{k+1}} \\ &\equiv g_k h_k + (\hat g_k h_k + \hat h_k g_k) p^k \pmod{p^{k+1}} \end{aligned}$$

эквивалентны сравнению

$$f - g_k h_k \equiv (\hat g_k h_k + \hat h_k g_k) p^k \pmod{p^{k+1}}.$$

Обе части этого сравнения делятся на p^k. После деления получаем сравнение $\frac{f - g_k h_k}{p^k} \equiv (\hat g_k h_k + \hat h_k g_k) \pmod p$. В правой части этого сравнения мы можем заменить g_k и h_k на g_1 и h_1 соответственно. Обозначим $d_k = \frac{f - g_k h_k}{p^k}$. Домножим сравнение (18.1) на d_k и приравняем коэффициенты при g_1 и h_1. Получим $\hat g_k \equiv d_k \tilde h \pmod{p, g_1}$, $\hat h_k \equiv d_k \tilde g \pmod{p, h_1}$.

Итак, алгоритм линейного подъема Гензеля можно записать в следующем виде.

А30. Алгоритм (линейного подъема для двух сомножителей).
Дано: $f(x)$, $g_1(x)$, $h_1(x)$, $\tilde{g}(x)$, $\tilde{h}(x) \in \mathbb{Z}[x]$,
$p \in \mathbb{Z}$ — простое число,
$f(x) \equiv g_1(x)h_1(x) \pmod{p}$,
$1 \equiv g_1(x)\tilde{g}(x) + h_1(x)\tilde{h}(x) \pmod{p}$, $k \in \mathbb{N}$
Надо: g и h такие, что $f(x) \equiv g(x)h(x) \pmod{p^k}$

Начало
$g := g_1$
$h := h_1$
цикл для t **от** 1 **до** $k-1$
$d := \dfrac{f - g \cdot h}{p^t} \pmod{p}$
$g_c := d \cdot \tilde{h} \pmod{p, g_1}$
$h_c := d \cdot \tilde{g} \pmod{p, h_1}$
$g := g + g_c \cdot p^t$
$h := h + h_c \cdot p^t$
конец цикла
Конец

Отметим, что для применения этого алгоритма для произвольного числа сомножителей нужно получить соответствующее представление единицы:

$$1 \equiv \sum_i \left(\prod_{j \neq i} g[j] \right) \tilde{g}[i] \pmod{p},$$

в котором $\deg \tilde{g}[i] < \deg g[i]$ (индекс в квадратных скобках означает номер сомножителя). Один из способов получения такого представления заключается в поочередном выделении одного из делителей полинома f и последовательном применении расширенного алгоритма Евклида. Другой способ — искать полиномы $\tilde{g}[i] \pmod{p}$ в кольце $F_p[x]$ методом неопределенных коэффициентов. Относительно этих коэффициентов получается система линейных уравнений порядка $n = \deg f$, условие невырожденности которой совпадает с условием, что полиномы $g[i]$ не имеют общих делителей. (Нетрудно заметить, что нам нужно решить задачу, эквивалентную разложению дроби $\frac{1}{\left(\prod_i g[i](x)\right)} \pmod{p}$ в сумму простейших.)

Снова предполагаем, что старший коэффициент полинома $g[1]$ совпадает со старшим коэффициентом полинома f, а старшие коэффициенты остальных сомножителей $g[i]$ равны 1.

А31. Алгоритм (линейного подъема для нескольких множителей).
Дано: $f(x)$, $g_1[i](x)$, $\tilde{g}[i](x) \in \mathbb{Z}[x]$ $i = 1..r$,
$p \in \mathbb{Z}$ — простое число,
$f(x) \equiv \prod\limits_i g_1[i](x) \pmod p$,
$1 \equiv \sum\limits_i \prod\limits_{j \neq i} g_1[j](x)\tilde{g}[i](x) \pmod p$, $k \in \mathbb{N}$
Надо: $g[i]$ такие, что $f(x) \equiv \prod\limits_i g[i](x) \pmod{p^k}$

Начало
цикл для i **от** 1 **до** r
$g[i] := g_1[i]$
конец цикла
цикл для t **от** 1 **до** $k-1$
$d := \dfrac{f - \prod\limits_i g[i]}{p^t} \pmod p$
цикл для i **от** 1 **до** r
$g_c := d \cdot \tilde{g}[i] \pmod{p, g_1[i]}$
$g[i] := g[i] + g_c \cdot p^t$
конец цикла
конец цикла
Конец

Изложим теперь вариант леммы Гензеля, основанный на квадратичном подъеме, т. е. на переходе от сравнения по модулю q к сравнению по модулю q^2. Основное его отличие от линейного заключается в том, что сравнение $1 \equiv \sum\limits_i \prod\limits_{j \neq i} g_1[j](x)\tilde{g}[i](x) \pmod p$, заменяется аналогичным сравнением по переменному модулю q. Естественно, что такое сравнение недостаточно выполнить один раз, необходимо вычислять его в основном цикле, что существенно повышает сложность этого цикла.

Рассмотрим задачу в следующей постановке.

Дано: полином $f(x) \in \mathbb{Z}[x]$, число q взаимно простое с $\mathrm{lc}(f)$, разложение полинома $f(x)$ на взаимно простые множители над кольцом вычетов по модулю q:

$$f(x) \equiv u_1(x) \dots u_r(x) \pmod q. \tag{18.2}$$

Предполагается, что $\mathrm{lc}(u_1) = \mathrm{lc}(f)$, а старшие коэффициенты всех остальных множителей равны 1. Кроме того, заданы значения переменных $v_1, \dots, v_r$ типа полином, удовлетво-

ряющие условиям:

$$\deg(v_i) < \deg(u_i) \text{ для } 1 \leqslant i \leqslant r \tag{18.3}$$

и

$$\sum_{i=1}^{r} v_i(x)\tilde{u}_i(x) \equiv 1 \pmod{q}, \tag{18.4}$$

где $\tilde{u}_i(x) = \prod_{j=1, j\neq i}^{r} u_j(x)$.

Выше сказано, как найти полиномы $v_i(x)$ для первого шага алгоритма (когда $q = p$ является простым числом).

Надо: поднять это разложение до сравнения по модулю q^2, т. е. найти такие $\hat{u}_1(x), \ldots, \hat{u}_r(x)$, что $\mathrm{lc}(\hat{u}_1) = \mathrm{lc}(f)$, старшие коэффициенты всех остальных множителей равны 1, и $f(x) \equiv \hat{u}_1(x) \ldots \hat{u}_r(x) \pmod{q^2}$. Требуется также найти новые значения переменных $v_1, \ldots, v_r$, удовлетворяющие соотношениям (18.3) и (18.4), в которых полиномы $u(x)$ заменены на $\hat{u}(x)$, а q заменено на q^2.

В рассматриваемом алгоритме факторизации q является степенью p, а множители $u_1, \ldots, u_r$ получаются подъемом неприводимых делителей $f(x)$ по модулю p.

А32. Алгоритм (квадратичный подъем$(q, f(x), u, v)$).

Дано: $f(x) \in \mathbb{Z}[x]$
$q \in \mathbb{Z}$ // основание сравнения
u, v — векторы типа $\mathbb{Z}[x]$ с индексом $1..r$

Надо: q // новое значение основания сравнения
u, v новые значения векторов

Переменные: $t(x) \in \mathbb{Z}[x]$
w — вектор элементов типа $\mathbb{Z}[x]$ с индексом $1..r$

Начало

$t(x) := (f(x) - \prod_{i=1}^{r} u_i(x)) \pmod{q^2}$
$t(x) := t(x)/q$
цикл для i **от** 1 **до** r
$w_i(x) :=$ остаток от деления $t(x) \cdot v_i(x)$ на $u_i(x)$ по $\pmod{q}$
$u_i(x) := u_i(x) + q \cdot w_i(x)$
конец цикла
$t(x) := (1 - \sum_{i=1}^{r} v_i(x)\tilde{u}_i(x)) \pmod{q^2}$
$t(x) := t(x)/q$

цикл для i **от** 1 **до** r
$w_i(x) :=$ остаток от деления $t(x) \cdot v_i(x)$ на $u_i(x)$ по $\pmod q$
$v_i(x) := v_i(x) + q \cdot w_i(x)$
конец цикла
Конец

Работа алгоритма начинается с вычисления вспомогательного многочлена $t(x)$. Заметим, что из условий, наложенных на старшие коэффициенты, следует, что $\deg t < \deg f$. Кроме того, из (18.2) следует, что $t(x) \equiv 0 \pmod q$, поэтому деление во второй строке выполняется нацело. В первом цикле мы ищем многочлены $\hat u_i(x)$ в виде $u_i(x) + qw_i(x)$, для чего находим $w_i(x)$, такие, что $\deg w_i < \deg u_i$ и

$$\sum_i w_i(x)\tilde u_i(x) \equiv t(x) \pmod q. \tag{18.5}$$

Условию (18.5) удовлетворяют многочлены $t(x)v_i(x)$, но для них не выполняется ограничение по степеням. При переходе от $t(x) \cdot v_i(x)$ к его остатку от деления на $u_i(x)$ значение соответствующего слагаемого по модулю $u_i(x)\tilde u_i(x) = \prod\limits_i u_i(x)$ не изменится. Выполнение равенства (18.5) после замены всех полиномов $t \cdot v_i$ соответствующими остатками следует из того, что степени и левой, и правой его части меньше степени полинома $f(x)$.

По завершении работы первого цикла многочлены $\hat u_i(x)$ найдены, и мы переходим к модификации полиномов v_i. Снова вводим вспомогательный многочлен $t(x)$. Из условий (18.3) следует, что $\deg t < \deg f$, а из (18.4) — что $t(x) \equiv 0 \pmod q$, так что в следующей строке деление выполняется нацело.

В цикле мы ищем многочлены $\hat v_i(x)$ в виде $v_i(x) + q \cdot w_i(x)$, для чего находим $w_i(x)$, такие, что $\deg w_i < \deg u_i$ и

$$\sum_i \tilde w_i(x) \cdot u_i(x) \equiv t(x) \pmod q \tag{18.6}$$

Условию (18.6) удовлетворяют полиномы $t(x) \cdot v_i(x)$, но для них не выполняется ограничение по степеням; при переходе от $t(x) \cdot v_i(x)$ к его остатку от деления на $u_i(x)$ значение соответствующего слагаемого по модулю $u_i(x)\tilde u_i(x) = \prod\limits_i u_i(x)$ не изменится. Выполнение равенства (18.6) после замены всех полиномов $t \cdot v_i$ соответствующими остатками следует из того, что степени и левой, и правой его части меньше степени полинома $f(x)$.

18.1. Обсуждение алгоритма. Выше изложена общая схема алгоритма факторизации, основанного на разложении полинома над

полем p-адических чисел и на рассмотрении произведений неприводимых над этим полем множителей. Различные этапы алгоритма допускают некоторые вариации, часть из которых мы и обсудим.

18.1. Замечание. Наибольшее количество операций в рассмотренном алгоритме факторизации требуется при выполнении перебора множителей. Версия алгоритма, излагаемая Калтофеном в [**10**], предполагает, что старший коэффициент первого множителя над полем $\mathbb{Z}/p\mathbb{Z}$ совпадает со старшим коэффициентом исходного полинома $f(x) \in \mathbb{Z}[x]$. При этом из перебора исключался первый сомножитель, перебор осуществлялся по всем подмножествам множества $\{2, \ldots, r\}$, максимальное возможное их количество равно 2^{r-1}. Если первый сомножитель разделить на $\mathrm{lc}(f)$, что можно выполнить в кольце $\mathbb{Z}p$, то достаточно организовать перебор только по тем подмножествам множества $\{1, \ldots, r\}$, которые содержат не более $[r/2]$ элементов. В действительности деление на $\mathrm{lc}(f)$ происходит не в кольце $\mathbb{Z}p$, а в некотором кольце вычетов $\mathbb{Z}/q\mathbb{Z}$, где q является степенью p. Целесообразно, по-видимому, это деление выполнять после подъема разложения на неприводимые множители до сравнения по модулю q. При этом коэффициенты полинома $f/\mathrm{lc}(f)$ увеличатся, что потребует большего времени для выполнения пробных делений, однако более существенным представляется сокращение времени работы за счет меньшего количества рассматриваемых вариантов перебора.

18.2. Замечание. Ограничение вариантов перебора можно организовать не по максимальному количеству сомножителей, а по максимальной степени делителя. Достаточно ограничиться степенью $[n/2]$, где $n = \deg(f)$. При этом получается лучшее ограничение на необходимую точность разложения q. Количество рассматриваемых вариантов может быть в этом случае существенно б/'ольшим.

18.3. Замечание. Как отмечалось выше, проверку, представляет ли произведение $g(x)$ неприводимых над O_p полиномов делитель $f(x)$ в кольце $\mathbb{Z}[x]$, целесообразнее производить путем пробного деления $f(x)$ на $g(x)$. Напомним, что коэффициенты полинома $g(x)$ вычислены с определенной точностью, т. е. по модулю некоторого числа q, и представлены целыми числами. Прежде чем выполнять деление полинома $f(x)$ на $g(x)$, целесообразно проверить выполнение некоторых необходимых признаков делимости: например, свободный член полинома $g(x)$ должен делить свободный член полинома $f(x)$, можно оценить допустимую величину второго по старшинству коэффициента в $g(x)$ и сравнить ее с фактической и т. д.

18.4. Замечание. В процессе деления полиномов коэффициенты частного могут получиться по абсолютной величине больше, чем допустимые значения для коэффициентов делителя полинома $f(x)$. В таком случае деление нужно немедленно прекращать и переходить к следующей комбинации делителей.

18.5. Замечание. При изложении алгоритма уточнения решения мы пользовались квадратичным подъемом, который позволяет переходить от сравнения по модулю q к сравнению по модулю q^2. Чтобы избежать многократного превышения достигнутой точности над требуемой, на последнем шаге можно ограничиться меньшим значением q, либо применить линейный подъем.

18.6. Замечание. Как отмечалось выше, одно из преимуществ использования p-адической метрики состоит в том, что неприводимые по модулю p многочлены могут иметь сколь угодно высокие степени. Может возникнуть предположение, что для любого полинома $f(x) \in \mathbb{Z}[x]$ возможно выбрать простое число p так, что разложение $f(x)$ по модулю p на неприводимые множители будет совпадать с разложением $f(x)$ в кольце $\mathbb{Z}[x]$. Эта гипотеза неверна, можно привести пример неприводимого в $\mathbb{Z}[x]$ многочлена сколь угодно большой степени, который по модулю любого простого p разлагается на линейные или квадратичные множители. Берлекэмпом следующая теорема приписывается Х.П.Ф. Свиннертону-Дайеру.

18.7. Теорема. *Пусть n — целое число, а $p_1, \ldots, p_n$ — различные положительные простые числа. Тогда полином $f_{p_1 \ldots p_n}(x)$ со старшим коэффициентом, равным единице и степени 2^n, корни которого равны $e_1\sqrt{p_1} + \cdots + e_n\sqrt{p_n}$, причем $e_i = \pm 1$ для всех $1 \leqslant i \leqslant n$, имеет целые коэффициенты и неприводим в $\mathbb{Z}[x]$. Более того, для любого простого числа q полином $f_{p_1 \ldots p_n}(x)$ по модулю q раскладывается на неприводимые в $\mathbb{Z}_q[x]$ полиномы степени не выше второй.*

Для доказательства теоремы нам потребуется знакомство с основными фактами теории Галуа. Читателю, не знакомому с теорией Галуа, рекомендуется либо ознакомиться с нею, например, просмотрев соответствующую главу в монографии ван дер Вардена, либо пропустить доказательство данной теоремы, что можно сделать без существенного ущерба для понимания дальнейшего материала.

Доказательство. Пользуемся следующими обозначениями:
$f_k(x) = f_{p_1 \ldots p_k}(x)$ и
$K_k = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$, $1 \leqslant k \leqslant n$.

Методом математической индукции докажем, что $f_n(x) \in \mathbb{Z}[x]$, $[K_n : \mathbb{Q}] = 2^n$ и $\theta = \sqrt{p_1} + \cdots + \sqrt{p_n}$ — примитивный элемент расширения K_n над $\mathbb{Q}$.

Для $n = 1$ эти факты очевидны.

Пусть $n > 1$. Из предположения индукции $f_{n-1}(x) \in \mathbb{Z}[x]$ и из соотношения $f_n(x) = f_{n-1}(x + \sqrt{p_n})f_{n-1}(x - \sqrt{p_n})$ следует, что $f_n(x) \in \mathbb{Z}[\sqrt{p_n}, x]$, причем коэффициенты симметричны относительно $\sqrt{p_n}$ и $-\sqrt{p_n}$. Из фундаментальной теоремы о симметрических функциях следует, что эти коэффициенты должны быть целыми. Из предположения индукции $[K_{n-1} : \mathbb{Q}] = 2^{n-1}$ заключаем, что множество

$$B_k = \{1\} \bigcup \{\sqrt{p_{i_1} \dots p_{i_j}} | j = 1, \dots, k, \quad 1 \leqslant i_1 < i_2 < \cdots < i_j \leqslant k\}$$

образует базис линейного пространства K_k над $\mathbb{Q}$ при $1 \leqslant k \leqslant n-1$.

Покажем, что $\sqrt{p_n}$ не принадлежит линейному пространству, порожденному множеством B_{n-1}.

Предположим противное. Тогда существуют рациональные числа $r_0, \dots, r_{i_1 \dots i_j}$, такие, что

$$r_0 + \sum_{1 \leqslant i_1 < \cdots < i_j < n} r_{i_1 \dots i_j} \sqrt{p_{i_1} \dots p_{i_j}} = \sqrt{p_n} \tag{18.7}$$

Поскольку все $p_i, 1 \leqslant i \leqslant n$, — различные простые числа, в левой части равенства (18.7) содержится не менее двух ненулевых коэффициентов. Тогда существует p_k, такое, что в одном из ненулевых слагаемых содержится $\sqrt{p_k}$, а в другом — нет. Без потери общности полагаем $p_k = p_{n-1}$. Тогда равенство (18.7) можно переписать в виде

$$s_0 + s_1 \sqrt{p_{n-1}} = \sqrt{p_n}, \text{ где } s_0, s_1 \in K_{n-2} \tag{18.8}$$

Из линейной независимости над $\mathbb{Q}$ элементов множества B следует, что $s_0 \neq 0$ и $s_1 \neq 0$. Возведя обе части равенства (18.8) в квадрат и выполнив несложные преобразования, получим

$$\sqrt{p_{n-1}} = (p_n - s_0^2 - s_1^2 p_{n-1})/2 s_0 s_1 \in K_{n-2},$$

что противоречит предположению индукции. Следовательно, $[K_n : K_{n-1}] = 2$ и $[K_n : \mathbb{Q}] = 2^n$.

Покажем, что $K_n = \mathbb{Q}(\theta)$.

Пусть $\alpha_1, \alpha_2, \dots, \alpha_{2^{n-1}}$ — корни полинома $f_{n-1}(x)$, причем $\alpha_1 = \sqrt{p_1} + \cdots + \sqrt{p_{n-1}}$. Рассмотрим полиномы $g_1(x) = f_{n-1}(\alpha_1 + \sqrt{p_n} - x)$ и $g_2(x) = x^2 - p_n$. Очевидно, что $g_1, g_2 \in \mathbb{Q}(\theta)[x]$ и имеют общий корень $\sqrt{p_n}$. Однако $g_1(-\sqrt{p_n}) \neq 0$, так как все корни полинома $f_1(x)$ лежат в поле K_{n-1}, а $\sqrt{p_n} \notin K_{n-1}$. Следовательно, НОД$(g_1, g_2) =$

$= x - \sqrt{p_n} \in \mathbb{Q}(\theta)[x]$, значит $\theta \in \mathbb{Q}(\alpha_1, \sqrt{p_n})$ и $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha_1, \sqrt{p_n})$. По предположению индукции $K_{n-1} = \mathbb{Q}(\alpha_1)$, следовательно, $\mathbb{Q}(\theta) = K_n$. Неприводимость полинома $f_n(x)$ следует теперь из равенства степени этого полинома степени расширения над $\mathbb{Q}$, порождаемого его корнем.

Свойство разложимости по модулю любого простого числа q выводится из следующих фактов. Все квадратные корни из элементов p_i лежат в некотором квадратичном расширении поля $\mathbb{Z}/q\mathbb{Z}$, а поскольку все квадратичные расширения поля $\mathbb{Z}/q\mathbb{Z}$ изоморфны, то можно считать, что все корни полинома f_n по модулю q лежат в поле Галуа $GF(q^2)$. Если у полинома f_n имеется неприводимый по модулю q множитель степени $m > 2$, то его корни порождают поле $GF(q^m)$ и не могут быть элементами поля $GF(q^2)$. □

18.8. Упражнение ([**7**, стр. 192]). Доказать, что полином x^4+1 является неприводимым над $\mathbb{Z}$, но разлагается на множители по модулю любого простого числа p.

18.9. Упражнение. Организовать перебор вариантов сомножителей с ограничением по суммарной степени.

18.10. Упражнение. Пусть $f(x), g(x) \in \mathbb{Z}[x]$, $g(x)$ делит $f(x)$ в кольце $\mathbb{Q}[x]$. Получить оценку для абсолютной величины коэффициента, следующего за старшим в $g(x)$, через коэффициенты полинома $f(x)$.

19. Редуцированные базисы решетки

19.1. Определение. *Решеткой* в n-мерном векторном пространстве над полем вещественных чисел $\mathbb{R}$ или над полем рациональных чисел $\mathbb{Q}$ называется свободный $\mathbb{Z}$-модуль L ранга n, т. е. существует базис $b_1, \ldots, b_n$ пространства $\mathbb{R}^n$ (соответственно $\mathbb{Q}^n$), такой, что

$$L = \sum_{i=1}^{n} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{n} r_i b_i \mid r_i \in \mathbb{Z}, \quad 1 \leqslant i \leqslant n \right\}.$$

В этом случае n называется *рангом* решетки, а множество векторов $b_1, \ldots, b_n$ — ее *базисом*.

19.2. Определение. *Детерминантом* $d(L)$ решетки L называется положительное число, определяемое формулой

$$d(L) = |\det(b_1, b_2, \ldots, b_n)|,$$

для некоторого базиса $b_1, b_2, \ldots, b_n$ решетки L.

19.3. Упражнение. Показать, что определение 19.2 является корректным, т. е. $d(L)$ не зависит от выбора базиса решетки L.

Прежде чем дать определение редуцированного базиса решетки, нам необходимо напомнить *процесс ортогонализации Грама–Шмидта*. Векторы b_i^* $(1\leqslant i\leqslant n)$ и вещественные числа $\mu_{i,j}$ $(1\leqslant j<i\leqslant n)$ определяются по индукции формулами

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*, \tag{19.1}$$

$$\mu_{i,j} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}. \tag{19.2}$$

Отметим, что b_i^* — проекция вектора b_i на ортогональное дополнение к пространству $\sum\limits_{j=1}^{i-1} \mathbb{R}b_j$ в пространстве $\sum\limits_{j=1}^{i} \mathbb{R}b_j$ и что $\sum\limits_{j=1}^{i} \mathbb{R}b_j = \sum\limits_{j=1}^{i} \mathbb{R}b_j^*$ для $1 \leqslant i \leqslant n$. Таким образом векторы $b_1^*, \ldots, b_n^*$ образуют ортогональный базис пространства $\mathbb{R}^n$.

В дальнейшем символ $|\ |$ используется как для обозначения абсолютной величины вещественных или комплексных чисел, так и для обозначения евклидовой длины вектора в вещественном векторном пространстве.

19.4. Упражнение. Показать, что

$$|\det(b_1^*, \ldots, b_n^*)| = d(L) = \prod_{i=1}^{n} |b_i^*|.$$

19.5. Упражнение. Показать, что для любого базиса $b_1, \ldots, b_n$ решетки L выполняется *неравенство Адамара*

$$d(L) \leqslant \prod_{i=1}^{n} |b_i|. \tag{19.3}$$

19.6. Определение. Базис $b_1, \ldots, b_n$ решетки L называется *редуцированным*, если выполняются неравенства

$$|\mu_{i,j}| \leqslant 1/2 \text{ для } 1 \leqslant j \leqslant i \leqslant n \tag{19.4}$$

и

$$|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geqslant \frac{3}{4} |b_{i-1}^*|^2 \quad \text{для} \quad 1 < i \leqslant n. \tag{19.5}$$

Векторы $b_i^* + \mu_{i,i-1} b_{i-1}^*$ и b_{i-1}^* имеют простой геометрический смысл — это проекции векторов b_i и b_{i-1} на ортогональное допол-

нение к пространству $\sum_{j=1}^{i-2} \mathbb{R}b_j$ в $\sum_{j=1}^{i} \mathbb{R}b_j$. Константа 3/4 выбирается в значительной мере произвольно: вместо нее можно взять любое фиксированное вещественное число y, удовлетворяющее условию $1/4 < y < 1$.

Грубо говоря, редуцированный базис состоит из «почти ортогональных» векторов, расположенных в порядке «почти неубывания длин».

Использование редуцированных базисов решеток для целей факторизации многочленов основано на следующем свойстве таких базисов: если $b_1, \ldots, b_n$ — редуцированный базис решетки L, то

$$|b_1|^2 \leqslant 2^{n-1}|x|^2$$

для любого вектора $x \in L$. К доказательству этого свойства и его обобщений мы сейчас и переходим.

19.7. Предложение. *Пусть $b_1, \ldots, b_n$ — редуцированный базис решетки L в $\mathbb{R}^n$ и векторы $b_1^*, \ldots, b_n^*$ получены из этого базиса процессом ортогонализации Грама — Шмидта. Тогда*

$$|b_j|^2 \leqslant 2^{i-1} \cdot |b_i^*|^2 \quad \text{для} \quad 1 \leqslant j \leqslant i \leqslant n, \tag{19.6}$$

$$d(L) \leqslant \prod_{i=1}^{n} |b_i| \leqslant 2^{n(n-1)/4} \cdot d(L), \tag{19.7}$$

$$|b_1| \leqslant 2^{(n-1)/4} \cdot d(L)^{1/n}. \tag{19.8}$$

Доказательство. Сначала докажем формулу (19.6). Из формул (19.4) и (19.5) получаем

$$|b_i^*|^2 \geqslant \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \cdot |b_{i-1}^*|^2 \geqslant \frac{1}{2} \cdot |b_{i-1}^*|^2 \tag{19.9}$$

для $1 < i \leqslant n$, откуда по индукции выводится неравенство

$$\begin{aligned} |b_i|^2 &= |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 |b_j^*|^2 \\ &\leqslant |b_i^*|^2 + \sum_{j=1}^{i-1} \frac{1}{4} \cdot 2^{i-j} |b_i^*|^2 \\ &= \left(1 + \frac{1}{4}(2^i - 2)\right) \cdot |b_i^*|^2 \\ &\leqslant 2^{i-1} \cdot |b_i^*|^2. \end{aligned}$$

Из этих формул следует, что

$$|b_j|^2 \leqslant 2^{j-1} \cdot |b_j^*|^2 \leqslant 2^{i-1} \cdot |b_i^*|^2$$

для $1 \leqslant j \leqslant i \leqslant n$. Таким образом, формула (19.6) доказана.

Для доказательства формулы (19.7) достаточно воспользоваться упражнением 19.4 и неравенствами

$$|b_i^*| \leqslant |b_i| \leqslant 2^{(i-1)/2} \cdot |b_i^*|.$$

Полагая $j = 1$ в формуле (19.6) и перемножив левые и правые части этой формулы для i от 1 до n, получим неравенство (19.8). Этим заканчивается доказательство предложения 19.7. □

19.8. Упражнение. Показать, что если в формуле (19.5) заменить 3/4 на некоторое вещественное число y, $1/4 < y < 1$, то появляющиеся в формулах (19.6), (19.7) и (19.8) степени числа 2 заменятся на такие же степени числа $4/(4y-1)$.

19.9. Предложение. *Пусть $b_1, \ldots, b_n$ — редуцированный базис решетки L. Тогда для любого ненулевого вектора $x \in L$ выполняется неравенство*

$$|b_1|^2 \leqslant 2^{n-1} \cdot |x|^2.$$

Доказательство. Любой вектор $x \in L$ может быть выражен через векторы базиса $b_1, \ldots, b_n$ с целыми коэффициентами r_i, а через векторы $b_1^*, \ldots, b_n^*$ — в виде линейной комбинации с вещественными коэффициентами r_i', т. е.

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r_i' b_i^*.$$

Если i — наибольший индекс, для которого $r_i \neq 0$, то $|r_i'| = |r_i| \geqslant 1$. Таким образом,

$$2^{n-1}|x|^2 \geqslant 2^{n-1} r_i'^2 \cdot |b_i^*|^2 \geqslant 2^{n-1}|b_i^*|^2 \geqslant 2^{i-1}|b_i^*|^2 \geqslant |b_1|^2.$$

Последние два неравенства вытекают из формулы (19.6). □

Обобщением полученного результата является следующее

19.10. Предложение. *Пусть $b_1, \ldots, b_n$ — редуцированный базис решетки L, $x_1, \ldots, x_t$ — линейно независимые векторы решетки L. Тогда для любого j от 1 до t выполняется неравенство*

$$|b_j|^2 \leqslant 2^{n-1} \cdot \max\{|x_1|^2, \ldots, |x_t|^2\}.$$

Доказательство. Выразим векторы x_j через элементы базиса b_i:

$$x_j = \sum_{i=1}^{n} r_{ij} b_i,$$

где $r_{ij} \in \mathbb{Z}$ $(1 \leqslant i \leqslant n)$ для $1 \leqslant j \leqslant t$. Для каждого фиксированного j через $i(j)$ обозначим наибольшее значение i, для которого $r_{ij} \neq 0$. Перенумеруем векторы x_j так, чтобы числа $i(j)$ не убывали, т. е. $i(1) \leqslant i(2) \leqslant \cdots \leqslant i(t)$. Из доказательства предыдущего предложения можно получить неравенство

$$|x_j|^2 \geqslant |b^*_{i(j)}|^2 \quad \text{для всех } j \text{ от 1 до } t. \tag{19.10}$$

Покажем, что $j \leqslant i(j)$ для всех j от 1 до t. Если это неравенство для некоторого j не выполняется, то все векторы $x_1, \ldots, x_j$ принадлежат подпространству $\mathbb{R}b_1 + \mathbb{R}b_2 + \cdots + \mathbb{R}b_{j-1}$, что противоречит линейной независимости векторов $x_1, \ldots, x_t$. Воспользовавшись неравенством $j \leqslant i(j)$ и формулами (19.6) и (19.10), получаем для всех j от 1 до t неравенство

$$\begin{aligned} |b_j|^2 &\leqslant 2^{i(j)-1} \cdot |b^*_{i(j)}|^2 \\ &\leqslant 2^{n-1} \cdot |b^*_{i(j)}|^2 \\ &\leqslant 2^{n-1} \cdot |x_j|^2. \end{aligned}$$

Этим доказательство предложения 19.10 заканчивается. □

20. Редуцирование базиса в решетке

В этом параграфе рассмотрим алгоритм построения редуцированного базиса решетки, полученный в работе [**24**]. Определение решетки и редуцированного базиса приведены в параграфе 19. Там же описаны основные свойства редуцированных базисов, которые понадобятся нам в алгоритмах факторизации многочленов.

Ниже сформулирован и обоснован алгоритм построения редуцированного базиса решетки. Построение редуцированного базиса ведем, последовательно присоединяя очередной (k-ый) элемент исходного базиса решетки и редуцируя базис подрешетки, натянутой на векторы с 1-го по k-ый. Алгоритм содержит два основных шага: на одном из них мы из присоединяемого вектора вычитаем целые кратные векторов, уже включенных в редуцированный базис, чтобы обеспечить выполнение условия (19.4). При этом длина редуцированной части базиса не меняется. Второй шаг, направленный на выполнение условия (19.5), сводится к перестановке добавляемого

вектора с последним вектором, уже включенным в редуцированный базис, при такой перестановке длина редуцированной части базиса уменьшается на 1. Переменная k указывает номер элемента, который пытаемся присоединить к редуцированной части базиса, т. е. редуцированная часть базиса содержит в каждый момент $k-1$ вектор. Начальное значение k равно 2, т. к. любой базис решетки, порождаемой одним вектором, является редуцированным (условия (19.4) и (19.5) выполняются автоматически, поскольку нет различных индексов).

В описании алгоритма редуцирования базиса пользуемся типом данных "решетка". В отличие от принятых ранее обозначений, здесь значения индексов принадлежат отрезку $1..n$ (а не $0..n-1$), т. е.

решетка: запись(ранг $==n$: $\mathbb{Z}+$
базис: вектор b элементов типа (вектор элементов типа $\mathbb{R}$ или $\mathbb{Q}$ с индексом $1..n$)
с индексом $1..n$

А33. Алгоритм (редуцирование-базиса).
Дано: L — решетка, задаваемая исходным базисом
Надо: L — решетка, задаваемая редуцированным базисом
Обозначения: $n == L$.ранг
$b == L$.базис
Переменные: μ — нижняя треугольная матрица коэффициентов, вычисляемых по формулам (19.1) и (19.2)
B — вектор элементов типа $\mathbb{R}$ с индексом $1..n$

Элементы вектора B представляют собой квадраты длин соответствующих векторов из ортогонального базиса b^*, вычисляемого по формулам (19.1) и (19.2).

Начало
начальная установка (L, μ, B)
$k := 2$
цикл пока $k \leqslant n$
обеспечить выполнение условия (19.4) для $i = k$ и $j = k-1$
если условие (19.5) не выполнено, **то**
переставить k-ый элемент базиса b с $(k-1)$-м
если $k > 2$ **то**
$k := k-1$
конец если
иначе
цикл для j **от** $k-2$ **до** 1 **шаг** -1

обеспечить выполнение условия (19.4) для k, j
конец цикла
$k := k + 1$
конец если
конец цикла
Конец

Детализируем предложенный алгоритм.

А34. Алгоритм (начальная-установка).
Дано: L — решетка
Надо: μ — нижняя треугольная матрица коэффициентов, вычисляемых по формулам (19.1) и (19.2).
B — вектор элементов типа $\mathbb{R}$ с индексом $1..n$. Элементы вектора B представляют собой квадраты длин соответствующих векторов из ортогонального базиса $b1$, вычисляемого по формулам (19.1) и (19.2).
Переменные: $b1$ — вектор элементов типа (вектор элементов типа $\mathbb{R}$ с индексом $1..n$) с индексом $1..n$
Обозначения: $n == L$.ранг
$b == L$.базис исходный базис решетки
$(a, b) ==$ скалярное произведение векторов

Начало
цикл для q **от** 1 **до** n
$b1[q] := b[q]$
цикл для l **от** 1 **до** $q - 1$
$$\mu[q, l] := \frac{(b[q], b1[l])}{B[l]}$$
$b1[q] := b1[q] - \mu[q, l] \cdot b1[l]$
конец цикла
$B[q] := (b1[q], b1[q])$
конец цикла
Конец

Отметим, что в предлагаемой версии алгоритма переменная $b1$ (двумерный массив, соответствующий ортогональному базису b^*) локальна, в остальной части алгоритма этот базис в явном виде не используется. Применяется вектор B, элементы которого представляют собой квадраты длин ортогонального базиса, что позволяет значительно экономить память, используемую основной программой (вместо двумерного массива хранится одномерный). При этом нужно проследить, как изменяются компоненты вектора B при различных

выполняемых преобразованиях, что сделано при описании соответствующих предписаний.

А35. Алгоритм (обеспечить-выполнение-условия-(19.4)).
Дано: L — решетка
μ — матрица "проекций"
$k > j$ — индексы
Надо: μ — треугольная матрица коэффициентов,
вычисляемых по формулам (19.1) и (19.2).
Переменные: r — целое

Начало
если $|\mu[k,j]| > 1/2$ **то**
$r :=$ ближайшее целое к $\mu[k,j]$
$b[k] := b[k] - r \cdot b[j]$
цикл для i **от** 1 **до** $j-1$
$\mu[k,i] := \mu[k,i] - r \cdot \mu[j,i]$
конец цикла
$\mu[k,j] := \mu[k,j] - r$
конец если
Конец

Элементы нижней треугольной матрицы μ вычисляются по формулам (19.2). В данном алгоритме меняем только вектор с индексом k. При этом меняется только k-ая строка матрицы μ, из нее вычитается j-ая строка матрицы $(\mu - E)$, умноженная на r. (E — единичная матрица.)

Прежде чем переходить к формулировке алгоритма перестановки k-го элемента базиса с $(k-1)$-м, выведем соответствующие формулы. Пусть $b_1, \ldots, b_n$ — текущий базис, ему соответствует ортогональный базис b^* и нижняя треугольная матрица μ. Элементы нового базиса обозначим буквой c с соответствующим индексом, соответствующий ортогональный базис — c^*, нижнюю треугольную матрицу — ν. Вычислить элементы базиса c не представляет труда:

$$c_{k-1} = b_k, \quad c_k = b_{k-1}, \quad c_i = b_i \quad \text{для} \quad i \neq k, k-1. \tag{20.1}$$

Переходим к вычислению ортогонального базиса. Как отмечалось выше, левая часть равенства (19.5) представляет собой квадрат длины ортогонального дополнения i-го вектора к подпространству, порожденному векторами с 1-го по $(i-2)$-ой.

Таким образом,

$$c^*_{k-1} = b^*_k + \mu_{k,k-1} b^*_{k-1}. \tag{20.2}$$

Для вычисления c_k^* спроектируем b_{k-1}^* на ортогональное дополнение к $\mathbb{R}c_{k-1}^*$. Получим

$$\nu_{k,k-1} = \frac{(b_{k-1}^*, c_{k-1}^*)}{(c_{k-1}^*, c_{k-1}^*)}$$

$$= \mu_{k,k-1}|b_{k-1}^*|^2/|c_{k-1}^*|^2 \tag{20.3}$$

$$c_k^* = b_{k-1}^* - \nu_{k,k-1}c_{k-1}^*. \tag{20.4}$$

$$c_i^* = b_i^* \quad \text{для} \quad i \neq k-1, k. \tag{20.5}$$

Для вычисления коэффициентов ν нам понадобится выразить старый ортогональный базис через новый. Из соотношений (20.2), (20.4) и (20.5) получаем

$$b_{k-1}^* = \nu_{k,k-1}c_{k-1}^* + c_k^* \tag{20.6}$$

$$b_k^* = (1 - \mu_{k,k-1}\nu_{k,k-1})c_{k-1}^* - \mu_{k,k-1}c_k^*$$

$$= (|b_k^*|^2/|c_{k-1}^*|^2) \cdot c_{k-1}^* - \mu_{k,k-1}c_k^*. \tag{20.7}$$

Подставив соотношения (20.1)–(20.7) в формулу (19.1) и приведя подобные члены, получим для $i > k$

$$\nu_{i,k-1} = \mu_{i,k-1}\nu_{k,k-1} + \mu_{i,k}|b_k^*|^2/|c_{k-1}^*|^2, \tag{20.8}$$

$$\nu_{i,k} = \mu_{i,k-1} - \mu_{i,k}\mu_{k,k-1}. \tag{20.9}$$

Наконец,

$$\nu_{k-1,j} = \mu_{k,j}, \qquad \nu_{k,j} = \mu_{k-1,j} \quad \text{для} \quad 1 \leqslant j < k-1; \tag{20.10}$$

$$\nu_{i,j} = \mu_{i,j} \quad \text{для} \quad 1 \leqslant j < i \leqslant n, \quad \{i,j\} \cap \{k-1,k\} = \emptyset. \tag{20.11}$$

Реализация полученных формул описывается следующим алгоритмом:

А36. Алгоритм (переставить-k-ый-элемент-базиса-b-с-$(k-1)$-м).
Дано: $k \in \mathbb{Z}$,
L — решетка,
μ — нижняя треугольная матрица коэффициентов, вычисляемых по формулам (19.1) и (19.2),
B — вектор элементов типа вещественное число с индексом $1..n$. Элементы вектора B — это квадраты длин соответствующих векторов из ортогонального базиса $b1$, вычисляемого по формулам (19.1) и (19.2).
Надо: L, μ, B
В векторе L.базис поменялись местами два элемента. Соответствующие изменения произошли с элементами матрицы μ и вектора B.

Обозначения: $n == L.$ранг
$b == L.$базис
Переменные: $BB, \mu\mu$ — вещественные числа

Начало
$\mu\mu := \mu[k, k-1]$
$BB := B[k] + \mu\mu^2 \cdot B[k-1]$
$\mu[k, k-1] := \dfrac{\mu\mu \cdot B[k-1]}{BB}$
$B[k] := \dfrac{B[k-1] \cdot B[k]}{BB}$
$B[k-1] := BB$
$\begin{pmatrix} b[k-1] \\ b[k] \end{pmatrix} := \begin{pmatrix} b[k] \\ b[k-1] \end{pmatrix}$
цикл для i **от** 1 **до** $k-2$
$\quad \begin{pmatrix} \mu[k-1, i] \\ \mu[k, i] \end{pmatrix} := \begin{pmatrix} \mu[k, i] \\ \mu[k-1, i] \end{pmatrix}$
конец цикла
цикл для i **от** $k+1$ **до** n
$\quad \begin{pmatrix} \mu[i, k-1] \\ \mu[i, k] \end{pmatrix} := \begin{pmatrix} 1 & \mu[k, k-1] \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu\mu \end{pmatrix} \begin{pmatrix} \mu[i, k-1] \\ \mu[i, k] \end{pmatrix}$
конец цикла
Конец

Переходим к обоснованию алгоритма **A**33 построения редуцированного базиса решетки. Оно состоит из доказательства двух утверждений. Во-первых, докажем, что если алгоритм завершит свою работу, то в результате получим редуцированный базис данной решетки. Во-вторых, докажем, что для любого исходного базиса решетки алгоритм после конечного числа шагов закончит работу.

Для доказательства первого утверждения заметим, что мы выполняем над элементами базиса только элементарные преобразования, которые переводят базис $\mathbb{Z}$-модуля в другой базис того же самого $\mathbb{Z}$-модуля, т. к. и перестановка элементов базиса и прибавление к одному из элементов целого кратного другого — обратимые операции. Таким образом, в любой момент времени b представляет собой базис исходной решетки. Элементы этого базиса с 1-го по $(k-1)$-ый представляют собой редуцированный базис подрешетки, порожденной этими элементами, т. к. для них выполнены условия (19.4) и (19.5). Когда мы производим преобразования вектора $b[k]$, направленные на то, чтобы для него выполнялись условия (19.4), эти преобразования никак не отражаются на векторах с 1-го по $(k-1)$-ый, а

если мы производим перестановку k-го элемента базиса с $(k-1)$-ым, то уменьшаем длину редуцированной части базиса на 1 (если она больше 1; меньше 1 длина редуцированной части базиса быть не может) и одновременно уменьшаем значение k. Для векторов с 1-го по $(k-1)$-ый снова выполнены условия (19.4) и (19.5). Таким образом, если алгоритм завершил свою работу, то получившийся базис — редуцированный базис исходной решетки L.

Прежде чем перейти к доказательству второго утверждения, приведем несколько определений и задач различной степени сложности.

20.1. Упражнение. Пусть $m(L) = \min\{|x|^2 : x \in L, x \neq 0\}$. Показать, что для любой решетки L выполняется неравенство $m(L) > 0$.

Введем обозначение

$$d_i = \det((b_j, b_l))_{1 \leqslant j,l \leqslant i} \text{ для } 0 \leqslant i \leqslant n. \tag{20.12}$$

20.2. Упражнение. Показать, что для всех i от 1 до n выполняется равенство $d_i = \prod_{j=1}^{i} |b_j^*|^2$.

Для всех $i > 0$ числа d_i могут быть интерпретированы как квадраты детерминантов решеток ранга i, порожденных векторами $b_1, \ldots, b_i$ в векторных пространствах $\sum_{j=1}^{i} Rb_j$.

20.3. Упражнение. Показать, что каждая такая решетка содержит ненулевой вектор x, удовлетворяющий неравенству

$$|x|^2 \leqslant (4/3)^{(i-1)/2} \cdot d_i^{1/i}.$$

Переходим теперь к доказательству второй части утверждения о корректности алгоритма построения редуцированного базиса. Пусть

$$D = \prod_{j=1}^{n-1} d_i.$$

Из упражнения 20.2 следует, что значение D меняется только тогда, когда изменяется хотя бы один из векторов b_i^*. Это может произойти только при перестановке двух векторов базиса. При этом новое значение $|b_{i-1}^*|$ равно $|b_i^* + \mu_{i\,i-1} b_{i-1}^*|$, что по условию меньше, чем 3/4 от прежнего значения этой величины. Таким образом, при каждой выполняемой перестановке элементов базиса значение величины D умножается на положительное число, меньшее 3/4. Из упражнений 20.1–20.3 следует, что D ограничено снизу некоторой

положительной величиной, следовательно, перестановка элементов выполняется в алгоритме только конечное число раз, обозначим его m. При каждом выполнении перестановки значение i уменьшается на 1, при выполнении команд, следующих за ключевым словом "иначе" в алгоритме, значение i увеличивается на 1. Начальное значение i равно 2, алгоритм продолжает работу до тех пор, пока $i \leqslant n$, следовательно, ситуация "иначе" встречается $m+n-1$ раз, т. е. тело цикла "пока" выполняется конечное число раз. Таким образом, алгоритм завершает работу после выполнения конечного числа шагов. Ниже мы оценим это число для случая, когда все координаты исходного базиса решетки — целые числа.

Итак, переходим к оценке сложности алгоритма построения редуцированного базиса решетки в предположении, что все координаты исходного базиса являются целыми числами. Именно такой случай нам понадобится для получения алгоритма факторизации полиномиальной сложности. Наша цель сейчас — доказательство следующего предложения.

20.4. Предложение. *Пусть $L \subset \mathbb{Z}^n$ — решетка с базисом $b_1, \ldots, b_n$ и предположим, что задано положительное число $B \geqslant 2$, такое, что для любого вектора b_i из исходного базиса решетки выполняется неравенство $|b_i|^2 \leqslant B$. Тогда алгоритм построения редуцированного базиса, описанный выше, требует для своего выполнения $O(n^4 \log B)$ арифметических операций над целыми числами, двоичная длина которых представляет $O(n \log B)$. Таким образом, для построения редуцированного базиса достаточно $O(n^6 \log^3 B)$ бинарных операций.*

Доказательство. Перед началом работы алгоритма величи́ны d_i, определенные формулами (20.12) удовлетворяют неравенству $d_i \leqslant B^i$, что легко следует из упражнения 20.2. Таким образом, перед началом работы алгоритма $D \leqslant B^{n(n-1)/2}$. Из определения D легко следует, что в случае, когда $L \subset \mathbb{Z}^n$, D — неотрицательное целое число, которое не может обратиться в нуль, в силу линейной независимости векторов, составляющих базис решетки. Таким образом, $D \geqslant 1$ во все время работы алгоритма. Выше отмечалось, что при перестановках элементов базиса, выполняемых алгоритмом построения редуцированного базиса, величина D убывает не медленнее геометрической прогрессии со знаменателем 3/4, следовательно, таких перестановок выполняется $O(\log B^{n(n-1)/2}) = O(n^2 \log B)$. Мы

оценили, таким образом, сколько раз в головной программе, в цикле "пока" встречается ситуация "то" в условии "если". Из доказательства конечности времени работы алгоритма следует, что ситуация "иначе" встречается также $O(n^2 \log B)$ раз. Итак, тело цикла в основном алгоритме выполняется $O(n^2 \log B)$ раз. Внутренний цикл в ситуации "иначе" дает еще один множитель n для алгоритма **А**35, который выполняется таким образом $O(n^3 \log B)$ раз. Переходим теперь к оценке сложности отдельных предписаний алгоритма **А**33.

В предписании "начальная-установка" два вложенных цикла дают $O(n^2)$ повторений тела цикла, в котором встречаются векторные операции: скалярное произведение векторов, умножение вектора на число, вычитание векторов, что дает еще один множитель n. При этом арифметические операции выполняются над рациональными числами. Сложность выполнения операций над этими числами оценим несколько позже.

Количество арифметических операций в алгоритме **А**35, как легко видеть, равно $O(n)$, такое же количество операций в алгоритме **А**36. Сравнивая количество проходов через отдельные ветви алгоритма, получаем, что количество арифметических операций в алгоритме представляется величиной $O(n^4 \log B)$, что и утверждалось в первой части предложения.

Оценим теперь сложность выполнения арифметических операций, выполняемых над рациональными числами в процессе работы алгоритма **А**33. Прежде всего, опишем множество значений, которые могут принимать знаменатели всех встречающихся во время вычислений рациональных чисел. Покажем, что в качестве знаменателей всех встречающихся чисел могут быть использованы только числа d_i, вычисляемые по формулам (20.12), а именно:

$$|b_i^*|^2 = \frac{d_i}{d_{i-1}}, \qquad (1 \leqslant i \leqslant n), \tag{20.13}$$

$$d_{i-1} b_i^* \in L \subset \mathbb{Z}^n, \qquad (1 \leqslant i \leqslant n), \tag{20.14}$$

$$d_j \mu_{ij} \in \mathbb{Z}, \qquad (1 \leqslant j < i \leqslant n). \tag{20.15}$$

Первое из этих соотношений следует из упражнения 20.2.

Для доказательства второго соотношения выразим векторы b_i^* с неопределенными коэффициентами y_{ij} через исходный базис:

$$b_i^* = b_i - \sum_{j=1}^{i-1} y_{ij} b_j.$$

Неизвестные коэффициенты с фиксированным первым индексом i определяются из системы линейных уравнений

$$(b_i, b_l) = \sum_{j=1}^{i-1} y_{ij}(b_j, b_l) \qquad (1 \leqslant l \leqslant i-1). \tag{20.16}$$

Решая систему (20.16) методом Крамера, воспользовавшись формулой (20.12) получаем, что $d_{i-1}y_{ij} \in \mathbb{Z}$ для всех допустимых значений индексов. Отсюда уже вытекает соотношение (20.14).

Воспользовавшись соотношениями (19.2), (20.13) и (20.14), получаем цепочку равенств

$$d_j\mu_{ij} = d_j\frac{(b_i, b_j^*)}{(b_j^*, b_j^*)} = d_{j-1}(b_i, b_j^*) = (b_i, d_{j-1}b_j^*) \in Z,$$

чем заканчивается доказательство соотношения (20.15).

Посмотрим теперь, как меняются величины d_i в процессе работы алгоритма. В начале работы алгоритма они вычисляются по формулам (20.12). В процессе работы эти величины меняются только при перестановке элементов базиса (в алгоритме **A**36). В этом случае d_{k-1} заменяется (в обозначениях (20.1)–(20.5)) на

$$d_{k-1} \cdot \frac{|c_{k-1}^*|^2}{|b_{k-1}^*|^2} = d_{k-2} \cdot |c_{k-1}^*|^2,$$

значения d_i при $i \neq k-1$ не меняются. При этом все значения d_i остаются целыми и во все время работы алгоритма удовлетворяют неравенствам $d_i^i \leqslant B$. Таким образом, мы оценили множество чисел, которые могут появляться в вычислениях в качестве знаменателей.

Для оценки числителей достаточно найти верхнюю грань для величин $|b_i^*|^2$, $|b_i|^2$ и $|\mu_{ij}|$. Первая из этих величин оценивается просто: в начале работы алгоритма выполняются неравенства $|b_i^*|^2 \leqslant |b_i|^2 \leqslant B$. В процессе работы величина $\max\{|b_i^*|^2 : 1 \leqslant i \leqslant n\}$ не возрастает, для доказательства чего достаточно заметить, что изменение векторов b_i^* происходит только при перестановке элементов базиса, при этом выполняются неравенства $|c_{k-1}^*|^2 < \frac{3}{4}|b_{k-1}^*|^2$ и $|c_k^*|^2 \leqslant |b_{k-1}^*|^2$, поскольку c_k^* — проекция вектора b_{k-1}^*. Таким образом, во все время работы алгоритма $|b_k^*|^2 \leqslant B$. Оценка величин $|b_i|^2$ и μ_{ij} существенно сложнее. Чтобы получить ее, докажем, что всякий раз в точке проверки условия окончания цикла “пока” выполняются следующие

неравенства:

$$|b_i|^2 \leqslant nB \qquad \text{для } i \neq k; \tag{20.17}$$

$$|b_k|^2 \leqslant n^2(4B)^n, \qquad \text{если } k \neq n+1; \tag{20.18}$$

$$|\mu_{ij}| \leqslant 1/2 \qquad \text{для } 1 \leqslant j < i < k; \tag{20.19}$$

$$|\mu_{ij}| \leqslant (nB^j)^{1/2} \qquad \text{для } 1 \leqslant j < i,\ i > k; \tag{20.20}$$

$$|\mu_{kj}| \leqslant 2^{n-k}(nB^{n-1})^{1/2} \qquad \text{для } 1 \leqslant j < k, \text{ если } k \neq n+1. \tag{20.21}$$

При доказательстве этих неравенств пользуемся следующим соотношением:

$$\mu_{ij}^2 \leqslant \frac{|b_i|^2}{|b_j^*|^2} = \frac{d_{j-1}|b_i|^2}{d_j} \leqslant B^{j-1}|b_i|^2. \tag{20.22}$$

Перед первым выполнением тела цикла неравенства (20.17) и (20.18) следуют из неравенства $|b_i|^2 \leqslant B$, которое выполняется по определению B. Вместе с (20.22) это неравенство дает соотношение $|\mu_{ij}| \leqslant B^{j/2}$, откуда следует (20.19) и (20.20), а учитывая, что $B2$, и (20.21). Таким образом, перед первым выполнением тела цикла неравенства (20.17)–(20.21) справедливы.

Предположим теперь, что неравенства (20.17)–(20.21) выполнены перед началом выполнения тела цикла, и покажем, что эти неравенства будут выполнены и в конце тела цикла, т. е. перед выполнением следующего цикла. Неравенство (20.19) совпадает с (19.4), которое выполняется для текущего k все время работы алгоритма **A**33, в том числе и в начале цикла. Выполнение неравенства (20.17) для $i < k$ следует из соотношений (19.1), (20.19) и неравенства $|b_i^*|^2 < B$. Покажем, что из (20.17) для $i > k$ и из неравенства (20.21) следуют неравенства (20.18) и (20.20). Доказательство (20.18) сводится к разложению b_k в сумму по формуле (19.1), применению неравенства (20.21) и вычислению суммы геометрической прогрессии. Неравенство (20.20) непосредственно вытекает из (20.22) и (20.17).

Итак, покажем, что если перед началом выполнения тела цикла справедливы неравенства (20.17)–(20.21), то и после его выполнения неравенства (20.17) и (20.21) также имеют место. Отдельно рассмотрим два случая: работа алгоритма осуществляется по ветви “то”, т. е. два вектора меняются местами; второй случай — алгоритм идет на ветвь “иначе”, т. е. осуществляется выполнение условия (19.4) для всех $j < k$.

В первом случае множество векторов $\{b_i : i < k\}$ не изменилось (мы поменяли местами k-ый вектор с $(k-1)$-ым и уменьшили после

этого k на 1). Во втором случае множество $\{b_i : i > k\}$ векторов, для которых нам нужно доказать неравенство (20.17), заменилось на собственное его подмножество. Этим заканчивается индуктивный шаг для неравенства (20.17).

Переходим к оценке μ_{kj} (если $k \neq n+1$). Снова в теле цикла может выполняться одна из двух серий команд, причем в конце каждой серии значение переменной k меняется, либо увеличиваясь, либо уменьшаясь на 1. Значение k увеличивается, когда алгоритм идет по второй ветви, т. е. достигается выполнение условия (19.4) для всех $j < k$ (отдельно, до цикла достигается это условие для $j = k-1$, в цикле — для $j < k-1$). Эти операции никак не влияют на μ_{ij}, если $i > k$, в частности, при $i = k+1$. На следующем шаге значение k увеличивается на 1, и неравенства (20.21) следуют из (20.20), которые выполняются на предыдущем этапе.

Значение k уменьшается на 1, если в теле цикла выполняется перестановка векторов, при этом после ее выполнения новые значения коэффициентов μ_{kj} совпадают со старыми значениями (с учетом замены k на $k-1$). Остается только проследить, как изменилось значение коэффициентов μ_{kj}, когда до перестановки векторов мы добивались выполнения условия (19.4) для $\mu_{k\,k-1}$. При этом к k-ой строке матрицы μ прибавлялась $(k-1)$-я строка, умноженная на r, где $|r| < 2|\mu_{k\,k-1}|$. Учитывая, что $|\mu_{k-1\,j}| < 1/2$, получаем

$$|\mu_{kj} - r\mu_{k-1\,j}| \leqslant |\mu_{kj}| + |\mu_{k\,k-1}| \leqslant$$
$$\text{(по индуктивному предположению)}$$
$$\leqslant 2^{n-k+1}(nB^{n-1})^{1/2}. \quad (20.23)$$

Поскольку новое значение k на 1 меньше старого, получаем требуемую формулу, доказательство неравенств (20.17)–(20.21) закончено.

Для завершения доказательства предложения 20.4 нам осталось только оценить значения, получающиеся на промежуточных этапах алгоритма. Заметим, что при выполнении алгоритма **A**35 значения коэффициентов μ не более, чем удваиваются. Поскольку в одном теле основного цикла алгоритм **A**35 выполняется не более, чем $k-1$ раз, то

$$|\mu_{ij}| \leqslant 2^{n-1}(nB^{n-1})^{1/2} \text{ для } j < k-1,$$

откуда, воспользовавшись формулами (19.1), ортогональностью векторов b_i^*, неравенствами $|b_i^*| < B$ получаем неравенства $|b_i|^2 \leqslant n^2(4B)^n$ для $1 \leqslant i \leqslant n$. Остается перемножить границы для знаменателей и для абсолютных величин, прологарифмировать и выделить главную часть, чтобы получить оценки, фигурирующие в предложении 20.4. □

21. Алгоритмы факторизации, основанные на выборе малого вектора в решетке

Теперь рассмотрим второй подход к решению задачи факторизации, предложенный в п. 16.1, а именно, выделяем неприводимый в $\mathbb{Z}[x]$ делитель многочлена $f(x)$ путем построения некоторой решетки и отысканием в ней "малого" вектора.

21.1. Общая схема факторизации. В самых общих чертах алгоритм выделения неприводимого множителя с использованием редуцированного базиса решетки имеет следующий вид:

А37. Алгоритм (выделить-неприводимый-множитель (f, g)).
Дано: $f(x) \in \mathbb{Z}[x]$, $\deg f(x) = m$
Надо: $g(x) \in \mathbb{Z}[x]$, $g(x)$ неприводим в $\mathbb{Z}[x]$

Начало
выбрать полное нормированное поле K, содержащее $\mathbb{Z}$
ограничить степень неприводимого множителя, например,
    $\deg g(x) \leqslant n = m - 1$
определить достаточную точность вычислений
найти с требуемой точностью неприводимый $h(x) \in K[x]$, делящий $f(x)$
    //В результате дальнейших вычислений будет найден
    //неприводимый над $\mathbb{Z}$ многочлен, делящийся на $h(x)$.
сформировать решетку L, ввести на ней норму $\| \ \|$
    //Искомый многочлен $g(x)$ должен принадлежать L
    //и быть в ней вектором минимальной длины
оценить норму искомого $g(x)$,
    //найти B такое, что $\|g(x)\| < B$
если существует в L вектор v, такой, что $\|v\| < B$ **то**
    найти такой вектор v;
    $g(x) := v$
иначе
    $g(x) := f(x)$
конец если
Конец

Некоторые дополнительные комментарии к сформулированному алгоритму.

Наиболее трудный этап в этом алгоритме заключается в нахождении минимального вектора решетки. Для решения этой задачи воспользуемся алгоритмом построения редуцированного базиса ре-

шетки. В общем случае этот алгоритм не позволяет находить минимальный вектор в решетке, но находит вектор, длина которого отличается от длины минимального не более, чем в 2^n раз, где n — размерность решетки. Таким образом, на вводимую норму $\|\ \|$ накладывается более сильное условие: $\|g(x)\|$ должна отличаться от нормы любого взаимно простого с $g(x)$ многочлена $w(x) \in \mathbb{Z}[x]$ не менее, чем в 2^n раз. Константа B должна быть выбрана таким образом, чтобы выполнялись неравенства $\|w(x)\| > B$ и $\|g(x)\| < B$ и алгоритм построения редуцированного базиса решетки давал положительный ответ на вопрос о существовании вектора, длина которого меньше B, в том и только в том случае, когда $\|g(x)\| < B$. Искомая норма $\|\ \|$ зависит от неприводимого над $K[x]$ многочлена $h(x)$, при этом нужно помнить, что многочлен $h(x)$ мы вычисляем с некоторой точностью (не абсолютной), эта точность должна быть достаточно хорошей для того, чтобы сформулированные выше условия на $\|\ \|$ остались справедливыми.

Нахождение с требуемой точностью неприводимого множителя $h(x) \in K[x]$ можно разделить на два этапа: нахождение нулевого приближения и уточнение множителя.

Перепишем алгоритм **А**37 с учетом сделанных замечаний.

АЛГОРИТМ выделить-неприводимый-множитель (многочлены $f(x), g(x)$)

Дано: $f(x) \in \mathbb{Z}[x], \deg f(x) = m$
Надо: $g(x) \in \mathbb{Z}[x], g(x)$ неприводим в $\mathbb{Z}[x]$

Начало
выбрать полное нормированное поле K, содержащее $\mathbb{Z}$
ограничить сверху степень неприводимого множителя
    натуральным числом n, например, $n := m - 1$
определить достаточную точность вычислений
найти нулевое приближение неприводимого $h(x) \in K[x]$
цикл пока не достигнута требуемая точность
    уточнить $h(x) \in K[x]$
конец цикла
сформировать решетку L, ввести на ней норму $\|\ \|$
оценить норму искомого $g(x)$: $\|g(x)\| < B$
редуцировать базис решетки L
если L.базис[0] $< B$ **то**
    $g(x) := L$.базис[0]
конец если
Конец

Рассмотрим основные особенности алгоритма факторизации при использовании архимедовой и p-адической метрики на поле $\mathbb{Q}$. В первом случае в качестве поля K выберем поле комплексных чисел $\mathbb{C}$, во втором — поле p-адических чисел R_p.

21.2. Архимедова метрика. При использовании архимедовой метрики на поле рациональных чисел $\mathbb{Q}$ в качестве полного нормированного расширения поля $\mathbb{Q}$ возьмем поле комплексных чисел K. В комплексном случае неприводимый многочлен $h(x) \in K[x]$ является линейным, мы можем считать его нормированным, т. е. $h(x) = x - \alpha$ для некоторого $\alpha \in \mathbb{C}$. Вычисление α сводится к нахождению комплексного корня многочлена f, что можно сделать с произвольной наперед заданной точностью. Решетка L совпадает в этом случае с $\mathbb{Z}$-модулем всех многочленов с целыми коэффициентами степени $\leqslant n$. Норму многочлена $g \in L$ определим следующим образом: $||g||^2 = \|g\|^2 + c \cdot |g(\alpha)|^2$, где $|\ |$ — норма комплексного числа, $\|\|$ — обычная евклидова норма на пространстве многочленов, а $c = c(f)$ — некоторая константа, зависящая от исходного многочлена f. При вычислениях на ЭВМ α задается в виде $s + t \cdot i$, где s и t — рациональные числа. Пусть S — точность вычисления α, т. е. $|\alpha - (s + t \cdot i)| < 2^{-S}$. Введенная выше норма будет зависеть от точности, с которой вычислено значение корня α. Таким образом, для обоснования алгоритма достаточно показать, что для произвольно заданного многочлена $f(x) \in \mathbb{Z}[x]$ можно явно вычислить положительные числа S, c и B, такие, что норма $\|\ \|$, которая определена значением корня α многочлена f, вычисленного с точностью 2^{-S}, и константой c, удовлетворяет условиям:

$$2^n \cdot ||g||^2 < B \tag{21.1}$$

если g — минимальный многочлен для α над $\mathbb{Z}$, n — ранг решетки L,

$$||p||^2 > B \tag{21.2}$$

для любого многочлена $p \in \mathbb{Z}[x]$, не делящегося на g.

После этого задача сводится к построению редуцированного базиса решетки. Цель данного раздела — показать, что числа B, c и S можно выбрать следующим образом:

$$B = \binom{2n}{n} \|f\|^2 + 1 \tag{21.3}$$

$$c \geqslant 2^{\frac{n^2}{2} + \frac{n}{2} + 4} B^{n + \frac{1}{2}} \|f\|^{n-1} \tag{21.4}$$

$$S \geqslant \log_2(c \cdot 4n \|f\| (2 + \|f\|)^{n-1}) \tag{21.5}$$

Обоснование такого выбора произведено позднее, сейчас же перепишем получившийся алгоритм с учетом выбора значений B, c, S. Отметим, что для использования приведенных выше формул нам удобно поменять местами некоторые команды алгоритма.

А38. Алгоритм (выделить-неприводимый-множитель).
Дано: $f(x) \in \mathbb{Z}[x], \deg f(x) = m$
Надо: $g(x) \in \mathbb{Z}[x], g(x)$ неприводим в $\mathbb{Z}[x]$
Переменные: решетка L
$S \in \mathbb{Z}$, $B, c \in \mathbb{R}$

Начало
L.ранг $:= m$
$n := m - 1$
$B := \binom{2n}{n}\|f\|^2 + 1$;
$c := 2^{\frac{n^2}{2}+\frac{n}{2}+4} B^{n+1/2}\|f\|^{n-1}$
$S := [\log_2(c \cdot 4n\|f\|(2 + \|f\|)^{n-1})] + 1$.
найти комплексный корень $(f(x), \alpha, 2^{-S})$
цикл для i **от** 0 **до** n
    L.базис$[i] := x^i$
конец цикла
редуцировать базис (L)
если $||L$.базис$[0]|| < B$ **то**
    $g(x) := L$.базис$[0]$
иначе
    $g(x) := f(x)$
конец если
Конец

В получившейся версии алгоритма осталось детализировать два предписания:

- найти комплексный корень $(f(x), \alpha, 2^{-S})$;
- редуцировать базис (L).

Нахождение комплексных корней многочлена представляет собой одну из классических задач вычислительной математики, мы не останавливаемся на ней. Алгоритм редуцирования базиса решетки изложен в параграфе 20.

21.3. Обоснование выбора значений B, c, S. Пусть $f \in \mathbb{Z}[x]$ — примитивный многочлен степени n и $\alpha \in \mathbb{C}$ — корень многочлена f. Предположим, что $h \in \mathbb{Z}[x]$ — минимальный многочлен для α. Очевидно, что h — неприводимый множитель многочлена f. Цель этого

параграфа состоит в том, чтобы показать, как вычисление α с достаточной точностью дает нам возможность определить многочлен h.

В данном параграфе символ δ используется для обозначения степени многочлена ($\delta f = \deg f$, $\delta h = \deg h$ и т. д.).

21.1. Предложение. *Пусть $s \in \mathbb{Z}$, $s \geqslant 0$ и предположим, что $\tilde{\alpha}$ удовлетворяет неравенству*

$$|\alpha - \tilde{\alpha}| < 2^{-s} \tag{21.6}$$

Тогда

$$|h(\tilde{\alpha})| < 2^{-s}\delta h\|f\|(2 + \|f\|)^{\delta h - 1} \tag{21.7}$$

Доказательство. Для доказательства этого предложения нам потребуются оценки $|\alpha| \leqslant \|f\|$ (так как α — корень многочлена f) и оценки коэффициентов многочлена h:

$$|h_j| \leqslant \binom{\delta h}{j} \cdot \|f\| \tag{21.8}$$

Собственно доказательство проводится путем разложения h в ряд Тейлора в окрестности точки α и несложных вычислений с использованием приведенных оценок. □

Следующий этап вычислений заключается в приближении с точностью 2^{-s} значений $\tilde{\alpha}^i$ рациональными числами с не слишком большими знаменателями (чтобы не проводить вычислений со слишком большими знаменателями). После этого, выбрав произвольным образом рациональное число c, можем вложить многочлены с целыми коэффициентами степени не выше m (рассматриваем случай $m = \delta f$) в $(m+3)$-мерное пространство над полем $\mathbb{Q}$, тогда образ модуля многочленов образует в этом пространстве решетку размерности $m+1$. Эту решетку обозначаем L. Наша задача заключается в выборе констант s и c таким образом, чтобы кратчайший вектор этой решетки давал нам неприводимый множитель многочлена f. (Квадрат нормы элемента решетки равен сумме квадрата нормы многочлена и приближенного значения квадрата модуля значения многочлена в точке α, умноженного на c^2.)

21.2. Предложение. *Пусть $g \in \mathbb{Z}[x]$ — многочлен степени не выше m, такой, что НОД$(h, g) = 1$. Предположим, что $\delta h \leqslant m$ и что*

$$2^{\frac{m^2}{2}+\frac{m}{2}+4}B^{1/2+m}\|f\|^{m-1} \leqslant c \leqslant \frac{2^s}{4m\|f\|(2+\|f\|)^{m-1}} \tag{21.9}$$

где $B = \binom{2m}{m}\|f\|^2 + 1$. Тогда $||\hat{h}||^2 < B$ и $||\hat{g}||^2 \geqslant 2^m B$.

Доказательство. Первым делом покажем, что $||\hat{h}||^2 < B$. Так как $||\hat{h}||^2 = \|h\|^2 + c^2|\tilde{h}(\tilde{\alpha})|^2$ и $|\tilde{h}(\tilde{\alpha})| \leqslant |h(\tilde{\alpha})| + |h(\tilde{\alpha}) - \tilde{h}(\tilde{\alpha})|$, получаем

$$||\hat{h}||^2 \leqslant \|h\|^2 + c^2(|h(\tilde{\alpha})|^2 + 2|h(\tilde{\alpha})||h(\tilde{\alpha}) - \tilde{h}(\tilde{\alpha})| + +|h(\tilde{\alpha}) - \tilde{h}(\tilde{\alpha})|^2) \tag{21.10}$$

Оценки на слагаемые:

$$|h(\tilde{\alpha})| < \frac{1}{2c} \tag{21.11}$$

$$|h(\tilde{\alpha}) - \tilde{h}(\tilde{\alpha})| < \frac{1}{2c} \tag{21.12}$$

$$\|h\|^2 \leqslant \binom{2\delta h}{\delta h} \|f\|^2 \tag{21.13}$$

оставляются читателю в качестве упражнения.

Доказательство неравенства $||\hat{g}||^2 \geqslant 2^m B$.

Предполагаем, что $\|g\|^2 < 2^m B$ (в противном случае неравенство очевидно). Должны доказать, что $c^2|\tilde{g}(\tilde{\alpha})|^2 \geqslant 2^m B$. Поскольку

$$|g(\tilde{\alpha}) - \tilde{g}(\tilde{\alpha})| \leqslant 2^{-s+\frac{m}{2}} \cdot (m+1) \cdot B^{1/2} \tag{21.14}$$

и $2^{-s}(m+1) \leqslant \frac{1}{c}$, то достаточно доказать неравенство $c|g(\tilde{\alpha})| \geqslant \square 2(2^m B)^{1/2}$.

Найдем $a, b \in \mathbb{Z}[x]$, такие, что $\delta a < \delta g$ и $\delta b < \delta h$, и $ah + bg = r$, где $R \in \mathbb{Z}$ обозначает результант многочленов h и g. Из неравенства Адамара (19.3) следует, что абсолютные значения коэффициентов a и b ограничены величиной $\|h\|^{m-1}\|g\|^m$, а значит и $2^{\frac{m^2}{2}} B^m$. Отсюда, пользуясь тем, что $\|f\| - 1 \geqslant \|f\|/4$, можно получить неравенство

$$\max(|a(\tilde{\alpha})|, |b(\tilde{\alpha})|) < 2^{2+\frac{m^2}{2}} B^m \|f\|^{m-1} \tag{21.15}$$

Отсюда $|a(\tilde{\alpha})h(\tilde{\alpha})| < 1/2$ и $|g(\tilde{\alpha})| \geqslant 1/(2|b(\tilde{\alpha})|)$. $\square$

21.4. Обсуждение алгоритма. Отметим, что введенные выше константы B, c и S можно вычислять не для максимально возможной степени делителя многочлена f, т. е. $m-1$, а для текущей степени n. При этом точность вычислений на промежуточных этапах понизится, соответственно скорость счета увеличится, кроме того с большой вероятностью нам не придется считать до максимального значения n. Так будет, если неприводимый множитель, соответствующий корню α, имеет степень меньше, чем $m-1$. С учетом этого замечания и использованием алгоритма редуцирования базиса решетки вышеприведенный алгоритм принимает вид:

А39. Алгоритм (выделить-неприводимый-множитель).
Дано: $f(x) \in \mathbb{Z}[x],\ \deg f(x) = m$
Надо: $g(x) \in \mathbb{Z}[x],\ g(x)$ неприводим в $\mathbb{Z}[x]$
Переменные: решетка L

Начало
вычислить начальное приближение $\tilde{\alpha}$ корня α и значение S, такое, что в шаре с центром $\tilde{\alpha}$ радиуса S содержится ровно один корень многочлена f
L.базис$[0] := 1$
успех := "нет"
цикл для n **от** 1 **до** $m-1$ **пока** не успех
    L.базис$[n] := x^n$
    минимальный многочлен (L, успех)
конец цикла
если успех **то**
    $g(x) := L$.базис$[0]$
иначе
    $g(x) := f(x)$
конец если
Конец

21.5. *p*-адическая метрика. Переходим к подробному изложению алгоритма факторизации многочленов от одной переменной, основанному на использовании p-адической метрики и построении редуцированного базиса решетки. Предполагаем, что мы нашли неприводимый по модулю некоторого простого числа p множитель многочлена $f(x) \in \mathbb{Z}[x]$, и что мы подняли этот неприводимый множитель до некоторого множителя $h(x)$, делящего многочлен $f(x)$ по модулю некоторой степени числа p. Предположим также, что старший коэффициент многочлена $h(x)$ равен 1 и что многочлен $f(x)$ не делится на $h^2(x)$ по модулю p. Таким образом, предполагаем, что

$$\mathrm{lc}(h) = 1 \tag{21.16}$$

$$(h \mod p^k) \text{ делит } (f \mod p^k) \text{ в } (\mathbb{Z}/p^k\mathbb{Z})[x] \tag{21.17}$$

$$(h \mod p) \text{ неприводим в } F_p[x] \tag{21.18}$$

$$(h \mod p)^2 \text{ не делит } (f \mod p) \text{ в кольце } F_p[x] \tag{21.19}$$

Положим $l = \deg(h)$, тогда $0 < l \leqslant n = \deg(f)$.

Покажем, что множество многочленов $g(x) \in \mathbb{Z}[x]$, которые делятся по модулю p на многочлен $h(x)$, образуют в $\mathbb{Z}[x]$ главный

идеал, порожденный некоторым неприводимым множителем $h_0(x)$ многочлена $f(x)$.

Другими словами, пусть φ_k обозначает естественный гомоморфизм кольца $\mathbb{Z}[x]$ на факторкольцо $(\mathbb{Z}/p^k\mathbb{Z})[x]$, ядро гомоморфизма φ_k совпадает с главным идеалом (p^k) кольца $\mathbb{Z}[x]$, φ_1 обозначим просто φ. Пусть H — главный идеал кольца $\mathbb{Z}[x]$, порожденный многочленом h, удовлетворяющим условиям (21.16)–(21.19). Тогда существует $h_0 \in \mathbb{Z}[x]$, такой, что при любом k в $\mathbb{Z}[x]$ совпадают идеалы $\varphi_k^{-1}(\varphi_k(H)) = \varphi^{-1}(\varphi(H)) = (h_0)$. Многочлен h_0 является неприводимым в $\mathbb{Z}[x]$ и делит $f(x)$.

21.3. Предложение. *Существует неприводимый в кольце $\mathbb{Z}[x]$ множитель $h_0(x)$ многочлена $f(x)$, для которого $(h \mod p)$ делит $(h_0 \mod p)$, и этот множитель определен однозначно с точностью до знака. Кроме того, если $g(x) \in \mathbb{Z}[x]$ и $g(x)$ делит $f(x)$, то следующие условия эквивалентны.*

$$(h \mod p) \text{ делит } (g \mod p) \text{ в кольце } F_p[x] \tag{21.20}$$

$$(h \mod p^k) \text{ делит } (g \mod p^k) \text{ в кольце } (\mathbb{Z}/p^k\mathbb{Z})[x] \tag{21.21}$$

$$h_0 \text{ делит } g \text{ в кольце } \mathbb{Z}[x] \tag{21.22}$$

В частности, $(h \mod p^k)$ делит $(h_0 \mod p^k)$ в кольце $(\mathbb{Z}/p^k\mathbb{Z})[x]$. В теоретико-кольцевых терминах эти условия переписываются следующим образом:

$$\varphi(g) \in (\varphi(h)) \subset F_p[x] \tag{21.20$'$}$$

$$\varphi_k(g) \in (\varphi_k(h)) \subset (\mathbb{Z}/p^k\mathbb{Z})[x] \tag{21.21$'$}$$

$$g \in (h_0) \subset \mathbb{Z}[x] \tag{21.22$'$}$$

В частности,

$$\varphi_k(h_0) \in (\varphi_k(h)) \subset (\mathbb{Z}/p^k\mathbb{Z})[x]$$

Доказательство. Существование многочлена h_0 следует из того, что $\varphi(f)$ делится на $\varphi(h)$. Поскольку многочлен $\varphi(h)$ неприводим, на него делится $\varphi(h_i)$ хотя бы для одного из неприводимых делителей h_i многочлена f, а так как эти делители взаимно просты, то делится в точности один из них.

Поскольку φ является кольцевым гомоморфизмом, и разлагается в композицию гомоморфизмов $\psi_k \cdot \varphi_k$, где ψ_k — естественный гомоморфизмом кольца $\mathbb{Z}/p^k\mathbb{Z}[x] \to F_p[x]$, как из (21.22), так и из (21.21) следует (21.20).

Покажем, что из (21.20) следует (21.21) и (21.22).

Пусть выполнено условие (21.20). Тогда $\varphi(f/g) \notin (\varphi(h))$ в силу (21.19) и однозначности разложения на множители в $F_p[x]$. Значит, $f/g \notin (h_0) \subset \varphi^{-1}(\varphi(h))$. Из однозначности разложения на множители в $\mathbb{Z}[x]$ следует, что $g \in (h_0)$, т. е. выполнено (21.22).

Пусть снова выполнено условие (21.20). Поскольку $F_p[x]$ является областью главных идеалов, из (21.20) следует, что существуют $u(x), v(x) \in F_p[x]$, такие, что $u \cdot \varphi(h) + v \cdot \varphi(f/g) = 1$ в $F_p[x]$. Поскольку φ — эпиморфизм, ядро которого порождено числом p, выписанное соотношение можно поднять до равенства в кольце $\mathbb{Z}[x]$

$$u' \cdot h + v' \cdot f/g = 1 - p \cdot w. \tag{21.23}$$

Обозначим $w' = 1 + pw + p^2w^2 + \cdots + p^{k-1}w^{k-1}$. Применяя φ_k к предыдущему соотношению, умноженному на $g \cdot w'$, получим

$$\varphi_k(g \cdot w' \cdot u') \cdot \varphi_k(h) + \varphi_k(w' \cdot v') \cdot \varphi_k(f) = \varphi_k(g). \tag{21.24}$$

Из этого соотношения и (21.17) следует (21.21). □

Рассмотрим на кольце многочленов $\mathbb{R}[x]$ фильтрацию по степеням многочленов, т. е. для любого неотрицательного целого s векторное пространство, состоящее из многочленов степени не выше s, обозначается $\mathbb{R}_s[x]$. Введенная фильтрация индуцирует фильтрацию на кольце $\mathbb{Z}[x]$: $\mathbb{Z}_s[x] = \mathbb{Z}[x] \bigcap \mathbb{R}_s[x]$. $\mathbb{R}_s[x]$ образует вещественное линейное пространство размерности $s+1$, а $\mathbb{Z}_s[x]$ является в нем решеткой (свободным $\mathbb{Z}$-модулем максимального ранга).

Рассмотрим целое число $m \geqslant l$. Через $L = L(m,k)$ обозначим множество всех многочленов в кольце $\mathbb{Z}[x]$, которые делятся на $h(x)$ по модулю p^k и степень которых не превосходит m, т. е. $L(m,k) = \mathbb{Z}_m[x] \bigcap \varphi_k^{-1}((\varphi_k(h)))$. Другими словами, L состоит из тех многочленов, коэффициенты остатков от деления которых на $h(x)$ в p-адической метрике не превосходят p^{-k-1}, т. е. являются малыми величинами. Легко видеть, что базис решетки L образует следующее множество многочленов

$$\{p^k x^i \mid 0 \leqslant i < l\} \cup \{h \cdot x^j \mid 0 \leqslant j \leqslant m - l\}. \tag{21.25}$$

В качестве базиса всего вещественного пространства многочленов степени не выше m удобно выбрать одночлены x^i, $0 \leqslant i \leqslant m$. Длиной многочлена назовем евклидову длину этого многочлена в выбранном базисе, который мы предполагаем ортонормированным. Отождествляем многочлен с вектором его коэффициентов в выделенном базисе. Матрица коэффициентов базиса (21.25) имеет в этом базисе треугольную форму и легко видеть, что $d(L) = p^{kl}$.

Покажем, что элементы решетки L с малой длиной лежат в главном идеале, порожденном многочленом $h_0(x)$ в $\mathbb{Z}[x]$.

21.4. Предложение. *Предположим, что многочлен $b \in L$ удовлетворяет неравенству*

$$p^{kl} > |f|^m \cdot |b|^n. \tag{21.26}$$

Тогда b делится на $h_0(x)$ в кольце $\mathbb{Z}[x]$, в частности, НОД$(f,b) \neq 1$.

Доказательство. Можно считать, что $b \neq 0$. Положим $g = $ НОД(f,b). Достаточно показать, как следует из предыдущего предложения, что $\varphi(g) \in (\varphi(h))$. Предположим противное. Пользуясь неприводимостью $\varphi(h)$ и эпиморфностью гомоморфизма φ, получаем существование многочленов $u, v, w \in \mathbb{Z}[x]$, таких, что

$$u \cdot h + v \cdot g = 1 - p \cdot w. \tag{21.27}$$

Напомним, что $l = \deg(h)$, $n = \deg(f)$, $m+1$ — размерность решетки L. Положим $m' = \deg(b)$ и $e = \deg(g)$.

Очевидно, что $0 \leqslant e \leqslant m' \leqslant m$. Положим $s = n + m' - e - 1$.

Пусть $M_f = \mathbb{Z}_s[x] \cap (f)$, $M_b = \mathbb{Z}_s[x] \cap (b)$, и $M = M_f + M_b$, т. е. M является $\mathbb{Z}$-модулем, состоящим из всех многочленов вида $u \cdot f + v \cdot b$, где $u \in \mathbb{Z}_{m'-e-1}[x]$, $v \in \mathbb{Z}_{n-e-1}[x]$.

Покажем, что множество элементов

$$\{x^i f \mid 0 \leqslant i < m' - e\} \cup \{x^j b \mid 0 \leqslant j < n - e\} \tag{21.28}$$

образует базис $\mathbb{Z}$-модуля M. Очевидно, что они порождают M, остается только показать, что выписанная система многочленов линейно независима над $\mathbb{Z}$. Предположим, что $u \cdot f + v \cdot b = 0$, где $\deg(u) < m' - e, \deg(v) < n - e$. Разделим это соотношение на g. Получим, $u \cdot (f/g) + v \cdot (b/g) = 0$. Пользуясь взаимной простотой многочленов f/g и b/g и ограничениями на степени u и v, получаем, что $u = v = 0$.

Рассмотрим проекцию

$$\pi \colon \mathbb{R}_s[x] \to \mathbb{R}_s[x]/\mathbb{R}_{e-1}[x]. \tag{21.29}$$

Пусть $M' = \pi(M)$. Покажем, что M' — решетка в $\mathbb{R}_s[x]/\mathbb{R}_{e-1}[x]$. Для этого достаточно показать, что $M \cap \ker \pi = 0$, т. е. $M \cap \mathbb{Z}_{e-1}[x] = 0$. Пусть $w \in M \cap \mathbb{Z}_{e-1}[x]$, тогда $w = u \cdot f + v \cdot b$ по определению M, следовательно, w делится на g $(=$ НОД$(f,b))$. Поскольку $\deg(w) < \deg(g)$, получаем $w = 0$. Учитывая линейную независимость элементов множества (21.28) над $\mathbb{Z}$, получаем, что эти элементы образуют базис решетки M'. Неравенство Адамара (19.3)

утверждает, что $d(M') \leqslant |f|^{m'-e} \cdot |b|^{n-e} \leqslant |f|^m \cdot |b|^n$. Пользуясь предположением теоремы, получаем $d(M') < p^{kl}$.

Для получения желаемого противоречия, покажем, что из (21.27) следует обратное неравенство $d(M') \geqslant p^{kl}$.

Покажем, что для любого элемента $\mu \in M$, если $\deg \mu < e+l$, то $\varphi_k(\mu) = 0$, т. е. $\mu \in p^k\mathbb{Z}$. Домножим соотношение (21.27) на $\mu/g \times$ $\times(1+pw+\cdots+p^{k-1}w^{k-1})$. Получим $u_1 \cdot h + v_1 \cdot \mu \equiv \mu/g \pmod{p^k\mathbb{Z}[x]}$, где u_1, v_1 — некоторые многочлены из кольца $\mathbb{Z}[x]$. Поскольку $\mu \in M$, $\varphi(\mu)$ делится на $\varphi_k(h)$, следовательно, $\varphi_k(\mu/g)$ также делится на $\varphi_k(h)$. Сравнивая степени, получаем, что $\varphi_k(\mu) = 0$.

Для завершения доказательства достаточно теперь показать, что базис $b_e, b_{e+1}, \ldots, b_{n+m'-e-1}$ решетки M' можно выбрать таким образом, что $\deg(b_j) = j$. Это упражнение на приведение невырожденной целочисленной матрицы к треугольному виду оставляется читателю. При таком выборе базиса, старшие коэффициенты первых l многочленов делятся на p^k. Значит $d(M')$, который в полученном базисе равен произведению старших коэффициентов, удовлетворяет неравенству $d(M') \geqslant p^{kl}$, что завершает доказательство теоремы. □

Следующий результат позволяет находить неприводимый делитель многочлена f.

21.5. Предложение. *Пусть f, p, k, n, h, l выбраны так, как предполагалось в начале параграфа, L — решетка, заданная базисом* (21.25). *Предположим, что $b_1, \ldots, b_{m+1}$ — редуцированный базис решетки L и что выполняется неравенство*

$$p^{kl} > 2^{mn/2} \binom{2m}{m}^{n/2} |f|^{m+n}. \tag{21.30}$$

Если h_0 — неприводимый над $\mathbb{Z}$ многочлен, делящийся на h, то $\deg(h_0) \leqslant m$ тогда и только тогда, когда

$$|b_1| < \left(\frac{p^{kl}}{|f|^m}\right)^{1/n}. \tag{21.31}$$

Доказательство. Если условие (21.31) выполнено, то по предложению 21.4 многочлен b_1 делится на h_0. Решетка L выбрана так, что $\deg b \leqslant m$ для любого $b \in L$, следовательно, $\deg(h_0) \leqslant m$.

Предположим теперь, что $\deg(h_0) \leqslant m$. Тогда $h_0 \in L$ по предложению 21.4.

Полагая $x = h_0$ в предложении 19.9, получим $|b_1| \leqslant 2^{m/2} \cdot |h_0|$.

Теперь из задачи 7.6 следует неравенство $b_1 \leqslant 2^{m/2} \cdot \binom{2m}{m}^{1/2} \cdot |f|$. Подставляя сюда (21.30), получим (21.31). □

Теперь можно сформулировать следующий алгоритм нахождения неприводимого в $\mathbb{Z}[x]$ многочлена, делящегося по модулю p на неприводимый по модулю p многочлен $h(x)$.

А40. Алгоритм (неприводимый-множитель (f, h, g, p)).

Дано: $p \in \mathbb{Z}$, $f, h \in \mathbb{Z}[x]$
h — неприводимый по модулю p многочлен, делящий f по модулю p

Надо: g — неприводимый над $\mathbb{Z}$ многочлен, делящий f и делящийся по модулю p на h.

Обозначения: $n == f$.степень
$l == h$.степень

Переменные: целое k
решетка L

Начало
найден множитель := "нет"
цикл для m **от** l **до** $n-1$ **пока** не найден множитель
вычислить k, такое, чтобы выполнялось неравенство (21.30)
пользуясь леммой Гензеля, поднять сравнение $h \cdot u \equiv f \pmod{p}$ до сравнения по модулю p^k
получить базис решетки L по формулам (21.25)
редуцировать базис решетки L
если L.базис[1] удовлетворяет (21.31) **то**
g.степень := m
g.коэффициенты := L.базис[1]
найден множитель := "да"
конец если
конец цикла
Конец

Недостаток этого алгоритма заключается в том, что для каждого значения m нужно применять алгоритм Гензеля, строить новую решетку и редуцировать ее базис. Следующее предложение позволяет применять алгоритм построения редуцированного базиса решетки только один раз для максимального возможного значения $m = n-1$.

21.6. Предложение. *Предположим, что обозначения выбраны так же, как и в предложении 21.5, и что выполнены те же предположения. Предположим кроме того, что существуют индексы j, такие, что*

$$|b_j| < \left(\frac{p^{kl}}{|f|^m}\right)^{1/n}. \tag{21.32}$$

Пусть t — наибольшее значение j, для которого выполнено (21.32). *Тогда*

$$\deg(h_0) = m + 1 - t,$$
$$h_0 = НОД(b_1, \ldots, b_t)$$

и неравенство (21.32) *выполнено для всех j, таких, что $1 \leqslant j \leqslant t$.*

Доказательство. Пусть J обозначает множество индексов $j \in \{1, \ldots, m\}$, для которых выполнено неравенство (21.32), $\#J$ — мощность множества J. Тогда h_0 делит b_j для любого $j \in J$, следовательно, h_0 делит многочлен $h_1 = \text{НОД}(\{b_j \mid j \in J\})$. Положим $s = m - \deg(h_1)$. Поскольку $\deg(b_j) \leqslant m$ для всех $j \in J$, эти многочлены принадлежат $\mathbb{Z}$-модулю $\mathbb{Z}_s[x] \cdot h_1(x)$, ранг которого равен $s + 1 = m + 1 - \deg(h_1)$. В силу линейной независимости векторов b_j получаем

$$\#J \leqslant m + 1 - \deg(h_1). \tag{21.33}$$

Применяя результат задачи 7.6 к многочленам $h_0 x^i$, получаем

$$\|h_0 x^i\| = \|h_0\| \leqslant \binom{2m}{m}^{1/2} \cdot \|f\| \quad \text{для всех} \quad i \geqslant 0.$$

Для $0 \leqslant i \leqslant m - \deg(h_0)$ имеем $h_0 x^i \in L$, так что из предложения 19.9 получаем

$$\|b_j\| \leqslant 2^{m/2} \cdot \binom{2m}{m}^{1/2} \cdot \|f\| \quad \text{для} \quad 1 \leqslant j \leqslant m - \deg(h_0).$$

Из неравенства (21.30) следует, что индексы от 1 до $m + 1 - \deg(h_0)$ принадлежат множеству J. Поскольку h_1 делится на h_0 и выполняется неравенство (21.33), получаем $\{1, \ldots, m+1-\deg(h_0)\} \subset J$, откуда $\deg(h_0) = \deg(h_1) = m + 1 - t$.

Остается установить, что h_1 с точностью до знака совпадает с h_0. Для этого достаточно показать, что многочлен h_1 примитивный, т. е. наибольший общий делитель его коэффициентов равен 1, а примитивность многочлена h_1 легко вытекает из примитивности хотя бы одного b_j, $j \in J$.

Возьмем произвольный индекс $j \in J$ и пусть $d_j = \operatorname{cont}(b_j)$. Тогда многочлен b_j/d_j делится на h_0, следовательно, $b_j/d_j \in L$, так как $h_0 \in L$. Поскольку b_j принадлежит базису решетки L, получаем $d_j = 1$. □

Полученный результат используется в следующем алгоритме.

А41. Алгоритм (неприводимый-множитель (f, h, g, p)).

Дано: $p \in \mathbb{Z}$, $f, h \in \mathbb{Z}[x]$
h — неприводимый по модулю p многочлен, делящий f по модулю p

Надо: g — неприводимый над $\mathbb{Z}$ многочлен, делящий f и делящийся по модулю p на h.

Обозначения: $n == f$.степень
$l == h$.степень

Переменные: цел k, t
решетка L

Начало
найден множитель := "нет"
вычислить k, такое, чтобы выполнялось неравенство (21.30) для $m = n - 1$
пользуясь леммой Гензеля, поднять сравнение $h \cdot u \equiv f \pmod{p}$ до сравнения по модулю p^k
построить базис решетки L по формулам (21.25)
редуцировать базис решетки L
найти максимальное значение t, для которого L.базис$[t]$ удовлетворяет (21.31)
если $t > 0$ **то**
g.степень := $n - t$
g.коэффициенты := НОД (L.базис[1], ..., L.базис[t])
найден множитель := "да"
конец если
Конец

Глава 6

Интегрирование в конечном виде

22. Интегрирование полиномов и рациональных функций

Для решения простейших дифференциальных уравнений вида

$$y' = f(x) \tag{22.1}$$

существует множество методов, которые применимы для функций $f(x)$ из некоторых классов. При этом обычно недостаточно четко задается класс функций, в котором выбираются решения. Решение $g(x)$ уравнения (22.1) определяется с точностью до произвольной константы и называется *неопределенным интегралом* или *первообразной* функции $f(x)$.

Прежде чем переходить к основной части данного раздела, напомним некоторые результаты математического анализа.

В этом разделе символом $\mathcal{A}$ будем обозначать класс функций, к которому принадлежит функция $f(x)$ из правой части уравнения (22.1), а символом $\mathcal{B}$ — класс функций, в котором выбирается решение.

Прежде всего рассмотрим случай, когда $\mathcal{A}$ — кольцо полиномов $K[x]$ от одной переменной над некоторым кольцом K характеристики 0. Предполагается, что мы умеем выполнять арифметические операции в поле K, в частности, K может совпадать с полем $\mathbb{Q}$. В этом случае любое уравнение вида (22.1) имеет решение в этом же классе функций, и алгоритм его нахождения хорошо известен: если $f(x) = \sum\limits_{i=0}^{n} a_i x^i$, то первообразная имеет вид $g(x) = \sum\limits_{i=0}^{n} \frac{a_i}{i+1} x^{i+1} + c$, где c — произвольная константа (*константа интегрирования*).

Следующим по сложности идет случай, когда $\mathcal{A}$ — поле рациональных функций $K(x)$ от одной переменной. Для простоты будем считать, что поле коэффициентов K совпадает с полем рациональных чисел $\mathbb{Q}$. Если класс $\mathcal{B}$ совпадает с $\mathcal{A}$, то решение уравнения (22.1) существует далеко не всегда. Однако можно класс $\mathcal{B}$

несколько расширить, добавив к нему алгебраические числа и операцию логарифмирования полиномов. Полученный класс будем обозначать $\mathcal{B} = \bar{\mathcal{A}}(x, +, -, *, /, \log)$, и тогда любое уравнение вида (22.1), где $f(x) \in \mathbb{Q}(x)$, разрешимо в классе $\mathcal{B}$.

Напомним два метода решения уравнения (22.1) в этом случае.

I метод. Пусть $f(x) = \frac{p(x)}{q(x)}$. Предположим, что мы умеем находить разложение функции $f(x)$ в сумму простейших дробей: $f(x) = p_0 + \sum\limits_{i,j} \frac{c_{ij}}{(x-\alpha_i)^j}$. Проинтегрировать сумму почленно не представляет труда, пользуясь тем, что

$$\int \frac{1}{(x-\alpha)^j}\,dx = \begin{cases} \ln(x-\alpha) + c & \text{при } j = 1 \\ -\frac{1}{(j-1)(x-\alpha)^{j-1}} + c & \text{при } j > 1. \end{cases}$$

Основная сложность этого метода приходится на нахождение полюсов функции $f(x)$, т. е. корней α_i ее знаменателя и разложение функции $f(x)$ в сумму простейших дробей.

II метод. Как и прежде, предполагаем, что $f(x) = \frac{p(x)}{q(x)}$ и что мы нашли все полюса α_i функции $f(x)$ на комплексной плоскости. Разложим в окрестности каждого полюса α_i функцию $f(x)$ в ряд Лорана, точнее, вычислим главную часть разложения, $\sum\limits_{j=n_i}^{1} c_{ij}(x-\alpha_i)^{-j}$, где n_i — порядок полюса в точке α_i. Если $g(x)$ — первообразная функции $f(x)$, то главная часть разложения функции $g(x)$ в точке α_i имеет вид

$$\bar{g}_i(x) = \sum_{j=n_i}^{2} \frac{c_{ij}}{-j+1}(x-\alpha_i)^{-j+1} + c_{i1}\ln(x-\alpha_i).$$

Функция $g(x) - \sum\limits_i \bar{g}_i(x)$ не имеет особенностей в комплексной плоскости и является просто полиномом, степень которого равна $\max(\deg p - \deg q, -1) + 1$. Для нахождения этого полинома можно также проинтегрировать главную часть разложения функции $f(x)$ в точке ∞.

При реализации обоих методов основная трудность состоит в нахождении полюсов α_i функции $f(x)$. При этом приходится работать в алгебраическом расширении $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ поля $\mathbb{Q}$. Однако для записи ответа часто оказывается достаточным меньшее расширение поля $\mathbb{Q}$, чем $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$.

Читателю из курса анализа известно, что интегрирование рациональных функций с действительными коэффициентами осуществ-

ляется без алгебраического расширений поля констант (т. е. без использования комплексных чисел), а только с помощью логарифмов и арктангенсов рациональных функций. В действительности, в этих вычислениях неявно используются комплексные числа, поскольку арктангенсы выражаются через логарифмы с комплексными аргументами.

Вычисления в полях алгебраических чисел легко описываются теоретически, но при реализации на компьютере эти вычисления требуют весьма значительного времени счета и памяти для размещения результатов (особенно промежуточных). И время счета, и объем используемой памяти сильно зависят от степени расширения. В последнее время получены более эффективные алгоритмы интегрирования рациональных функций, позволяющие выполнять все вычисления, не прибегая к алгебраическим расширениям, большим чем то, которое требуется для записи ответа. Не рассматривая этот вопрос в полном объеме, приведем ниже метод Остроградского нахождения рациональной части интеграла рациональной функции.

Предположим, что рациональная функция $f(x)$ представлена в виде суммы полинома $f_0(x)$ и правильной дроби (т. е. отношения двух полиномов, в котором степень числителя меньше степени знаменателя) $f_1(x)$. Мы можем отдельно интегрировать полиномиальную $f_0(x)$ и рациональную $f_1(x)$ части функции $f(x)$. Интеграл от $f_0(x)$ является полиномом, и его вычисление не представляет труда. Интеграл от $f_1(x)$ представляется в виде суммы правильной дроби $g_1(x)$ и логарифмической части $g_2(x)$ интеграла. Логарифмическая часть получается от интегрирования правильных дробей, в знаменателе которых стоят неприводимые полиномы (в первой степени). Сумма таких дробей является правильной дробью, знаменатель $q_2(x)$ которой свободен от квадратов и делит знаменатель исходной функции $f_1(x)$. Алгоритм нахождения $q_2(x)$ описан в параграфе "Разложение на свободные от квадратов множители". Как легко следует из первого метода интегрирования, рациональная часть $g_1(x)$ интеграла функции $f_1(x)$ является правильной дробью, знаменатель $q_1(x)$ которой получается из знаменателя функции $f_1(x)$ делением его на $q_2(x)$. Числитель $r_1(x)$ рациональной части однозначно определяется условиями: $\deg r_1(x) < \deg q_1(x)$ и $f_2(x) - \left(\frac{r_1(x)}{q_1(x)}\right)'$ — правильная рациональная дробь со знаменателем $q_2(x)$. Вычисление полинома $r_1(x)$ осуществляется методом неопределенных коэффициентов.

Два изложенных выше метода интегрирования рациональных функций обобщаются на различные более общие классы функций.

Для формулирования основных результатов нам понадобится ввести некоторые определения. В частности, выше было использовано обозначение $\ln(x-\alpha)$, где α — алгебраическое число. Ниже будет объяснено, что скрывается за этим обозначением.

Хотя проблематика интегрирования в конечном виде возникла из математического и функционального анализа, описание удобнее давать в терминах дифференциальной алгебры.

23. Некоторые сведения из дифференциальной алгебры

В дифференциальной алгебре рассматриваются алгебраические структуры (кольца, поля), в которых наряду с арифметическими операциями имеется операция дифференцирования. При этом дифференцирование определяется не через предельный переход, а с использованием алгебраических свойств. Типичными объектами, с которыми имеет дело дифференциальная алгебра, являются кольца (поля) функций, определенных на подмножестве вещественной прямой или евклидова пространства либо на подмножестве комплексной плоскости. В дифференциальной алгебре мы отвлекаемся от функциональной природы рассматриваемых объектов, не рассматриваем вопросы области определения функций, однозначности и т. д., например, $\log(x-\alpha)$, где α – алгебраическое число, не интерпретируется как функция на действительной оси или в области комплексной плоскости.

Прежде всего напомним формальное определение дифференцирования, дифференциального кольца и дифференциального поля (см. определение 3.2).

23.1. Определение. Отображение δ кольца R в себя называется *дифференцированием*, если оно удовлетворяет условиям

$$\begin{aligned} \delta(a+b) &= \delta a + \delta b \\ \delta(ab) &= \delta a \cdot b + a \cdot \delta b \end{aligned} \tag{23.1}$$

для всех $a, b \in R$.

23.2. Определение. *Обыкновенным дифференциальным кольцом* (*полем*) называется кольцо (поле), на котором действует оператор дифференцирования δ. Если на кольце (поле) задано несколько попарно коммутирующих дифференцирований, то оно называется *частным дифференциальным кольцом* (*полем*) или *кольцом* (*полем*) *с частными производными*.

В дальнейшем мы ограничимся рассмотрением только обыкновенных дифференциальных полей.

23.3. Примеры.

(1) Любое кольцо R можно рассматривать как дифференциальное кольцо с нулевым дифференцированием.

(2) Кольцо бесконечно дифференцируемых на отрезке функций с дифференцированием по координате d/dx является дифференциальным кольцом.

(3) Кольцо многочленов от одной переменной x над кольцом D можно превратить в дифференциальное кольцо, полагая дифференцирование δ тривиальным на D и произвольным образом задав значение $\delta(x)$. Продолжение дифференцирования на все кольцо многочленов определяется однозначно правилами (23.1).

23.4. Определение. Если R — дифференциальное кольцо (поле) с дифференцированием δ, то множество элементов $c \in R$, таких, что $\delta c = 0$ образует подкольцо (подполе) кольца (поля) R, называемое подкольцом (подполем) *констант*. Элемент δa называется *производной* элемента $a \in R$ и часто обозначается a'. Элемент $\delta^n(a)$ называется n-ой производной элемента a и обозначается обычно $a^{(n)}$.

23.5. Определение. Пусть $\mathcal{F}$ — дифференциальное поле с дифференцированием δ. Расширение $\mathcal{G}$ поля $\mathcal{F}$ называется *дифференциальным расширением* дифференциального поля $\mathcal{F}$, если на $\mathcal{G}$ определено дифференцирование δ_1, ограничение которого на $\mathcal{F}$ совпадает с δ. Дифференцирование δ_1 называется *продолжением дифференцирования* δ и обозначается, если это не приводит к двусмысленности, тем же символом δ.

Имеют место следующие теоремы о продолжении дифференцирований.

23.6. Теорема. *Пусть R — целостное кольцо, $\mathcal{F}$ — его поле частных, δ — дифференцирование кольца R. Тогда дифференцирование δ однозначно продолжается до дифференцирования поля $\mathcal{F}$.*

Нетрудно проверить, что, полагая $\delta\left(\frac{a}{b}\right) = \frac{\delta a\, b - a\, \delta b}{b^2}$, мы получаем нужное продолжение и из соотношения $\delta(b \cdot (\frac{a}{b})) = \delta a$ следует единственность этого продолжения.

23.7. Теорема. *Пусть $\mathcal{F}$ — дифференциальное поле с дифференцированием δ, $\mathcal{G}$ — алгебраическое расширение поля $\mathcal{F}$. Тогда дифференцирование δ однозначно продолжается до дифференцирования поля $\mathcal{G}$.*

Действительно, если α удовлетворяет алгебраическому уравнению

$$\sum_{i=0}^{n} a_i \alpha^i = 0,$$

то производная α' удовлетворяет соотношению

$$\alpha' \sum_{i=1}^{n} i a_i \alpha^{i-1} = -\sum_{i=0}^{n} a_i' \alpha^i.$$

В дифференциальной алгебре логарифмы и экспоненты определяются следующим образом.

23.8. Определение. Пусть $\mathcal{G}$ — дифференциальное расширение дифференциального поля $\mathcal{F}$. Элемент $\theta \in \mathcal{G}$ называется *логарифмом* над $\mathcal{F}$, если θ удовлетворяет дифференциальному уравнению $f\theta' = f'$ для некоторого ненулевого элемента $f \in \mathcal{F}$ (обозначается $\theta = \log f$).

23.9. Определение. Пусть $\mathcal{G}$ — дифференциальное расширение дифференциального поля $\mathcal{F}$. Элемент $\theta \in \mathcal{G}$ называется *экспонентой* над $\mathcal{F}$, если θ удовлетворяет дифференциальному уравнению $\theta' = f'\theta$ для некоторого ненулевого элемента $f \in \mathcal{F}$ (обозначается $\theta = \exp f$).

Легко видеть, что определяемые в курсе анализа функции $\ln f$ и e^f удовлетворяют этому определению.

Классической постановкой задачи интегрирования в конечном виде считается случай, когда $\mathcal{A} = \mathcal{B}$ – класс *элементарных функций*. Элементарные функции получаются из рациональных функций посредством арифметических операций и композиции функций (может быть вложенной) алгебраических, логарифмических и экспоненциальных. Более строго элементарные функции определяются следующим образом.

23.10. Определение.

(1) $\mathbb{Q}(x)$ — дифференциальное поле элементарных функций с дифференцированием $\frac{d}{dx}$.
(2) Если D — дифференциальное поле элементарных функций и $\mathcal{F}$ — его алгебраическое расширение, то $\mathcal{F}$ — также дифференциальное поле элементарных функций.
(3) Если $\mathcal{F}$ — дифференциальное расширение дифференциального поля D элементарных функций и $\mathcal{F} = D(\theta)$, где θ — либо логарифм, либо экспонента над D, то $\mathcal{F}$ — дифференциальное поле элементарных функций.

Хотя кажется, что это определение накладывает очень сильные ограничения на функции, называемые элементарными, в действительности элементарными является большинство функций, рассматриваемых в курсе математического анализа, в частности, тригонометрические, обратные тригонометрические, гиперболические, обратные гиперболические, как показывают следующие соотношения.

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}, \qquad \arcsin x = -i\ln(ix + \sqrt{1-x^2}),$$
$$\sinh x = \frac{e^{x} - e^{-x}}{2}, \qquad \operatorname{arsh} x = \ln(x + \sqrt{x^2+1}),$$
$$\cos x = \frac{e^{ix} + e^{-ix}}{2}, \qquad \arccos x = -i\ln(x + i\sqrt{1-x^2}),$$
$$\cosh x = \frac{e^{x} + e^{-x}}{2}, \qquad \operatorname{arch} x = \ln(x + \sqrt{x^2-1}).$$

Теперь мы можем сформулировать задачу интегрирования в конечном виде.

23.11. Задача. *Пусть $\mathcal{F}_n = K(x, \theta_1, \ldots, \theta_n)$ — дифференциальное поле, где K — конструктивное поле констант (т. е. предполагается, что мы можем реализовать вычисления в поле K на компьютере), x — переменная, для которой $x' = 1$, и для любого i от 1 до n элемент θ_i является либо алгебраическим элементом, либо логарифмом, либо экспонентой над полем $\mathcal{F}_{i-1} = K(x, \theta_1, \ldots, \theta_{i-1})$ ($\mathcal{F}_0 = K(x)$). Построить алгоритм, позволяющий для произвольной элементарной функции $f \in \mathcal{F}_n$ найти элементарную функцию $g(x)$, для которой $g'(x) = f$, если только такая функция существует.*

Естественно возникает вопрос о существовании универсального алгоритма, применимого к любой элементарной функции $f(x)$.

Как правило, подынтегральная функция зависит не только от переменной интегрирования, но и от некоторых других переменных, которые мы будем называть параметрами. Мы будем предполагать, что на параметры не наложено никаких соотношений. Вычисление неопределенных интегралов от функции, содержащей параметры, можно понимать двумя способами: нахождение формулы, которая представляет собой неопределенный интеграл данной функции при всех значениях параметров, или нахождение множества значений параметров, при которых функция интегрируема и вычисление интеграла для значений параметров из этого множества. Мы будем рассматривать задачу в первой постановке. Вторая постановка чаще

всего приводит к неразрешимым задачам. Приведем пример, когда простое подынтегральное выражение во второй постановке задачи интегрирования приводит к очень сложным вопросам.

23.12. Пример. Пусть

$$f(x) = \frac{x^k}{1+x} + h(k)\exp(-x^2),$$

где k — действительный параметр, а h — некоторая функция с действительными значениями. Можно показать, что первое слагаемое интегрируемо тогда и только тогда, когда k — рациональное число, а второе — когда $h(k) = 0$. Кроме того между интегралами слагаемых в этой сумме нет взаимодействия, т. е. сумма интегрируема тогда и только тогда, когда интегрируемо каждое слагаемое. Значит интегрируемость нашего выражения зависит от того, является ли рациональное число k корнем уравнения $h(y) = 0$.

Ключевым результатом для обоснования алгоритмов интегрирования в конечном виде является теорема Лиувилля, которую мы приводим без доказательства.

23.13. Теорема. *Пусть $\mathcal{D}$ — некоторое дифференциальное поле, K — его поле констант и $f \in \mathcal{D}$. Пусть $g(x)$ — элементарная над $\mathcal{D}$ функция, удовлетворяющая уравнению $g'(x) = f(x)$. Тогда $g(x)$ можно представить в виде $g(x) = v_0(x) + \sum\limits_i c_i \log v_i(x)$, где c_i — константы из алгебраического замыкания поля K, $v_0(x) \in \mathcal{D}$, $v_i(x) \in \mathcal{D}_0$, где $\mathcal{D}_0$ — некоторое расширение поля $\mathcal{D}$, получающееся присоединением к нему конечного числа констант, алгебраических над $\mathcal{D}$.*

Алгоритмы интегрирования имеют рекурсивный характер, когда от задачи, сформулированной в терминах поля $\mathcal{F}_i$, нужно перейти к одной или нескольким задачам над полем $\mathcal{F}_{i-1}$. При этом существенно различаются методы, используемые для трансцендентных и алгебраических расширений. В данном курсе мы рассмотрим только случай трансцендентных расширений, алгебраические расширения требуют значительно более сложной техники, основанной на фундаментальных результатах алгебраической геометрии.

Прежде чем излагать алгоритм интегрирования трансцендентных функций, рассмотрим несколько примеров.

23.14. Пример. Рассмотрим уравнение $g'(x) = f(x)$, где $f(x) = \log x$. Введем обозначение $\theta = \log x$. Тогда $\theta' = \frac{1}{x}$, т. е. $\theta = \log(x)$

в наших терминах. Легко видеть, что элемент θ трансцендентен не только над $\mathbb{Q}(x)$, но даже над $\mathbb{C}(x)$. Будем рассматривать θ как *независимую переменную* над основным полем функций $\mathbb{Q}(x)$.

Предположим, что интеграл от линейного полинома от переменной θ *должен* являться полиномом второй степени от θ, т. е. должен иметь вид $B_2\theta^2 + B_1\theta + B_0$, где $B_i \in \mathbb{Q}(x)$.

Задача интегрирования приняла вид уравнения

$$\int \theta\, dx = B_2\theta^2 + B_1\theta + B_0.$$

Дифференцируя по x, получим

$$\theta = B_2'\theta^2 + \left(\frac{2}{x}B_2 + B_1'\right)\theta + \left(\frac{1}{x}B_1 + B_0'\right),$$

где $'$ обозначает дифференцирование по x. Приравняв коэффициенты при одинаковых степенях переменной θ в правой и левой частях уравнения, мы получим систему трех линейных обыкновенных неоднородных дифференциальных уравнений:

$$\begin{cases} B_2' = 0 \\ \frac{2}{x}B_2 + B_1' = 1 \\ \frac{1}{x}B_1 + B_0' = 0, \end{cases}$$

которая равносильна системе

$$\begin{cases} B_2' = 0 \\ B_1' = 1 - \frac{2}{x}B_2 \\ B_0 = -\frac{B_1}{x}. \end{cases}$$

Решение каждого из этих уравнений сводится к интегрированию некоторой функции. При этом нужно помнить, что мы ищем неизвестные функции из поля $\mathbb{Q}(x)$. Интегрированием неизвестные функции B_i определяются с точностью до констант (констант интегрирования). Значения этих констант (кроме последней) однозначно определяются следующим уравнением в выписанной системе. Из первого уравнения получаем $B_2 = b_2 = \mathrm{const}$. Подставляя это значение во второе уравнение, после интегрирования получаем ограничения на константу b_2:

$$B_1 = x - 2b_2 \log x + b_1 = x - 2b_2\theta + b_1.$$

Учитывая, что функция B_1 должна принадлежать полю $\mathbb{Q}(x)$, получаем однозначно определенное значение константы b_2: $b_2 = 0$. Таким образом,

$$B_1 = x + b_1.$$

Последнее уравнение принимает вид

$$B_0' = -1 - \frac{b_1}{x}.$$

Интегрируя его, получаем

$$B_0 = -x - b_1\theta + b_0.$$

Откуда $b_1 = 0$ и $B_0 = -x + b_0$.

Таким образом, мы определили функции B_i с точностью до единственной константы b_0, значение которой не может быть определено условием задачи. Непосредственной проверкой убеждаемся, что полученное выражение $0\theta^2 + x\theta + (-x + b_0) = x\log x - x + \text{const}$ является решением исходного уравнения. Заметим, что в данном случае нам не требуется обосновывать выбор формы решения и трансцендентность элемента θ. Если предъявлена функция, удовлетворяющая исходному уравнению, то задача решена, независимо от того, какими соображениями мы пользовались при выборе этой функции.

При доказательстве неинтегрируемости некоторой функции в классе элементарных функций, наоборот, трансцендентность и возможный вид зависимости играет решающую роль.

23.15. Пример. Рассмотрим уравнение

$$g'(x) = e^{-x^2}. \tag{23.2}$$

Введем обозначение $\theta = e^{-x^2}$. Тогда элемент θ трансцендентен над $\mathbb{Q}(x)$ (даже над $\mathbb{C}(x)$) и $\theta' = -2x\theta$. Функция $f(x) = e^{-x^2}$ лежит в дифференциальном поле $\mathbb{Q}(x, \theta)$.

Предположим, что существует элементарная функция $g(x)$, такая, что $g'(x) = f(x)$. По теореме Лиувилля функция $g(x)$ имеет вид $v_0(\theta) + \sum c_i \log v_i(\theta)$, где v_0 — рациональная функция от θ, коэффициенты которой принадлежат полю $\mathbb{Q}(x)$, v_i — полиномы от θ, которые можно считать неприводимыми, коэффициенты которых являются рациональными функциями от x с алгебраическими (комплексными) коэффициентами. Пользуясь свойствами логарифмов, мы можем разбить сумму логарифмов на две части:

$$\sum c_i \log v_i(\theta) = \sum{}' c_i \log v_i + \sum{}'' c_i \log v_i$$

так, что в $\sum'$ полиномы $v_i(\theta)$ являются неприводимыми полиномами от θ со старшим коэффициентом 1, а в $\sum''$ полиномы v_i не зависят от θ.

Пусть $v_0(\theta) = p_0(\theta) + q_0(\theta)$, где p_0 — полином от θ, а $q_0(\theta)$ — правильная рациональная функция от θ. При дифференцировании по x

функции $p_0(\theta)+q_0(\theta)+\sum' c_i\log v_i(\theta)+\sum'' c_i\log v_i$ первое слагаемое дает регулярную часть (полином), второе и третье — правильные дроби от θ, а производная четвертого слагаемого не зависит от θ (является рациональной функцией от x). Поскольку в правой части равенства $g'(x)=\theta$ стоит полином от θ, этот полином (с точностью до свободного члена) должен сокращаться с $(p_0(\theta))'_x$.

Пусть $p_0(\theta)=\sum\limits_{i=0}^{k} A_i\theta^i$, где A_i — функции, зависящие от x. Дифференцируя по x, получаем

$$(p_0(\theta))'_x=\sum_{i=0}^{k} A_i'\theta^i+\sum_{i=0}^{k} iA_i\theta'\theta^{i-1}=\sum_{i=0}^{k} A_i'\theta^i+\sum_{i=0}^{k} A_ii(-2x)\theta^i$$
$$=\sum_{i=0}^{k}(A_i'-2ix\cdot A_i)\theta^i \quad (23.3)$$

Для $i>1$ должны выполняться равенства $A_i'-2ix\cdot A_i=0$, откуда $A_i=\alpha_i e^{-ix^2}$. Мы предполагали, что $A_i\in\mathbb{C}(x)$, а это возможно только при $\alpha_i=0$, поскольку функция e^{-ix^2} трансцендентна над $\mathbb{C}(x)$.

Для $i=1$ получаем уравнение

$$A_1'-2xA_1=1, \quad (23.4)$$

у которого нам нужно найти рациональное решение $A(x)\in\mathbb{C}(x)$. Предположим, что $A(x)=a(x)+b(x)$, где $a(x)$ — полином, а $b(x)$ — правильная рациональная дробь.

Подставляя в (23.4), получаем для полиномиальной части уравнение $a'(x)-2x\cdot a(x)=1$, которое не имеет решений в кольце полиномов $\mathbb{C}[x]$, поскольку при $a(x)\ne 0$ степень полинома в левой части равна $1+\deg a(x)>0=\deg 1$.

Таким образом, уравнение (23.3) не имеет рациональных решений, а уравнение (23.2) — элементарных, т. е. функция вероятности ошибки $\operatorname{Err}(x)=\int_0^x e^{-t^2}dt$ не является элементарной.

23.16. Пример. $g'(x)=\frac{1}{\log x}=f(x)$.

Введем обозначение $\theta=\log x$. Тогда $\theta'=\frac{1}{x}$. Легко видеть, что элемент θ трансцендентен над $\mathbb{C}[x]$.

Предположим, что $g(x)$ — элементарная функция. По теореме Лиувилля она имеет вид $\frac{p(\theta)}{q(\theta)}+\sum c_i\log v_i(\theta)$. Без ограничения общности можно считать, что $v_i(\theta)\in\mathbb{C}(x)[\theta]$ — неприводимые полиномы от θ со старшим коэффициентом 1 или (для одного значения i)

рациональная функция от x, не зависящая от θ. При дифференцировании по x слагаемые вида $\log v_i(\theta)$ дают либо правильную дробь $\left(\frac{\partial v_i}{\partial x} + \frac{\partial v_i}{\partial \theta} \cdot \frac{1}{x}\right) / v_i(\theta)$ от θ со знаменателем $v_i(\theta)$, либо рациональную функцию от x, если v_i не зависит от θ.

Пусть $q_1(\theta)$ — неприводимый делитель полинома $q(\theta)$. После дифференцирования выражения $\frac{p(\theta)}{q(\theta)}$ в знаменателе появится полином $q_1^{k+1}(\theta)$, если $q(\theta)$ делится на $q_1^k(\theta)$, а числитель останется взаимно простым с $q_1(\theta)$. Поскольку знаменатель правой части свободен от квадратов, отсюда вытекает, что $q(\theta) = 1$.

Из того, что разложение правой части исходного уравнения в сумму простейших дробей содержит единственное слагаемое $1/\theta$, и предположения, что различные полиномы $v_i(\theta)$ взаимно просты, следует, что от θ зависит единственное слагаемое $v_1(\theta) = \theta$, т. е. $g(x) = c_1 \log \theta + c_2 \log v_2(x) + p_1(\theta)$, где $p_1(\theta)$ — полином. Следовательно,

$$g'(x) = \frac{c_1 \cdot (\frac{1}{x})}{\theta} + c_2 \cdot \tilde{v}_2(x) + p_1'(\theta) = \frac{1}{\theta}.$$

Поскольку элемент θ трансцендентен над $\mathbb{C}(x)$, должно выполняться равенство $1 = c_1/x$, где c_1 — константа, что невозможно. Следовательно, исходное уравнение не имеет решений в элементарных функциях.

Алгоритм интегрирования трансцендентных функций известен как алгоритм Риша. В его основе лежит метод неопределенных коэффициентов. Искомая функция $g(x)$ выражается в виде функции от θ_n с коэффициентами из поля $\mathcal{F}_{n-1}$, и после дифференцирования $g(x)$ приравниваются коэффициенты при одинаковых степенях в левой и правой частях равенства (22.1). Найденное таким образом решение будет решением исходного уравнения и в том случае, если функции θ_i не являются трансцендентными, но отсутствие решения означает неинтегрируемость только при трансцендентных функциях θ_i. Проверка трансцендентности элементов θ_i осуществляется на основе структурной теоремы.

24. Структурная теорема

Для формулировки структурной теоремы нам понадобится ввести некоторые новые понятия.

24.1. Определение. Элемент θ назовем *регулярным мономом* над дифференциальным полем $\mathcal{F}$, если θ трансцендентен над $\mathcal{F}$ и является либо логарифмом, либо экспонентой над $\mathcal{F}$. Последователь-

ность элементов $\theta_1, \ldots, \theta_n$ называется *последовательностью регулярных мономов*, если каждый ее элемент θ_i является регулярным мономом над $K(x, \theta_1, \ldots, \theta_{i-1})$, $i = 1, \ldots, n$.

В структурной теореме нам нужно различать экспоненты и логарифмы, а именно через E обозначим множество индексов i, таких, что θ_i является экспонентой, а L — множество индексов i, таких, что θ_i является логарифмом. Структурная теорема дает необходимое и достаточное условие трансцендентности очередного элемента последовательности логарифмов и экспонент.

24.2. Теорема. *Пусть K — поле констант, $\theta_1, \ldots, \theta_{k-1}$ $(k \geqslant 1)$ — последовательность регулярных мономов, E — множество индексов $1 \leqslant i \leqslant k-1$, таких, что θ_i является экспонентой $\theta_i = \exp(f_i)$, а L — множество индексов $1 \leqslant i \leqslant k-1$, таких, что θ_i является логарифмом $\theta_i = \log(f_i)$.*

(1) *Пусть $\theta_k = \exp(f_k)$ — экспонента над дифференциальным полем $\mathcal{F}_{k-1} = K(x, \theta_1, \ldots, \theta_{k-1})$, $f_k \in \mathcal{F}_{k-1}$. Если элемент θ_k алгебраичен над $\mathcal{F}_{k-1}$, то f_k представляется в виде линейной комбинации с рациональными коэффициентами*

$$f_k = c + \sum_{i \in E} n_i f_i + \sum_{j \in L} m_j \theta_j, \quad n_i, m_j \in \mathbb{Q},$$

где c — некоторая константа.

(2) *Пусть $\theta_k = \log(f_k)$ — логарифм над дифференциальным полем $\mathcal{F}_{k-1} = K(x, \theta_1, \ldots, \theta_{k-1})$, $f_k \in \mathcal{F}_{k-1}$. Если элемент θ_k алгебраичен над $\mathcal{F}_{k-1}$, то f_k представляется в виде произведения рациональных степеней*

$$f_k = c \prod_{i \in E} \theta_i^{n_i} \times \prod_{j \in L} f_j^{m_j}, \quad n_i, m_j \in \mathbb{Q},$$

где c — некоторая константа.

Заметим, что оба выписанных соотношения выполняются в поле F_{i-1}, которое является полем рациональных функций над K от i независимых переменных. Освобождаясь от знаменателей и приравнивая коэффициенты при одинаковых мономах (во 2-м случае нужно предварительно перейти к логарифмической производной), получим систему линейных уравнений относительно c, n_i и m_j. Если эта система имеет решение в поле констант, такое, что все $n_i, m_j \in \mathbb{Q}$, то θ_i не является регулярным мономом.

Применение структурной теоремы проиллюстрируем следующими примерами.

24.3. Пример. Пусть $K = \mathbb{Q}$ — поле рациональных чисел, и предположим, что $F = \mathbb{Q}(x, \theta_1, \theta_2)$, где $\theta_1 = \log(x)$ и $\theta_2 = \exp(x)$ — регулярные мономы над $\mathbb{Q}(x)$. Используя структурную теорему легко видеть, что ни одна из следующих функций: $\log(\sqrt{x})$, $e^{\log(x)+3x}$, $\log(2x)$, e^{x+1} не является регулярным мономом над F.

24.4. Пример. Рассмотрим выражение

$$\log(x\exp(x)) + \exp(\exp(x) + \log(x)).$$

Будем строить последовательность расширений полей, начинающуюся с поля рациональных чисел $\mathbb{Q}$, и содержащую последовательно вычисляемые части выписанного выражения.

Положим $\theta_1 = \exp(x)$. Элемент θ_1 является регулярным мономом, если не существует константы c такой, что $x \equiv c$. Выполнение этого условия очевидно, значит θ_1 — регулярный моном над $\mathbb{Q}(x) = \mathbb{Q}(\theta_0)$.

Положим $\theta_2 = \log(x\theta_1)$. Если θ_2 не является регулярным мономом, то существует константа c и рациональное число n такие, что $x\theta_1 = c\theta_1^n$. Сравнивая степени x в левой и правой части, получаем, что такое соотношение не выполняется ни при каких c и n, следовательно, θ_2 — регулярный моном над $\mathbb{Q}(\theta_0, \theta_1)$.

Положим $\theta_3 = \log(x)$. Структурная теорема дает нам уравнение $x = c(x\theta_1)^m\theta_1^n$, которое имеет решение $\theta c = 1,\ m = 1,\ n = -1$. Заметим, что существование единственного решения у этого уравнения не означает, что θ_3 единственным образом выражается через θ_1 и θ_2; действительно, $\theta_3 = \theta_2 - x + c'$, где константа c' определена только по модулю $2\pi i$. В этом случае структурная теорема может только подсказать, как переформулировать исходную задачу: исходное выражение целесообразно переписать в виде

$$\log(x\exp(x)) + \exp(\exp(x) + \log(x\exp(x)) - x),$$

в котором константа c' не фигурирует.

Положим $\theta_3 = \exp(\theta_1 + \theta_2 - x)$. Структурная теорема дает нам условие

$$\theta_1 + \theta_2 - x = c + m\theta_2 + nx.$$

Сравнивая коэффициенты при одинаковых мономах в левой и правой частях, получаем систему

$$\begin{cases} c = 0 & \text{(свободный член)} \\ 1 = 0 & \text{(коэффициент при } \theta_1) \\ 1 = m & \text{(коэффициент при } \theta_2) \\ -1 = n & \text{(коэффициент при } x). \end{cases}$$

Очевидно, что выписанная система несовместна. Таким образом θ_3 является регулярным мономом. В поле $\mathbb{Q}(x, \theta_1, \theta_2, \theta_3)$ исходное выражение принимает вид $\theta_2 + \theta_3$.

Заметим, что исходным выражением последовательность элементов θ_i определяется неоднозначно. В частности, можно при рассмотрении того же выражения полагать $\theta_1 = \log(x)$, $\theta_2 = \exp(x)$, $\theta_3 = \exp(\exp(x) + \log(x))$ и $\theta_4 = \log(x \exp(x))$. Можно показать, что в этом случае θ_1, θ_2, θ_3 — регулярные мономы, а θ_4 — нет.

Прежде, чем переходить к подробному изложению алгоритма Риша, рассмотрим еще один

24.5. Пример.

$$\int f\,dx = \int \left[2xe^{x^2} \log x + \frac{e^{x^2}}{x} + \frac{\log x - 2}{(\log^2 x + x)^2} + \frac{\frac{2}{x}\log x + \frac{1}{x} + 1}{\log^2 x + x} \right] dx.$$

Положим $\gamma = e^{x^2}$, $\theta = \log x$. Структурная теорема дает возможность проверить, что γ и θ являются регулярными мономами над $\mathbb{Q}(x)$ и $\mathbb{Q}(x, \gamma)$ соответственно.

В терминах x, γ и θ подынтегральная функция принимает вид:

$$f = 2x\gamma\theta + \frac{\gamma}{x} + \frac{\theta - 2}{(\theta^2 + x)^2} + \frac{\frac{2}{x}\theta + \frac{1}{x} + 1}{\theta^2 + x}.$$

Рассматривая f как рациональную функцию от θ с коэффициентами в поле $\mathbb{Q}(x, \gamma)$ видим, что первые два слагаемых являются полиномами от θ, а последние два — рациональными функциями. Учитывая, что полином $\theta^2 + x$ абсолютно неприводим (т. е. неприводим при любом расширением поля констант), будем искать решение в виде

$$f = \frac{d}{dx} \left[B_2\theta^2 + B_1\theta + B_0 + \frac{B_{11}}{\theta^2 + x} + c_1 \log(\theta^2 + x) \right],$$

где c_1 — константа, $B_2, B_1, B_0 \in \mathbb{Q}(x, \gamma)$, $B_{11} \in \mathbb{Q}(x, \gamma, \theta)$ и линеен по θ. (Это согласуется с теоремой Лиувилля.)

Дифференцируя это соотношение, получим

$$f = B_2'\theta^2 + \left(\frac{2}{x} B_2 + B_1' \right) \theta + \left(\frac{1}{x} B_1 + B_0' \right) + \frac{-B_{11}(\frac{2}{x}\theta + 1)}{(\theta^2 + x)^2} + \frac{B_{11}'}{\theta^2 + x} + \frac{c_1(\frac{2}{x}\theta + 1)}{\theta^2 + x}.$$

Приравниваем коэффициенты при степенях θ, начиная со старшей. Для полиномиальной части получаем следующие соотношения.

Приравнивая коэффициенты при θ^2, получаем $B_2' = 0$, следовательно, $B_2 = \mathrm{const} = b_2$.

Приравнивая коэффициенты при θ, имеем $\frac{2}{x}b_2 + B_1' = 2x\gamma$, следовательно, $B_1' = 2x\gamma - \frac{2}{x}b_2$. Интегрируя это выражение в поле $\mathbb{Q}(x,\gamma)$, получаем $B_1 = -2b_2\theta + \gamma + b_1$, следовательно, $b_2 = 0$ и $B_1 = \gamma + b_1$.

Приравнивая слагаемые, не зависящие от θ, убеждаемся, что $\frac{\gamma+b_1}{x} + B_0' = \frac{\gamma}{x}$. Следовательно, $B_0 = -b_1\theta + b_0$, значит $b_1 = 0$ и $B_0 = \mathrm{const} = b_0$.

Разбор рациональной части начинаем со слагаемых с максимальной степенью знаменателя. Чтобы избавиться от слагаемых со знаменателем $(\theta^2 + x)^2$ нужно решить сравнение

$$-B_{11}\left(\frac{2}{x}\theta + 1\right) \equiv \theta - 2 \pmod{\theta^2 + x}.$$

Для нахождения коэффициента B_{11} нам нужно в поле $\mathbb{Q}(x,\gamma,\theta)$ решить уравнение

$$P(\theta)\left(-\left(\frac{2}{x}\theta + 1\right)\right) + Q(\theta)(\theta^2 + x) = \theta - 2,$$

где P — линейный относительно θ полином, $P(\theta), \mathbb{Q}(\theta) \in \mathbb{Q}(x,\gamma,\theta)$.

Получаем $P(\theta) = -\theta$, $Q(\theta) = -\frac{2}{x}$, следовательно, $B_{11} = -\theta$ и

$$\frac{\theta(\frac{2}{x}\theta + 1)}{(\theta^2 + x)^2} - \frac{\frac{1}{x}}{\theta^2 + x} + \frac{c_1(\frac{2}{x}\theta + 1)}{\theta^2 + x} = \frac{\theta - 2}{(\theta^2 + x)^2} + \frac{\frac{2}{x}\theta + \frac{1}{x} + 1}{\theta^2 + x},$$

откуда вытекает, что $c_1 = 1$.

После подстановки всех неизвестных, окончательный результат принимает вид

$$\int f\,dx = \gamma\theta + \frac{-\theta}{\theta^2+x} + \log(\theta^2+x) = e^{x^2}\log x - \frac{\log x}{\log^2 x + x} + \log(\log^2 x + x).$$

Отметим следующие моменты в рассмотренном примере.

(1) Мы пользовались абсолютной неприводимостью полинома $\theta^2 + x$ (т. е. его неприводимостью при произвольном расширении поля констант). Если знаменатель разлагается на множители (возможно, после расширения поля констант), то рациональная часть принимает более сложный вид.

(2) Возможную форму интеграла мы получали из теоремы Лиувилля.

(3) Вычисление неопределенных коэффициентов в формуле для интеграла сводилось путем дифференцирования к решению некоторого линейного дифференциального уравнения первого порядка над меньшим полем.

(4) Подынтегральная функция в меньшем поле зависела от параметров, и интегрировать ее было возможно только при некоторых ограничениях на параметры (например, $b_2 = 0$).

В разобранных выше примерах мы видели, что применение метода неопределенных коэффициентов приводит к задаче нахождения рациональных решений уравнений более общего вида, чем $y' = f$, а именно,

$$y' + f_1 y = f_2, \tag{24.1}$$

где f_1 и f_2 — известные элементарные функции. Уравнение (24.1) носит название уравнения Риша. В § 27 будет рассматриваться задача нахождения рациональных решений в более общем случае, а сейчас мы изложим алгоритм сведения задачи поиска неопределенных интегралов к нахождению рациональных решений уравнения Риша.

25. Интегрирование логарифмических функций

Пусть $\theta_0 = x$ — независимая переменная над вычислимым полем констант K, $\theta_1, \ldots, \theta_n$ — последовательность регулярных мономов, $\mathcal{F} = \mathcal{F}_n = K(\theta_0, \theta_1, \ldots, \theta_n)$ — соответствующее поле элементарных функций, $f \in \mathcal{F}$. Предположим, что $n > 0$, $\theta = \theta_n$ — логарифм над $\mathcal{F}_{n-1} = K(\theta_0, \theta_1, \ldots, \theta_{n-1})$ и что мы умеем интегрировать функции из поля $\mathcal{F}_{n-1}$. Опишем алгоритм, позволяющий найти неопределенный интеграл функции f, если он является элементарной функцией, или доказать, что в элементарных функциях f неинтегрируема.

Пусть $f(\theta) = p(\theta) + \frac{r(\theta)}{q(\theta)}$ — разложение функции f в сумму полинома и правильной рациональной дроби (как рациональной функции от θ с коэффициентами из поля $\mathcal{F}_{n-1}$). Прежде всего покажем, что можно отдельно рассматривать задачу для полиномиальной части $p(\theta)$ и рациональной части $\frac{r(\theta)}{q(\theta)}$.

25.1. Лемма (о разложении). *Элементарный интеграл функции $f(\theta) = p(\theta) + \frac{r(\theta)}{q(\theta)}$ существует тогда и только тогда, когда существуют элементарные интегралы функций $p(\theta)$ и $\frac{r(\theta)}{q(\theta)}$.*

Доказательство. Согласно теореме Лиувилля, если элементарный интеграл существует, то он имеет вид $g = v_0 + \sum\limits_{i=1}^{m} c_i \log v_i$, т. е. функцию f можно представить в виде

$$f = v_0' + \sum_{i=1}^{m} c_i \frac{v_i'}{v_i}, \tag{25.1}$$

где $v_0 \in \mathcal{F}$, c_i — алгебраические над K константы, v_i $(i=1,\dots,m)$ — элементы из дифференциального поля, получающегося присоединением к $\mathcal{F}$ конечного числа алгебраических над K констант. Дифференцирование $'$ означает дифференцирование по x. Рассматривая (25.1) как тождество в поле $\mathcal{F}_{n-1}(\theta)$, мы без потери общности можем предполагать, что v_i $(1 \leqslant i < k;\ k \geqslant 1)$ — нормированные (со старшим коэффициентом, равным 1) полиномы от θ, а v_i для $k \leqslant i \leqslant m$ — элементы поля $\mathcal{F}_{n-1}$. Разложим v_0 в сумму полинома $\tilde{p}(\theta)$ от θ и правильной рациональной дроби $\frac{\tilde{r}(\theta)}{\tilde{q}(\theta)}$ от θ. Заметим, что $\deg_\theta v_i'(\theta) < \deg_\theta v_i(\theta)$ (используется то, что старший коэффициент равен 1 и $\theta' \in \mathcal{F}_{n-1}$). Учитывая дифференциальное уравнение, которому удовлетворяет θ, после дифференцирования суммы $\tilde{p}(\theta) + \sum\limits_{i=k}^{m} c_i \frac{v_i'}{v_i}$ по x мы получаем полином от θ с коэффициентами в поле $\mathcal{F}_{n-1}$, а продифференцировав по x правильную рациональную функцию (от θ), снова получаем правильную рациональную функцию. Лемма о разложении теперь следует из единственности представления произвольной рациональной функции в виде суммы полинома и правильной рациональной функции. □

25.1. Интегрирование полиномиальной части. Сначала проинтегрируем полиномиальную часть $p(\theta)$.

Пусть $d = \deg_\theta p(\theta)$, $\tilde{d} = \deg_\theta \tilde{p}(\theta)$. Прежде всего покажем, что $\tilde{d} \leqslant d+1$. Для этого проверим, что при дифференцировании по x полинома от θ его степень уменьшается не более, чем на 1. Учитывая, что $\theta' \in \mathcal{F}_{n-1}$, видим, что степень полинома $(B\theta^i)' = B'\theta^i + iB\theta^{i-1}\theta'$ равна i, если $B' \neq 0$, т. е. B не является константой. Для того, чтобы степень полинома $\sum\limits_{i=0}^{k} B_i\theta^i$ при дифференцировании по x понизилась не менее, чем на два, требуется выполнение следующих условий: $B_k = \text{const}$, т. е. $B_k' = 0$ и $kB_k\theta' + B_{k-1}' = 0$, т. е. $\theta' = -\frac{1}{kB_k}B_{k-1}'$. Интегрируя выписанное соотношение, получаем $\theta = -\frac{1}{kB_k}B_{k-1} + c$, где c — константа интегрирования. По предположению, θ является регулярным мономом, т. е. трансцендентен над полем $\mathcal{F}_{n-1}$, которому принадлежит правая часть. Таким образом полученное противоречие показывает, что при дифференцировании по x полинома от θ его степень понижается не более, чем на 1.

Интегрируем полиномиальную часть методом неопределенных коэффициентов. Пусть $p(\theta) = \sum\limits_{i=0}^{d} A_i\theta^i$, $\tilde{p}(\theta) = \sum\limits_{i=0}^{d+1} B_i\theta^i$, $B_i \in \mathcal{F}_{n-1}$

при $i \geqslant 1$, B_0 принадлежит некоторому элементарному расширению поля $\mathcal{F}_{n-1}$. Как показано в предыдущем абзаце, старший коэффициент B_{d+1} является константой, обозначим ее b_{d+1}. Для нахождения остальных коэффициентов B_i, $i = d, d-1, \ldots, 0$, мы получаем, приравнивая коэффициенты при одинаковых степенях θ, систему дифференциальных уравнений

$$A_i = B_i' + (i+1)B_{i+1}\theta'. \tag{25.2}$$

Предположим, что элемент B_{i+1} уже определен с точностью до аддитивной константы b_{i+1} (в частности, можно считать, что $B_{d+1} = 0$). Для определения константы b_{i+1} и элемента B_i рассмотрим подробнее уравнение (25.2). Перепишем это уравнение в виде

$$B_i = \int (A_i - (i+1)(B_{i+1}+b_{i+1})\theta') = -(i+1)b_{i+1}\theta + \int A_i - (i+1)B_{i+1}\theta'.$$

Элемент $A_i - (i+1)B_{i+1}\theta'$ принадлежит полю $\mathcal{F}_{n-1}$, и мы можем по предположению индукции его проинтегрировать. Необходимым условием интегрируемости исходной функции в классе элементарных функций является то, что $\int A_i - (i+1)B_{i+1}\theta' = c_i\theta + \alpha$, где c_i — константа (алгебраическая над K), а $\alpha \in \mathcal{F}_{n-1}$. Если же это условие выполнено, то мы получаем значение константы $b_{i+1} = -\frac{c_i}{(i+1)}$ и значение коэффициента B_i. Интегрируя уравнение (25.2) при $i = 0$, т. е. вычисляя B_0, нужно отказаться от условия $\alpha \in \mathcal{F}_{n-1}$, достаточно, чтобы существовал элементарный интеграл $\int A_0 - B_1\theta'$. Этот интеграл определяется с точностью до аддитивной константы, которая является константой интегрирования и не может быть определена при рассматриваемой постановке задачи.

25.2. Вычисление рациональной и логарифмической части интеграла. Интегрируя правильную рациональную функцию $f(\theta)$ от θ, поступаем так же, как и в случае интегрирования правильных рациональных функций от независимой переменной x.

Прежде всего разлагаем знаменатель подынтегральной функции на неприводимые множители, добавляя, если необходимо, к полю констант K новые алгебраические над K константы. Можно предполагать, что эти константы уже принадлежат полю K. (Отметим, что, в отличие от случая поля рациональных функций, даже после добавления новых констант знаменатель не обязан разлагаться на линейные множители.) Далее выполняем разложение подынтегральной функции в сумму простейших дробей.

Пусть $f(\theta) = \sum\limits_{i=1}^{m} \sum\limits_{j=1}^{k_i} \frac{r_{ij}}{(q_i)^j}$ — разложение в сумму простейших дробей $r_{ij}, q_i \in \mathcal{F}_{n-1}[\theta]$. Без потери общности можно предполагать, что старшие коэффициенты полиномов q_i равны 1 (поскольку K — поле). Из условия, что $f(\theta)$ — правильная рациональная функция, следует неравенство $\deg_\theta r_{ij} < \deg_\theta q_i$ для любых i и j. Как и для рациональных функций от x показывается, что рациональная часть интеграла может содержать в знаменателе только функции q_i в степенях не выше $k_i - 1$. (При дифференцировании простейшей дроби $\frac{\tilde{r}_{ij}}{(q_i)^j}$ получается слагаемое $-\frac{j\tilde{r}_{ij}q_i'}{(q_i)^{j+1}}$, которое может сократиться только со слагаемыми, полученными от дифференцирования других простейших дробей, или со слагаемыми, полученными от разложения в сумму простейших дробей подынтегральной функции.) Из этого замечания следует также, что можно отдельно интегрировать слагаемые, относящиеся к разным полиномам q_i, т. е. вычислять интегралы $\int \sum\limits_{j_1}^{k_i} \frac{r_{ij}}{(q_i)^j}$ для каждого i отдельно. Если $k_i > 1$, то будем искать интеграл в виде $\frac{\tilde{r}_{ik_i-1}}{(q_i)^{k_i-1}} + \tilde{g}$, где $\tilde{g}$ — интеграл от некоторой правильной дроби со знаменателем $(q_i)^{k_i-1}$. Для нахождения полинома $\tilde{r}_{ik_i-1}$ нужно в множестве полиномов, степень которых меньше $\deg_\theta q_i$, найти решение сравнения $-j\tilde{r}_{ik_i-1}q_i' \equiv r_{ik_i} \pmod{q_i}$. Это можно сделать, например, при помощи расширенного алгоритма Евклида, поскольку из неприводимости полинома q_i следует, что он взаимно прост с полиномом q_i', степень которого на 1 меньше степени q_i. (Следует помнить, что дифференцирование осуществляется по независимой переменной x, т. е. дифференцируются не только θ, но и коэффициенты, и $\theta' \neq 1$). После нескольких шагов описанного типа (в которых нет неразрешимых шагов) мы придем к случаю, когда $k_i = 1$. Обработка этого случая заключается в проверке того, что частное от деления числителя на производную по x от знаменателя является константой. Если это не так, то исходная функция неинтегрируема в элементарном виде.

Так же, как и при интегрировании рациональных функций с постоянными коэффициентами, мы можем при нахождении рациональной части интеграла воспользоваться разложением знаменателя на свободные от квадратов множители, определить знаменатель рациональной части интеграла (кратность любого неприводимого множителя снова на 1 меньше его кратности в знаменателе подынтегрального выражения) и искать числитель методом неопределенных

коэффициентов. Для нахождения логарифмической части может потребоваться разложить знаменатель (свободный от квадратов) на неприводимые множители.

26. Интегрирование экспоненциальных функций

Интегрирование экспоненциальных функций проходит во многом параллельно интегрированию логарифмических функций, хотя есть существенные отличия. Мы работаем в следующих предположениях.

Дано конструктивное поле констант K, $\theta_0 = x$ — независимая переменная над этим полем, $\theta_1, \ldots, \theta_n$ — последовательность регулярных мономов, $\mathcal{F} = \mathcal{F}_n = K(\theta_0, \theta_1, \ldots, \theta_n)$ — соответствующее поле элементарных функций, $f \in \mathcal{F}$. Предполагается, что $n > 0$, $\theta = \theta_n$ — экспонента над $\mathcal{F}_{n-1} = K(\theta_0, \theta_1, \ldots, \theta_{n-1})$ и что мы умеем интегрировать функции из поля $\mathcal{F}_{n-1}$.

Описание алгоритма, позволяющего найти неопределенный интеграл функции f, если он является элементарной функцией, начнем снова с леммы о разложении. Ее формулировка будет слегка отличаться от логарифмического случая. Связано это с тем, что в экспоненциальном случае θ^{-i} ведет себя как полином: при дифференцировании ее степень не меняется. Поэтому в разложении функции в сумму простейших дробей слагаемые со знаменателем θ^{-i}, где i — натуральное число, мы будем относить к полиномиальной части и называть соответствующую сумму $\sum_{i=-m}^{k} a_i\theta^i$ обобщенным полиномом.

Пусть $f(\theta) = p(\theta) + \frac{r(\theta)}{q(\theta)}$ — разложение функции f в сумму обобщенного полинома и правильной рациональной функции, знаменатель которой не делится на θ (как рациональной функции от θ с коэффициентами из поля $\mathcal{F}_{n-1}$). Покажем, что можно отдельно рассматривать задачу для полиномиальной части $p(\theta)$ и правильной рациональной части $\frac{r(\theta)}{q(\theta)}$.

26.1. Лемма (о разложении). *Элементарный интеграл функции $f(\theta) = p(\theta) + \frac{r(\theta)}{q(\theta)}$ существует тогда и только тогда, когда существуют элементарные интегралы функций $p(\theta)$ и $\frac{r(\theta)}{q(\theta)}$.*

Доказательство. Согласно теореме Лиувилля, если элементарный интеграл существует, то он имеет вид $g = v_0 + \sum_{i=1}^{m} c_i \log v_i$, т. е. функцию f можно представить в виде

$$f = v_0' + \sum_{i=1}^{m} c_i \frac{v_i'}{v_i}, \tag{26.1}$$

где $v_0 \in \mathcal{F}$, c_i — алгебраические над K константы, v_i — элементы из дифференциального поля, получающегося присоединением к $\mathcal{F}$ конечного числа алгебраических над K констант. Дифференцирование $'$ обозначает дифференцирование по x. Разложим v_0 в сумму обобщенного полинома $\tilde{p}(\theta)$ от θ и правильной рациональной функции $\frac{\tilde{r}(\theta)}{\tilde{q}(\theta)}$ от θ (знаменатель которой не делится на θ). Заметим, что степень (по θ) полинома $v_i'(\theta)$ на этот раз равна степени (по θ) полинома $v_i(\theta)$ (используется то, что $\theta'/\theta \in \mathcal{F}_{n-1}$), поэтому слагаемые вида $\frac{v_i'}{v_i}$, где v_i — полиномы от θ не являются правильными рациональными функциями. Предполагая, что $\gamma = \log\theta$, $\deg_\theta v_i = m_i$ и старшие коэффициенты полиномов v_i равны 1, мы находим, что старший коэффициент полинома $v'i$ равен $n_i\gamma$, т. е. $\frac{v_i' - m_i\gamma' v_i}{v_i}$ — правильная рациональная от θ функция, интегрируемая в элементарном виде тогда и только тогда, когда интегрируема функция $\frac{v_i'}{v_i}$. □

26.1. Интегрирование обобщенной полиномиальной части. Решая уравнение $\left(\sum_i B_i\theta^i\right)' = \sum_i A_i\theta^i$ методом неопределенных коэффициентов, мы приходим к системе дифференциальных уравнений $B_i' + i\gamma' B_i = A_i$, называемых уравнениями Риша, для которых требуется найти решения в поле $\mathcal{F}_{n-1}$. Решение этой задачи будет рассмотрено в § 27.

26.2. Вычисление рациональной и логарифмической части интеграла. В основном, вычисления проходят параллельно случаю, когда θ является логарифмом. Основные отличия обусловлены тем, что при дифференцировании по x полинома от θ со старшим коэффициентом 1 степень полинома не меняется. Поэтому чуть сложнее обосновать взаимную простоту неприводимого полинома $p(\theta)$ и его производной $p'(\theta)$.

26.2. Лемма. *Пусть D — дифференциальное поле, θ — экспонента над D, $\theta' = \eta'\theta$, $\eta \in D$, $p(\theta) \in D[\theta]$ — неприводимый полином со старшим коэффициентом равным 1. Если НОД$(p(\theta), p'(\theta)) \neq 1$, то $p(\theta) = \theta$.*

Доказательство. Пусть $p(\theta) = \sum_{i=0}^{n} a_i\theta^i$, $f_n = 1$. Тогда

$$p'(\theta) = \sum_{i=0}^{n} (a_i' + ia_i(\theta'/\theta))\theta^i = \sum_{i=0}^{n} (a_i' + ia_i\eta')\theta^i.$$

Если НОД$(p(\theta), p'(\theta)) \neq 1$, то НОД$(p(\theta), p'(\theta)) = p(\theta)$ в силу неприводимости $p(\theta)$, т. е. $p'(\theta)$ отличается от $p(\theta)$ множителем из поля D. Значит отношение $\frac{a_i' + i a_i \eta'}{a_i}$ для всех ненулевых коэффициентов не зависит от i. Предположим, что $a_0 \neq 0$. Тогда

$$\frac{a_n' + n a_n \eta'}{a_n} = n\eta' = \frac{a_0' + 0 a_0 \eta'}{a_0} = \frac{a_0'}{a_0},$$

т. е. a_0 удовлетворяет условию $y' = (n\eta')y$. Этому же условию удовлетворяет элемент θ^n. Поскольку любые два решения линейного однородного дифференциального уравнения первого порядка отличаются постоянным множителем, получаем $a_0 = c\theta^n$ для некоторой константы c, что противоречит трансцендентности θ. Доказательство леммы закончено. □

Учитывая лемму и то, что дроби со знаменателями θ^{-k} относятся к обобщенной полиномиальной части, можно почти дословно повторить рассуждения о понижении степени знаменателя при интегрировании простейших дробей, приведенные выше для логарифмического случая. Небольшое отличие состоит в том, что при этих вычислениях мы выходим за рамки работы с правильными дробями, и у нас появляются полиномиальные слагаемые нулевой степени относительно θ. Эти слагаемые мы можем обрабатывать при интегрировании обобщенной полиномиальной части, если интегрирование рациональной части выполнено до интегрирования обобщенного полинома.

В заключение перечислим основные шаги алгоритма интегрирования трансцендентных функций.

(1) Выделить в подынтегральном выражении последовательность подвыражений, порождаемое которыми дифференциальное поле содержит подынтегральное выражение. С помощью структурной теоремы проверить, является ли выписанная последовательность $\theta_1, \ldots, \theta_n$ последовательностью регулярных мономов. При положительном ответе переходить к следующему пункту, в противном случае попытаться найти другую систему образующих. Если после нескольких попыток “хорошую” систему образующих найти не удается, нужно использовать методы интегрирования, позволяющие работать с алгебраическими расширениями (в данной книге не описанные).

(2) Представить подынтегральное выражение в виде рациональной функции переменной θ_n с коэффициентами из дифференциального поля $K(x, \theta_1, \ldots, \theta_{n-1})$. Если θ_n — логарифм, то разложить подынтегральное выражение в суммы полинома от θ_n и правильной рациональной дроби. Если θ_n — экспонента, то разложить подынтегральное выражение в сумму обобщенного полинома и правильной рациональной дроби, знаменатель которой не делится на θ_n.

(3) Найти рациональную часть интеграла. При этом нет необходимости разлагать знаменатель подынтегрального выражения на неприводимые множители, достаточно выполнить только разложение на свободные от квадратов множители.

(4) Применить алгоритм вычисления логарифмической части интеграла. Здесь может потребоваться разложить знаменатель на неприводимые множители. Если логарифмическая часть найдена, то перейти к следующему шагу. Если алгоритм вычисления логарифмической части приводит к несовместным уравнениям, то исходное выражение неинтегрируемо в элементарных функциях, сообщением о чем и следует закончить работу в этом случае.

(5) Интегрировать полиномиальную (обобщенную полиномиальную) часть подынтегрального выражения (без свободного члена). Находится ограничение на степень решения, далее решение находится методом неопределенных коэффициентов. Получается система линейных дифференциальных уравнений первого порядка, для которой нужно найти решения в поле $K(x, \theta_1, \ldots, \theta_{n-1})$. Если какое-либо из получившихся уравнений не имеет решений в дифференциальном поле $K(x, \theta_1, \ldots, \theta_{n-1})$, то исходная функция неинтегрируема в классе элементарных функций.

(6) Интегрировать свободный член, представляющий собой элемент из поля $K(x, \theta_1, \ldots, \theta_{n-1})$. Если $n = 1$, то получается задача интегрирования рациональной функции с постоянными коэффициентами, если $n > 1$, то имеем задачу аналогичную исходной, но число образующих дифференциального поля уменьшилось на 1. Выполняем все те же шаги алгоритма, начиная с шага 2.

27. Решение дифференциального уравнения Риша

27.1. Теорема (Риш). *Пусть $f, g_1, \dots, g_s \in \mathcal{F}$. Тогда можно за конечное число шагов найти элементы $h_1, \dots, h_r \in \mathcal{F}$ и систему линейных уравнений S от $s+r$ неизвестных с коэффициентами в поле K, такие, что уравнение*

$$y' + fy = \sum_{i=1}^{s} c_i g_i, \tag{27.1}$$

выполняется для $y \in \mathcal{F}$ и $c_i \in K$ тогда и только тогда, когда $y = \sum\limits_{i=1}^{r} y_i h_i$, где $y_i \in K$ и константы $c_1, \dots, c_s, y_1, \dots, y_r$ удовлетворяют системе S.

Доказательство. *Основание индукции*: $n = 0$, $\mathcal{F} = K(x)$.

Доказательство теоремы в этом случае проведем в два этапа: сначала избавляемся от знаменателей, затем решаем полиномиальное уравнение.

Этап 1. Пусть $y \in \mathcal{F}$ удовлетворяет уравнению (27.1). Мы можем записать $y = P(x)/Q(x)$, и пусть $q(x)$ — неприводимый в кольце $K[x]$ многочлен со старшим коэффициентом равным 1, делящий $Q(x)$. Предположим, что $q^k(x)$ делит $Q(x)$, а $q^{k+1}(x)$ не делит $Q(x)$. Воспользуемся техникой q-адических расширений и запишем

$$y = \frac{A}{q^k} + \dots, \qquad f = \frac{B}{q^l} + \dots, \qquad \sum c_i g_i = \frac{C}{q^m} + \dots, \tag{27.2}$$

где $A, B, C \in K[x]$, $\deg_x A < \deg_x q$, $\deg_x B < \deg_x q$, $\deg_x C < \deg_x q$, а точками обозначены слагаемые, имеющие в знаменателе q в меньшей степени, чем главный член (эти слагаемые могут также включать степенной ряд). Заметим, что B и l нам известны, т. к. известна функция f, а также нам известно ограничение на m сверху (максимальное значение m' соответствующего показателя для функций g_i). Поскольку c_i могут принимать любые значения, m может не совпадать с m'. Подставляя выражения (27.2) в уравнение (27.1), получим

$$\frac{-kAq'}{q^{k+1}} + \dots + \frac{AB}{q^{k+l}} + \dots = \frac{C}{q^m} + \dots \tag{27.3}$$

Многочлен q является неприводимым, следовательно, выписанные слагаемые не допускают сокращения числителя и знаменателя (q не делит ни Aq', ни AB). Выделяя главный член разложения по $1/q$,

получим или $\begin{cases} k+1 \leqslant m \leqslant m', \\ k+l \leqslant m \leqslant m', \end{cases}$ или $k+1 = k+l > m$. Последняя возможность встречается только в том случае, когда два старших члена в соотношении (27.3) взаимно сократятся, т. е. q делит $-kAq'+AB$, следовательно, q делит $-kq'+B$, а так как $\deg B < \deg q$ и $\deg q' < \deg q$, то $-kq'+B=0$, т. е. $k = B/q'$. Таким образом, число k ограничено сверху числом $\max(m'-1, m'-l, B/q')$, где B/q' появляется только в том случае, если оно является целым числом. Мы получили вычислимую границу для k и можем в уравнении (27.1) перейти к новой неизвестной функции yq^k, знаменатель которой не делится на q.

Заметим, что множитель q может появиться в Q только в том случае, если на q делится знаменатель хотя бы одного из элементов $f, g_1, \ldots, g_s$. Действительно, в противном случае $m' = l = 0$ и если $k > 0$, то слагаемое $-Akq'/q^{k+1}$ не может ни с чем сократиться. Таким образом, у нас имеется только конечное число неприводимых сомножителей q_i, которые могут появляться в знаменателе элемента y, и степени этих сомножителей ограничены вычисляемыми константами k_i. Положим $Y = y \cdot \prod q_i^{k_i}$. Тогда Y является многочленом (для любого решения $y \in \mathcal{F}$ исходного уравнения).

После подстановки $y = Y/\prod q_i^{k_i}$ в уравнение (27.1) и умножения получившегося уравнения на $\prod q_i^{k_i}$, получаем уравнение вида

$$RY' + VY = \sum c_i T_i, \tag{27.4}$$

где $R, V, T_i \in K[x]$ и не зависят от c_i, которые все еще не определены.

Этап 2. Тот же метод применим для ограничения сверху степени неизвестного многочлена Y. Запишем

$$\begin{aligned} Y &= y_0 x^a + \ldots, \\ R &= r_0 x^b + \ldots, \\ V &= v_0 x^c + \ldots, \\ \sum c_i T_i &= t_0 x^d + \ldots, \end{aligned} \tag{27.5}$$

где, как и прежде, мы не знаем точного значения d, а имеем ограничение $d \leqslant d' = \max_{i=1}^{s}(\deg_x T_i)$. Подставляя (27.5) в уравнение (27.4), получим

$$(r_0x^b+\ldots)(ay_0x^{a-1}+\ldots)+(v_0x^c+\ldots)(y_0x^a+\ldots) = t_0x^d+\ldots \tag{27.6}$$

Сравнивая старшие одночлены в правой и левой частях, снова получаем две возможности:

$$\begin{cases} a+b-1 \leqslant d \leqslant d', \\ a+c \leqslant d \leqslant d' \end{cases} \qquad \text{или} \quad a+b-1 = a+c > d. \tag{27.7}$$

Второй случай имеет место только тогда, когда старшие одночлены двух слагаемых в левой части взаимно уничтожаются, т. е.

$$ay_0 r_0 + y_0 v_0 = 0. \tag{27.8}$$

Таким образом получаем границу для a, а именно,

$$a \leqslant \max(d' - b - 1, d' - c, -v_0/r_0), \tag{27.9}$$

где последнее число появляется только в том случае, если оно целое и $c = b - 1$. Раскрывая скобки и приравнивая коэффициенты при одинаковых степенях переменной x в уравнении (27.6), получаем требуемую систему S линейных уравнений.

Шаг индукции: Предположим, теорема доказана для дифференциального поля $\mathcal{D} = K(x, \theta_1, \ldots, \theta_{n-1})$, и докажем ее для дифференциального поля $\mathcal{F} = \mathcal{D}(\theta_n)$, где для упрощения записи мы будем использовать обозначение $\theta = \theta_n$. Случаи, когда θ является логарифмом и экспонентой, будем рассматривать раздельно.

Случай 1. $\theta = \log \eta$.

Доказательство следует тем же путем, что и при $n = 0$.

Этап 1 проходит практически без изменений. Отметим только, что без потери общности мы можем считать многочлен q нормированным, т. е. его старший коэффициент равен 1. В этом случае $\deg q' < \deg q$ (мы рассматриваем операцию дифференцирования в дифференциальном поле $\mathcal{F}$, т. е. $q' = q'_x$, если $\mathcal{F}$ — некоторое поле функций, а степени многочленов рассматриваем относительно переменной θ).

Логика этапа 2 остается такой же, но уравнение (27.6) принимает теперь вид

$$(r_0\theta^b + \ldots)\big(y_0'\theta^a + (y_1' + a\eta'/\eta)\theta^{a-1} + \ldots\big) + (v_0\theta^c + \ldots)(y_0\theta^a + \ldots) = t_0\theta^d + \ldots \tag{27.10}$$

Здесь нужно рассматривать отдельно два подслучая: $y_0' = 0$ и $y_0' \neq 0$. Как и прежде, пусть d' обозначает верхнюю границу для d.

Выделяя старшие одночлены в слагаемых и сравнивая их степени, получаем следующие ограничения:

если $y_0' \neq 0$, то либо $\begin{cases} a+b \leqslant d'+1, \\ a+c \leqslant d'+1, \end{cases}$ либо $a+b = a+c > d'+1$;

если $y_0' = 0$, то либо $\begin{cases} a+b-1 \leqslant d', \\ a+c \leqslant d', \end{cases}$ либо $a+b-1 = a+c > d'$.

Как и в случае $n = 0$, вторая возможность в обоих случаях требует более детального рассмотрения.

Подслучай 1 $y_0' \neq 0$. Неравенство $a+b = a+c > d'+1$ может иметь место только тогда, когда

$$r_0 y_0' + v_0 y_0 = 0 \qquad \text{и}$$
$$r_0(y_1' + a\eta' y_0/\eta) + r_1 y_0' + v_0 y_1 + v_1 y_0 = 0.$$

(Заметим, что в отличие от случая $n = 0$ мы приравниваем нулю два старших коэффициента, поскольку старший коэффициент не зависит от a. Соответственно, этим же объясняется замена неравенства $a+b = a+c > d'$ на $a+b = a+c > d'+1$.)

Второе уравнение можно переписать в виде

$$r_0 y_1' + v_0 y_1 + r_1 y_0' + (a(\eta'/\eta)r_0 + v_1) y_0 = 0.$$

Обозначая $y_1/y_0 = w \in \mathcal{D}$, переписываем это уравнение в виде

$$r_0 y_0 w' + (r_0 y_0' + v_0 y_0) w + r_1 y_0' + (a(\eta'/\eta)r_0 + v_1) y_0 = 0.$$

Подставляя сюда $y_0' = -v_0 y_0 / r_0$ из первого уравнения, получаем

$$w' + r_1 v_0 / r_0^2 + v_1/r_0 + a\left(\frac{\eta'}{\eta}\right) = 0.$$

После интегрирования этого соотношения получаем

$$\int \frac{r_1 v_0 - r_0 v_1}{r_0^2} = w + a \log \eta.$$

Подынтегральное выражение в левой части лежит в дифференциальном поле $\mathcal{D}$, и по предположению индукции мы можем его проинтегрировать. Согласно принципа Лиувилля результат интегрирования (определенный с точностью до аддитивной константы) представляется в виде суммы рациональной функции (из поля $\mathcal{D}$, а точнее его конечного расширения, получаемого присоединением конечного числа алгебраических над K констант) и логарифмической части.

Эта логарифмическая часть определена однозначно, и если ее нельзя представить в виде $a\theta$, где a — целое положительное число, то старший член решения уравнения

$$RY' + VY = \sum c_i T_i, \tag{27.11}$$

где $R, V, T_i \in \mathcal{D}[\theta]$ и не зависят от c_i, не может иметь вид $y_0\theta^a$, где $y_0' \neq 0$ и a удовлетворяет неравенству $a + b = a + c > d' + 1$.

Подслучай 2 $y_0' = 0$. Неравенство $a + b - 1 = a + c > d'$ может иметь место только тогда, когда

$$r_0(y_1' + a\eta' y_0/\eta) + v_0 y_1 + v_1 y_0 = 0,$$

что после интегрирования дает

$$\int \frac{v_0}{r_0} = -\frac{y_1}{y_0} - a\log\eta.$$

Это соотношение дает другое возможное значение a. Заметим, что в этом случае мы снова воспользовались предположением индукции для выполнения операции интегрирования. Отметим также, что для каждого конкретного уравнения вида (27.11) нужно рассматривать не более одного интеграла, в зависимости от того, какое условие $b = c$ или $b = c + 1$ имеет место; если ни одно из этих равенств не выполняется, то $a \leqslant \min(d' + 1 - b, d' + 1 - c)$.

Окончание доказательства этапа 2 ничем не отличается от случая $n = 0$.

Случай 2. $\theta = \exp(\eta)$, т. е. $\theta' = \eta'\theta$.

В этом случае при дифференцировании степень многочлена от θ не понижается, поэтому доказательство этапа 1, проведенное выше, дословно не проходит (там существенно используется, что $\deg(q') < \deg(q)$). В данном случае нужно вместо q' рассматривать остаток от деления q' на q, т. е. такой многочлен q_1, что $q_1 \equiv q' \pmod q$ и $\deg(q_1) < \deg(q)$. Случай $q_1 = 0$ соответствует тому, что $q' = \beta q$, где $\beta \in \mathcal{D}$. Следовательно, β равняется отношению старших коэффициентов многочленов q' и q. Поскольку мы предполагаем, что старший коэффициент многочлена q равен 1, β равно старшему коэффициенту многочлена q', который равен $k\eta'$, где k степень многочлена q (и q'). Решение дифференциального уравнения $q' = k\eta' q$ определено с точностью до мультипликативной константы и имеет вид $q = c \cdot \exp(k\eta) = c\theta^k$. Из условия нормированности следует, что $c = 1$, а из неприводимости q следует, что $k = 1$.

Для неприводимых многочленов q отличных от θ этап 1 проходит с заменой q' на q_1, поскольку единственное место, где мы

по-существу пользовались тем, что q' — ненулевой многочлен, степень которого меньше степени q, это уравнение (27.3), главный член первого слагамого в котором теперь принимает вид $\frac{-kAq_1}{q^{k+1}}$.

Таким образом, на этапе 2 нам нужно рассматривать обобщенные многочлены, т. е. выражения вида $\sum\limits_{-m\leqslant i\leqslant k} A_i\theta^i$ и ограничивать их степени сверху и снизу. Вычисления для верхней и нижней оценок абсолютно аналогичны. Заметим, что дифференцируя одночлен $A_i\theta^i$, мы получаем одночлен той же степени (i), при этом нулевой результат может получиться только при $i = 0$, поскольку $(A_i\theta^i)' = (A_i' + A_i i\eta')\theta^i$ и решение дифференциального уравнения $A_i' + A_i i\eta' = 0$ имеет вид $A_i = c\cdot\theta^{-i}$, что при $i \neq 0$ не принадлежит полю $\mathcal{D}$.

Детали доказательства оставляются читателю в качестве упражнения.

□

Литература

[1] *Абрамов, С. А., Рыбин, С. И.* Обобщение бинарного алгоритма вычисления наибольшего общего делителя целых чисел // Вопросы математической логики и теории алгоритмов. — Москва: ВЦ АН СССР, 1988. — С. 34–37.

[2] *Бахвалов Н. С. и др.* Практикум по программированию. — Москва: МГУ, 1986.

[3] *Боревич З. И., Шафаревич И. Р.* Теория чисел. — Москва: Наука, 1964.

[4] *Ван дер Варден Б. Л.* Алгебра. — Москва: Наука, 1979.

[5] *Грегори Р., Кришнамурти Е.* Безошибочные вычисления. Методы и приложения. — Москва: Мир, 1988.

[6] *Дэвенпорт Д.* Интегрирование алгебраических функций. — Москва: Мир, 1985.

[7] *Дэвенпорт Д., Сирэ И., Турнье Э.* Компьютерная алгебра. — Москва: Мир, 1991.

[8] *Жарков А. Ю., Блинков Ю. А.* Инволютивные системы алгебраических уравнений // *Программирование*. — 1994. — С. 53–56.

[9] *Кнут Д.* Искусство программирования на ЭВМ. Т. 2, Получисленные алгоритмы. — Москва: Мир, 1977.

[10] Компьютерная алгебра. Символьные и алгебраические вычисления / Под ред. Б. Бухбергер, Д. Коллинз, Р. Лоос. — Москва: Мир, 1986.

[11] *Кондратьева М. В., Панкратьев Е. В., Серов Р. Е.* Вычисления в дифференциальных и разностных модулях // Тр. Междунар. совещ. по анал. вычисл. на ЭВМ и их применению в теор. физ., Дубна, 17-20 сент. 1985. — Дубна: 1985. — С. 208–213.

[12] *Лоос Р.* Обобщенные последовательности полиномиальных остатков // Компьютерная алгебра. Символьные и алгебраические вычисления / Под ред. Б. Бухбергер, Д. Коллинз, Р. Лоос. — Москва: Мир, 1986. — С. 151–171.

[13] *Михалев А. В., Панкратьев Е. В.* Дифференциальный размерностный многочлен системы дифференциальных уравнений // Алгебра. Сб. работ, посвящ. 90-летию со дня рожд. О.Ю. Шмидта. — Москва: МГУ, 1980. — С. 57–67.

[14] *Михалев А. В., Панкратьев Е. В.* Компьютерная алгебра. Вычисления в дифференциальной и разностной алгебре. — Москва: МГУ, 1989.

[15] *Панкратьев Е. В.* Компьютерная алгебра. Факторизация многочленов. — Москва: МГУ, 1988.

[16] *Becker T., Weispfenning V., Kredel H.* Gröbner Bases. A Computational Approach to Commutative Algebra. — New York: Springer-Verlag, 1993. — Vol. 141 of *Graduate Texts in Mathematics*.

[17] *Brown W. S.* On Euclid's algorithm and the computation of polynomial greatest common divisors // *J. ACM*. — 1971. — Vol. 18. — Pp. 478–504.
[18] *Cohn R. M.* Difference Algebra. — New York: Interscience, 1965.
[19] Computation of dimension polynomials / *M. V. Kondrat'eva, A. B. Levin, A. V. Mikhalev, E. V. Pankrat'ev* // *International J. of Algebra and Computation*. — 1992. — Vol. 2. — Pp. 117–137.
[20] Differential and difference dimension polynomials / *M. Kondratieva, A. Levin, A. Mikhalev, E. Pankratiev*. — Kluwer Academic Publisher, 1999. — P. 422.
[21] *Gerdt V. P.* Involutive division technique: Some generalizations and optimizations. — 1998.
[22] *Gerdt V. P., Blinkov Y. A.* Minimal involutive bases. — 1997.
[23] *Kolchin E. R.* Differential Algebra and Algebraic Groups. — New York – London: Academic Press, 1973.
[24] *Lenstra A. K., Lenstra C. W., Lovasz L.* Factoring polynomials with rational coefficients // *Math. Ann.* — 1982. — Vol. 261. — Pp. 515–534.
[25] *Mignotte M.* Some inequalities about univariate polynomials // SYMSAC 1981. — 1981. — Pp. 195–199.
[26] *Möller H. M., Mora F.* New constructive methods in classical ideal theory // *J. Algebra*. — 1986. — Vol. 100. — Pp. 138–178.
[27] *Mora F., Möller H. M.* The computation of the Hilbert function // *Lect. Notes Comput. Sci.* — 1983. — Vol. 162. — Pp. 157–167.
[28] *Pinkert J. R.* An exact method for finding the roots of a complex polynomial // *Trans. Amer. Math. Soc.* — 1976. — Vol. 2. — Pp. 351–363.
[29] *Risch R. H.* The problem of integration in finite terms // *Trans. Amer. Math. Soc.* — 1969. — Vol. 139. — Pp. 167–189.
[30] *Zharkov A. Y., Blinkov Y. A.* Involutive approach to investigating polynomial systems // *Math. Comp. Simul.* — 1996. — Vol. 42. — Pp. 323–332. — Proceedings of "SC 93", International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14–17, 1993).

Предметный указатель

Программа экзамена

(1) Задача представления данных. Представление данных в основных областях: кольце целых чисел, поле рациональных чисел, кольце многочленов, поле рациональных функций.
(2) Факториальные и евклидовы кольца. НОД.
(3) Вычисление НОД целых чисел. Алгоритм Евклида, бинарный алгоритм, расширенный алгоритм Евклида, расширенный бинарный алгоритм.
(4) Операции с вещественными числами в компьютерной алгебре, интервальная арифметика, вычисления в поле алгебраических чисел.
(5) p-адические числа, коды Гензеля.
(6) Многомодульная арифметика, китайская теорема об остатках для целых чисел и многочленов.
(7) Вычисление НОД многочленов с рациональными и целыми коэффициентами. Лемма Гаусса. Алгоритм Барейса. Модулярный метод.
(8) Базисы Гребнера в полиномиальных кольцах. Определение и алгоритмы вычисления.
(9) Многочлены Гильберта. Определение и алгоритмы вычисления.
(10) Задача факторизации многочленов. Алгоритмы Кронекера.
(11) Границы корней и коэффициенты делителей данного многочлена: неравенство Коши; мера многочлена; границы для коэффициентов делителя.
(12) Редуцированные базисы решетки. Определение и алгоритм построения.
(13) Разложение многочленов на свободные от квадратов множители. Выделение линейных сомножителей многочленов.
(14) Метрики на поле рациональных чисел; полные нормированные поля; вложения поля рациональных чисел в полное нормированное поле.
(15) Общая схема факторизации многочленов (с перебором комбинаций неприводимых в кольце $K[x]$ сомножителей).
(16) Алгоритм Берлекэмпа (с обоснованием).
(17) Лемма Гензеля и метод Ньютона.
(18) Теорема Свиннертона-Дайера.
(19) Алгоритм факторизации, основанный на выборе малого вектора в решетке: архимедова метрика; p-адическая метрика.
(20) Интегрирование в конечном виде. Постановка задачи. Интегрирование многочленов и рациональных функций. Элементарные функции. Теорема Лиувилля (формулировка).
(21) Интегрирование трансцендентных функций. Структурная теорема. Алгоритм Риша интегрирования логарифмических и экспоненциальных функций.
(22) Решение дифференциального уравнения Риша.
(23) Основные сведения о системах компьютерной алгебры.