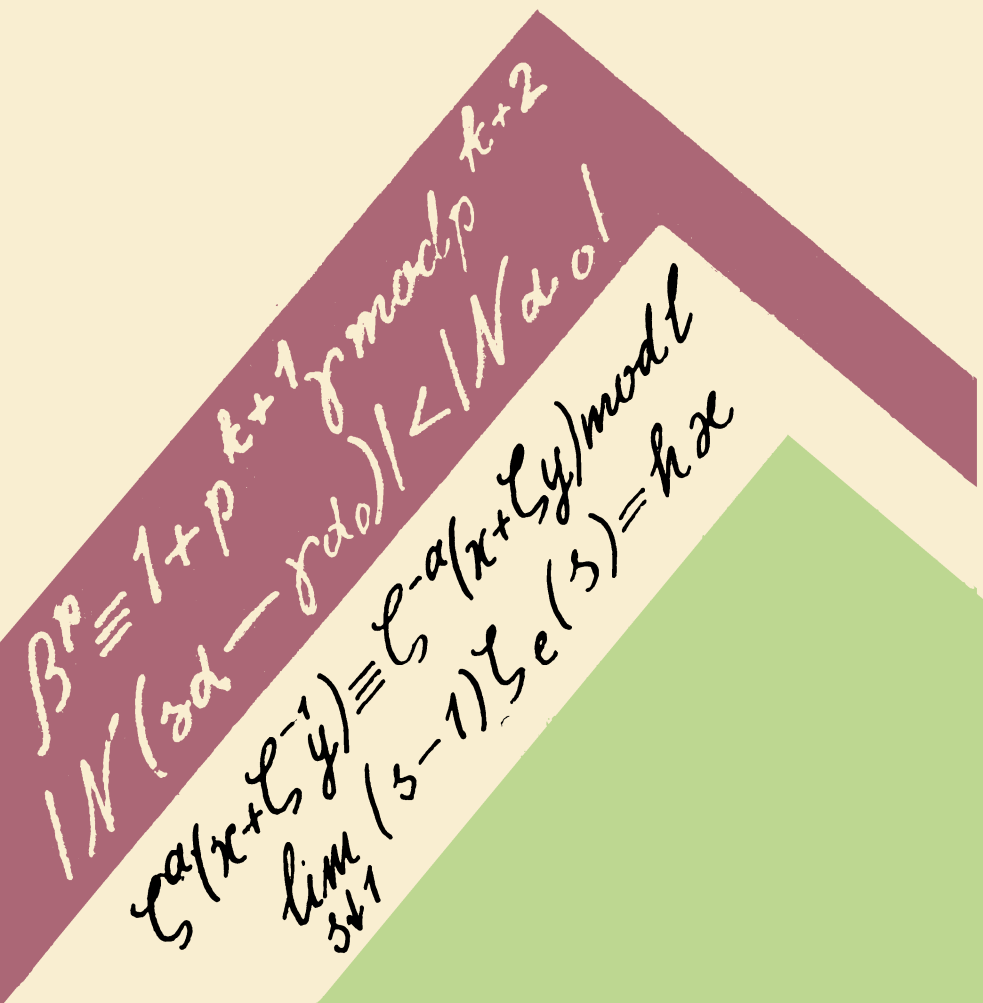


Введение в теорию алгебраических чисел

М.М. Постников



М. М. Постников

Введение в теорию алгебраических чисел



МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ

1982

22.14
П 63
УДК 512

Постников М. М.

П 63 Введение в теорию алгебраических чисел. —
М.: Наука, 1982. — 240 с. — 40 к.

Книга является введением в теорию алгебраических чисел. Основные понятия и идеи этой теории изложены в ней в связи с теоремой Ферма. Читатель должен видеть, что их появление не случайно и диктуется логикой решения конкретной задачи.

Книга предназначена школьникам старших классов (в ее первых главах), студентам, учителям и всем любителям математики. Она может быть интересна и более квалифицированным читателям, которые хотят познакомиться с теорией алгебраических чисел в ее классическом аспекте.

П $\frac{1702030000-040}{053(02)-82}$ 71-82

ББК 22.14
512

П $\frac{1702030000-040}{053(02)-82}$ 71-82

© Издательство «Наука».
Главная редакция
физико-математической
литературы, 1982

СОДЕРЖАНИЕ

Предисловие	6
История теоремы Ферма	11
<p>Ферма и его работы по теории чисел. — Теорема Ферма. — Премия Вольфскеля и «ферматисты». — Замечание Грюнберга. — Эйлер, Ламе, Куммер. — Теоремы Куммера. — Теорема Вандивера. — Первый случай теоремы Ферма. — Жермен, Лежандр, Вендт. — Первый случай теоремы Ферма после Куммера.</p>	
§ 1. Теорема Жермен	21
<p>Предварительные замечания. — Лемма о произведении n-х степеней. — Формулы Абеля. — Сравнения. — Доказательство теоремы Жермен. — Следствия.</p>	
§ 2. Теорема Ферма для показателя 4	30
<p>Случай показателя 2. — Доказательство теоремы Ферма для показателя 4.</p>	
§ 3. Теорема Ферма для показателя 3	34
<p>Лемма Эйлера. — Вывод теоремы Ферма для показателя 3 из леммы Эйлера.</p>	
§ 4. Арифметика кольца D_3	38
<p>Эйлерово «доказательство» леммы. — Обсуждение. — Кольцо D_3 и поле K_3. — Норма. — Целые кольца. — Единицы колец. — Простые элементы. — Разложение на простые множители. — Арифметика в кольцах. — Кольца главных идеалов. — Евклидовы кольца. — Алгоритм деления в кольце D_3. — Доказательство леммы Эйлера.</p>	
<p>П р и л о ж е н и е. Об арифметике многочленов 53</p>	
<p>Неприводимые многочлены. — Неприводимые многочлены и многочлены меньшей степени.</p>	
§ 5. Поле K_l и кольцо D_l	54
<p>Неприводимость многочлена деления круга. — Поле K_l. — Его автоморфизмы. — Существование первообразных корней. — Норма. — Кольцо D_l. — Сравнения в кольце D_l. — Число λ и его свойства.</p>	
§ 6. Единицы кольца D_l	71
<p>Корни из единицы, содержащиеся в кольце D_l. — Вещественные единицы. — Замечание о первообразном корне g. — Формулы</p>	

обращения Фурье для сравнений по модулю l . — Базис кольца D_l по модулю l . — Куммеровы числа. — Вспомогательные тождества. — Специальные единицы. — Условие К. — Лемма Куммера.

§ 7. Первый случай теоремы Ферма 89

Вспомогательное утверждение. — Вывод первого случая теоремы Ферма из Вспомогательного утверждения. — Доказательство Вспомогательного утверждения в случае, когда в кольце D_l выполнена основная теорема арифметики. — Теорема Ламе.

§ 8. Теория дивизоров 95

Свободные коммутативные моноиды. — Кольца, допускающие теорию дивизоров. — Дивизоры в кольцах с однозначным разложением на множители. — Классы дивизоров. — Регулярные простые числа. — Доказательство Вспомогательного утверждения для регулярных простых чисел.

§ 9. Второй случай теоремы Ферма 101

Предварительные замечания. — Доказательство теоремы Ферма для регулярных показателей.

§ 10. Теория идеалов 108

Примеры идеалов. — Идея Дедекнда. — Моноид идеалов. — Кольца, аддитивная группа которых является решеткой. — Кольца, алгебраически вкладываемые в поле \mathbb{C} . — Конечность числа классов идеалов. — Целозамкнутые кольца. — Свойства идеалов. — Идеалы как дивизоры. — Необходимость условия целозамкнутости.

§ 11. Целые алгебраические числа 124

Поле алгебраических чисел и кольцо целых алгебраических чисел. — Поля конечной степени. — След. — Целозамкнутость кольца D_f . — Дивизоры в произвольных полях алгебраических чисел. — Окончательное определение регулярных простых чисел.

§ 12. Куммеровы простые числа 133

Куммеровы числа и произведение $h_1 h_2$. — Предварительная формулировка критерия Куммера. — Числа и многочлены Бернулли. — Окончательная формулировка критерия Куммера. — Примеры. — Вещественные элементы кольца D_f . — Отображение L . — Формула для ΣL . — Отображение X . — Доказательство условия К. — Теорема Куммера.

§ 13. Свойства дивизоров 160

Вводные замечания. — Сравнения по модулю дивизора. — Дополнение дивизора до главного дивизора. — Норма дивизора. — Мультипликативность нормы. — Обобщенная лемма Гаусса. — Нормальные кольца. — Норма дивизора в нормальном кольце. — Свойства простых дивизоров нормальных колец. — Разложение простых чисел в произведение дивизоров кольца D_f .

§ 14. ζ -функция поля K_f и ее вычет при $s = 1$ 176

ζ -функция Римана. — ζ -функция Дедекнда. — Функция $\Xi(s)$. — Пространство RD_f . — Преобразование области Γ_R . — Интеграл $I(s)$. — Сравнение ряда $\Xi(s)$ с интегралом $I(s)$. — Обобщение. — Вычисление вычета ζ -функции Дедекнда поля K_f .

§ 15. Формула Эйлера и L -ряды Дирихле 202

Формула Эйлера.—Проблема сходимости.—Преобразование формулы Эйлера.—Характеры и L -ряды Дирихле.—Функция $L(1, \chi)$ при $\chi \neq \chi_0$.—Формула для чисел $L(1, \chi)$.—Преобразование этой формулы.—Теорема о неравенстве чисел $L(1, \chi)$ нулю.—Окончательные формулы для чисел $L(1, \chi)$.—Доказательство формулы Куммера.

ДОБАВЛЕНИЕ. Теорема Дирихле о простых числах в арифметических прогрессиях 220

Идея доказательства.—Характеры по произвольному модулю.—Число характеров.—Редукция теоремы Дирихле к вопросу о числах $L(1, \chi)$.—Ряды Дирихле и их области сходимости.—Аналитическое продолжение функции Римана.—Функция $P(s)$.—Завершение доказательства теоремы Дирихле.

ПРЕДИСЛОВИЕ

В основе этой книги лежит моя книжка «Теорема Ферма»¹⁾, замысел которой следующим образом был описан в предисловии к ней:

«Теория алгебраических чисел является одним из красивейших созданий математики XIX века. Основные ее идеи легли в основу современной общей алгебры и тем самым оказали стимулирующее влияние на развитие всей математики. В последнее время наблюдается и обратный процесс: конструкции и методы современной абстрактной математики интенсивно вторгаются в прежде запретную для них область теории чисел, быстро меняющей поэтому свое лицо. Это новейшее развитие теории вполне удовлетворительно отражено в литературе, в том числе и учебной: достаточно назвать две недавно переведенные у нас книги Вейля и Ленга. Более классическое направление нашло отражение в книге З. И. Боровича и И. Р. Шафаревича «Теория чисел», в 1972 г. вышедшей вторым изданием. Однако книга Боровича и Шафаревича представляет собой обстоятельный (можно сказать даже энциклопедический) учебник, предназначенный в первую очередь для студентов и аспирантов, специализирующихся по теории алгебраических чисел. Поэтому эта книга для первоначального ознакомления с основными идеями и положениями теории мало пригодна. К тому же она требует от читателя достаточно солидной математической подготовки.

Как ни странно, но на русском языке отсутствуют книги, предназначенные для не очень искушенного

¹⁾ Постников М. М. Теорема Ферма. Введение в теорию алгебраических чисел. — М.: Наука, 1978. В дальнейшем эта книга обозначается ТФ.

читателя, желающего лишь познакомиться с главнейшими идеями теории алгебраических чисел. Заполнить в определенной мере этот пробел имеет целью предлагаемая небольшая книжка. Она посвящена не всей теории алгебраических чисел, а только одному ее разделу — теории делимости целых алгебраических чисел. Однако читатель, изучивший ее, сможет уже увереннее ориентироваться и в более трудных вопросах.

При последовательном чтении книги читатель будет встречаться со все более и более сложным материалом. Однако книга составлена так, что на каждом этапе сообщается некоторый в достаточной степени законченный комплекс сведений. Таким образом, даже читатель со слабой математической подготовкой (например, школьник) узнает достаточно много, чтобы иметь стимул для дальнейшей работы.

Эта «сверхзадача» определила несколько необычный план изложения, устремленный к тому, чтобы, во-первых, на каждом шагу получилось нечто законченное, а во-вторых, было ясно, что нужно делать дальше.

Исторически теория делимости целых алгебраических чисел была создана в связи с теоремой Ферма. Поскольку эта мотивация теории сохраняет всю свою силу и сегодня, мы имеем уникальную возможность объединить концептуальный подход с историческим. Изложение начинается с теоремы Ферма, и теория постепенно разворачивается с единственной, формально, целью — доказать эту теорему. Очень быстро это делается для некоего класса простых показателей, а все дальнейшее преподносится как постепенная расшифровка этого класса и представление его в удобной алгоритмической форме. К сожалению, заключительные этапы этой расшифровки пришлось изложить без доказательства в обзорном порядке.»

Основное отличие настоящей книги от ТФ состоит в том, что она содержит подробное изложение всех этапов упомянутой расшифровки.

Поскольку ТФ была в основном ориентирована на изложение элементов теории делимости целых алгебраических чисел, в ней отсутствовал не относящийся к теории делимости наиболее трудный момент кумеровского доказательства теоремы Ферма — так

называемая лемма Куммера. По существу отсутствовал и использующий числа Бернулли критерий Куммера, только и позволяющий указывать конкретные показатели, для которых справедлива теорема Ферма. Теперь этот пробел заполнен, так что лежащая перед читателем книга содержит полное доказательство теоремы Ферма для регулярных показателей. Это потребовало включения довольно обширного нового материала, что и вызвало изменение названия.

В доказательстве леммы Куммера можно четко отделить арифметические аспекты от аналитических. Именно, можно чисто арифметически и достаточно просто доказать эту лемму для некоторого класса простых чисел, которые в этой книге называются «куммеровыми», после чего остается лишь доказать идентичность куммеровых и регулярных чисел. Только последнее требует аналитических средств.

Настоящая книга фактически подразделяется на четыре части. Первая (§§ 1—4) часть вполне элементарна и доступна, скажем, школьникам. В ней доказываются теорема Жермен и теорема Ферма для показателей 4 и 3. Общетеоретическое значение здесь имеет только обсуждение в § 4 простейших понятий арифметики в произвольных целых кольцах. Эта часть полностью перенесена из ТФ лишь с незначительными, чисто редакционными изменениями.

Вторая часть (§§ 5—9) хотя и несколько труднее, но в основном также вполне доступна школьнику и, во всяком случае, не требует от читателя никаких познаний, существенно выходящих за рамки школьной математики. В ней исследуется кольцо D_l целых чисел поля деления круга на l частей, излагается понятие дивизора, вводится понятие куммеровых и регулярных чисел и на этой основе доказывается теорема Ферма для любого показателя, являющегося одновременно и куммеровым, и регулярным числом. Без доказательства здесь остается только тот фундаментальный факт, что кольцо D_l допускает теорию дивизоров (а также некое условие K , нужное для доказательства леммы Куммера в § 6). По сравнению с ТФ теперь подробнее обсуждено кольцо D_l в § 5 и существенно расширен § 6, посвященный его единицам.

В третью часть (§§ 10—13) из ТФ почти без изменений перешли §§ 10 и 11. Бывшее приложение к § 10

пополнилось новыми материалом, связанным с законами разложения простых чисел в кольце D_l и превратилось в § 13. Практически заново написан § 12. Основная задача этой части — исследовать объем понятий регулярных и куммеровых чисел.

В §§ 10, 11 показывается, что кольцо D_l допускает теорию дивизоров и тем самым что регулярные числа суть в точности простые числа l , не делящие число h классов дивизоров кольца D_l . В новом § 12, посвященном куммеровым числам, устанавливается, что число l тогда и только тогда куммерово, когда оно не делит произведение $h_1 h_2$ некоторого числа h_1 , определенного в этом параграфе, и числа h_2 , введенного и частично изученного в § 6. Здесь же доказывается критерий Куммера регулярности (= куммеровости) простого числа l , основывающийся на числах Бернулли, а также для любого l проверяется условие К, использованное в § 6. Здесь требования к читателю уже более суровые, хотя изложение и построено так, что, приняв несколько фактов на веру, внимательный и трудолюбивый читатель сможет все понять даже при недостаточной подготовке.

В силу результатов третьей части для доказательства совпадения регулярных и куммеровых чисел и, тем самым, для завершения доказательства основной теоремы Куммера остается лишь доказать равенство $h = h_1 h_2$ (формулу Куммера для числа классов). Это делается в целиком новой четвертой части (§§ 14, 15) на основе довольно сложного аналитического аппарата (теории ζ -функций и L -рядов), включающего в себя, в частности, вычисление некоторого многомерного несобственного интеграла. Поэтому здесь у читателя предполагается достаточная аналитическая подготовка.

Основным источником при написании §§ 12, 14 и 15 мне послужила книга Г. Эдвардса «Последняя теорема Ферма»¹⁾.

В Добавлении доказывается знаменитая теорема Дирихле о простых числах в арифметической прогрессии. Хотя эта теорема и не имеет отношения к теореме Ферма, но она немедленно доказывается (по крайней

¹⁾ Эдвардс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел. — М.: Мир, 1980.

мере, в случае, когда разность прогрессии является простым числом) с помощью результатов § 14. Основная трудность, преодолению которой, главным образом, и посвящено это Добавление, состоит в перенесении на случай произвольной разности некоего технического утверждения об L -рядах, доказанного в § 14 для простых чисел. К сожалению, это делается на основе довольно сложной техники теории функций, но другие пути доказательства, по-видимому, еще сложнее.

Таким образом, настоящая книга фактически охватывает все главнейшие разделы классической теории алгебраических чисел — теорию дивизоров и идеалов (которая по существу только и обсуждалась в ТФ), теорию единиц (фундаментальная теорема Дирихле об единицах доказывается на основе конструкций, являющихся непосредственным развитием соображений из § 12) и теорию ζ -функций и L -рядов. Несмотря на это, я льщу себя надеждой, что (за исключением последних параграфов) мне удалось сохранить первоначальный элементарный характер книги.

М. М. Постников

История теоремы Ферма

В XVII веке жил один из величайших математиков Пьер Ферма (1601—1665). Он заложил основы аналитической геометрии (одновременно то же сделал Декарт) и нашел общий метод разыскания максимумов и минимумов (впоследствии развившийся в исчисление бесконечно малых). Однако более всего известны результаты Ферма в области теории чисел.

Свои теоретико-числовые результаты Ферма не публиковал. Они известны из его писем, а также из бумаг, оставшихся после его смерти. Как правило, доказательства Ферма до нас не дошли. Эти доказательства были восстановлены последующими математиками, в основном Эйлером.

Некоторые свои утверждения Ферма сопровождал пометкой, что он не располагает удовлетворительным их доказательством. Впоследствии выяснилось, что часть этих утверждений была ошибочна. Например, Ферма ошибался, утверждая, что все числа вида $2^{2^n} + 1$ простые; уже при $n = 5$, как показал Эйлер, получается составное число.

Однако во всех случаях, когда Ферма определенно утверждал, что он доказал то или иное предложение, впоследствии удавалось это предложение доказать.

Замечательным исключением является так называемая «Большая теорема Ферма» (она же «Великая» или «Последняя»), утверждающая, что не существует отличных от нуля целых чисел x , y и z , для которых

$$x^n + y^n = z^n,$$

где $n > 2$. (Общеизвестно, что при $n = 2$ такие числа существуют, например, 3, 4, 5.)

В бумагах Ферма было найдено доказательство этой теоремы при $n = 4$ (любопытно, что это единственное полное доказательство теоретико-числового результата, сохранившееся от Ферма). Относительно же общего случая любого $n > 2$ Ферма лишь написал (на полях «Арифметики» Диофанта), что он нашел «поистине замечательное доказательство» этого факта, но «поля слишком малы, чтобы его уместить».

Несмотря на усилия многих математиков (в «Истории теории чисел» Диксона прореферировано более трехсот (!) работ на эту тему), это доказательство найдено не было, и можно сомневаться, существовало ли оно вообще.

Более того, кроме показателя 4, нет ни одного показателя n , для которого теорему Ферма удалось бы доказать элементарными средствами.

Этим объясняется, почему в настоящее время все специалисты твердо уверены в невозможности доказать теорему Ферма элементарными методами.

В 1908 г. немецкий любитель математики Вольфскель завещал 100 000 марок тому, кто докажет теорему Ферма. Немедленно сотни и тысячи людей, движимых одним лишь стремлением к наживе, стали бомбардировать научные общества и журналы своими рукописями, якобы содержащими доказательство теоремы Ферма. Только в Гёттингенское математическое общество за первые три года после объявления завещания Вольфскеля пришло более тысячи (!) решений.

Рассказывают, что то ли в Гёттинген, то ли в нашу Академию наук однажды поступила следующая телеграмма: «Решил проблему Ферма двт икс степени эн плюс игрек степени эн не равно зет степени эн тчк доказательство двт переносим игрек степени эн правую часть тчк подробности письмом тчк». Неизвестно, так это или не так, но эта история хорошо отражает как ажиотаж, возникший вокруг теоремы Ферма, так и уровень предлагаемых «доказательств».

В период инфляции после первой мировой войны премия Вольфскеля обесценилась, и ныне «ферматисты» (так называют математики лиц, пытающихся явно с негодными средствами атаковать теорему Ферма) ни на какое финансовое вознаграждение рассчитывать не могут. Поток «ферматистских доказа-

тельств» после этого, естественно, сильно ослаб, но, к сожалению, не прекратился. В научные математические центры постоянно продолжает течь струйка писем, авторы которых мечтают во что бы то ни стало прославиться, хотя и не имеют на это никаких объективных оснований. Часто они с негодованием заявляют, что гонятся вовсе не за личной славой, а хотят прославить свою страну и принести пользу науке. На самом же деле это в лучшем случае — печальное заблуждение.

Значение теоремы Ферма для математики в том, что при попытках ее доказательства были, как мы увидим, выкованы новые мощные средства, приведшие к созданию обширного отдела математики — так называемой «теории алгебраических чисел». Тот факт, что до сих пор теорема Ферма не доказана, по-видимому, означает необходимость в еще более мощных и утонченных методах. Элементарное же доказательство теоремы Ферма (или, более общо, доказательство, не вводящее новых идей и остающееся в рамках уже известных методов), хотя и закрывает проблему, но большого значения для математики иметь заведомо не будет.

Следует со всей решительностью предостеречь читателя от попыток искать элементарное доказательство теоремы Ферма. Можно быть уверенным, что это будет лишь ненужная потеря труда и времени.

Одна из целей настоящей книги — показать, с какими трудными и глубокими вопросами теории чисел соприкасается теорема Ферма, и тем самым обескуражить каждого, кто подумывал взяться за эту теорему и пополнить ряды ферматистов (раз вступившие на эту стезю уже, как правило, недоступны никаким доводам).

Быть может, стоит в связи с этим заметить, что пытаться «вслепую» искать контрпример к теореме Ферма также безнадежно. Еще в 1856 г. Грюберт заметил, что натуральные числа x , y , z , удовлетворяющие соотношению

$$x^n + y^n = z^n$$

(если такие числа существуют), должны удовлетворять неравенствам

$$x > n, \quad y > n, \quad z > n.$$

Действительно, пусть $z = x + a$, где $a \geq 1$. Тогда

$$x^n + y^n = x^n + nx^{n-1}a + \dots + nxa^{n-1} + a^n,$$

и потому $y^n > nx^{n-1}a > nx^{n-1}$. Аналогично доказывается, что $x^n > ny^{n-1}$. Следовательно,

$$(y^n)^n > n^n x^{n(n-1)} > n^n n^{n-1} (y^{n-1})^{n-1},$$

т. е. $y^{2n-1} > n^{2n-1}$ и, значит, $y > n$. По симметрии $x > n$, и потому $z > n$.¹⁾

К настоящему времени теорема Ферма доказана для всех показателей $n < 100\,000$ (см. ниже). Поэтому в опровергающем ее примере мы должны были бы иметь дело с числами, превосходящими $10^{500\,000}$.

Как уже говорилось, *элементарного доказательства теоремы Ферма нет ни для одного показателя $n \neq 4$* . Даже в случае $n = 3$, который был рассмотрен Эйлером в 1768 г., оказались необходимыми соображения, использующие числа вида

$$(1) \quad a + b\sqrt{-3},$$

где a, b — целые числа. Такого рода методы были полностью чужды Ферма, и он их заведомо использовать не мог.

Собственно говоря, доказательство Эйлера было дефектным, поскольку он без всякого обоснования перенес на числа вида (1) рассуждения, эксплуатировавшиеся до него лишь в области целых чисел. Например, он пользовался для чисел (1) простейшими фактами теории делимости, никак это не оправдывая.

Первым, кто построил арифметику чисел (1) и, тем самым, подвел под рассуждения Эйлера надежный фундамент, был, по-видимому, Гаусс.

Доказательство теоремы Ферма для случая $n = 5$ предложили в 1825 г. почти одновременно Лежен Дирихле и Лежандр. Свое доказательство Дирихле опубликовал в 1828 г. Оно было очень сложным. В 1912 г. его упростил Племель.

Для следующего простого показателя $n = 7$ теорема Ферма была доказана лишь в 1839 г. Ламе. Доказательство Ламе было почти сразу же существенно усовершенствовано и упрощено Лебегом.

В 1847 году Ламе объявил, что ему удалось найти доказательство теоремы Ферма для всех простых показателей $n \geq 3$. Метод Ламе представлял собой весь

¹⁾ Знаком ■ мы отмечаем конец доказательства.

ма далекое развитие идей Эйлера и основывался на арифметических свойствах чисел вида

$$(2) \quad a_0 + a_1 \zeta + \dots + a_{n-2} \zeta^{n-2},$$

где a_0, a_1, \dots, a_{n-2} — целые числа, а

$$\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

— первообразный корень n -й степени из 1.

Однако сразу же Лиувилль обнаружил в рассуждениях Ламе серьезный пробел, заключающийся в том, что Ламе без доказательства предполагал, что числа вида (2), подобно обыкновенным целым числам, единственным образом разлагаются в произведение простых (далее неразложимых) чисел. Ламе был вынужден признать свою ошибку.

Пока во Франции происходили эти события, в Германии молодой математик Куммер упорно занимался теоремой Ферма. Сперва он полагал, что ему удалось найти полное доказательство этой теоремы, и в 1843 г. он представил Дирихле соответствующий мемуар. Доказательство также использовало числа вида (2), и, подобно Ламе, Куммер предполагал, что эти числа единственным образом разлагаются на простые множители. Дирихле указал, что этот факт требует доказательства, и Куммер забрал свой манускрипт обратно.

Впрочем, Эдвардс в упомянутой на стр. 9 книге утверждает, что вся эта история является весьма поздней легендой (появившейся только в 1910 г. в лекции Гензеля). По мнению Эдвардса, центр интересов Куммера лежал в так называемых «высших законах взаимности», а теорему Ферма он рассматривал лишь как «любопытную диковинку из теории чисел».

Как бы то ни было, но уже в 1844 г. Куммер знал, что теорема о единственности разложения на простые множители для чисел вида (2) неверна и искать ее доказательство бессмысленно. В этой ситуации он нашел замечательный выход, который прославил его и породил целый ряд разделов современной алгебры. Этот выход состоял в том, что Куммер добавил к числам (2) еще некие новые, несуществующие числа, которые он назвал «идеальными» и для которых свойство

единственности разложения на простые множители восстанавливается.

Например, легко можно показать (сделайте это!), что в области чисел вида

$$(3) \quad a + b\sqrt{-5},$$

где a и b — целые числа, число 21 двумя различными способами разлагается в произведение простых множителей:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Хотя числа вида (3) и не являются числами вида (2) ни при каком n (для чисел (2) аналогичный пример возможен только при $n \geq 23$), но идея Куммера к ним применима. Таким образом, следует добавить к числам (3) некие идеальные числа A, B, C, D и считать, что

$$3 = AB, \quad 7 = CD, \quad 1 + 2\sqrt{-5} = AC, \quad 1 - 2\sqrt{-5} = BD.$$

Ясно, что тогда единственность разложения числа 21 на простые (уже идеальные) множители будет восстановлена.

Конечно, «идеальность» новых чисел привела к своим трудностям, но с ними оказалось легче сладить. Уже в 1847 г. Куммер опубликовал статью, в которой он доказал теорему Ферма для всех простых показателей $n = l$, удовлетворяющих неким условиям (A) и (B). В это время он думал (как доказывает его письмо к Лиувиллю), что эти условия выполнены для всех простых чисел, но вскоре он пришел к заключению, что, по-видимому, имеются исключения (например, число 37). Рассуждения Куммера были упрощены в 1894 г. Гильбертом.

Конечно, этот результат Куммера заставлял желать большего, поскольку он не давал пока ни одного конкретного простого показателя l , для которого справедлива теорема Ферма. Тем не менее, это было замечательное продвижение, и в этой книге мы его подробно обсудим и докажем.

Весьма искусным, тонким и очень трудным анализом арифметики чисел (2) Куммер к 1851 г. добился серьезных усовершенствований своих результатов 1847 года. Ему удалось доказать, что условие (B) вытекает из условия (A) (это — так называемая «лемма Куммера»; см. ниже § 6) и потому излишне. Он существенно упростил условие (A) и придал ему легко проверяемую форму. Это условие в первоначальной формулировке состояло в требовании, чтобы простое чис-

ло l не делило некоторого трудно определяемого числа h . Куммер разложил число h на два множителя:

$$h = h_1 h_2;$$

нашел явные (хотя и довольно сложные) формулы для h_1 и h_2 ; показал, что число h тогда и только тогда делится на l , когда на l делится число h_1 (так называемый *первый множитель*), и, основываясь на этом, весьма изящными теоретико-числовыми рассуждениями доказал, что условие (A) выполнено тогда и только тогда, когда простое число l не делит числителей первых $l - 3$ членов ряда, состоящего из так называемых *чисел Бернулли* (в их несократимом представлении). Такие простые числа Куммер назвал *регулярными*.

Числа Бернулли — это рациональные числа

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = 0, \dots,$$

которые могут быть вполне автоматически вычислены друг за другом по очень простым правилам (см. § 12). Поэтому условие Куммера проверяется для каждого l без особого труда.

В частности, оказывается, что *среди простых чисел $l < 100$ нерегулярны только числа 37, 59 и 67*.

Это было замечательным завершением исследований 1847 г., но, к сожалению, доказательства этих результатов отнюдь не элементарны. Мы все же изложим их здесь, чтобы иметь полную картину.

Куммер всю жизнь думал, что регулярных чисел бесконечно много, и эту уверенность разделяли с ним многие математики. Однако до сих пор этот факт не доказан.

Более того, в 1915 г. Иенсен очень просто доказал, что напротив, *имеется бесконечно много нерегулярных простых чисел*.

После 1851 г. Куммер обратился к исследованию нерегулярных простых чисел и пытался доказать для них теорему Ферма. В очень трудной работе 1858 года он доказал теорему Ферма для некоторого класса нерегулярных простых показателей, включающего показатели 37, 59 и 67. Тем самым теорема Ферма оказалась доказанной для всех простых показателей $l < 100$. Правда, позднее (в первой четверти XX века) Мертенс и Вандивер обнаружили в рассуждениях

Куммера неточности, но они оказались вполне исправимыми.

Специальное, более простое, доказательство теоремы Ферма для показателя $l = 37$ в 1893 г. дал Мирманов.

Около 1850 г. Французская академия наук учредила награду в 3 тыс. франков за доказательство теоремы Ферма. Присуждение несколько раз откладывалось, пока, наконец, в 1857 г. премия не была присуждена Куммеру (который, кстати сказать, даже не был вначале среди претендентов).

После Куммера серьезных сдвигов в доказательстве теоремы Ферма не произошло до 1929 г., когда Вандивер доказал, что *теорема Ферма справедлива для простого показателя l , если*

- 1) *второй множитель h_2 числа h не делится на l ;*
- 2) *числители $l - 3$ чисел Бернулли*

$$B_{2l}, B_{4l}, \dots, B_{2l(l-3)}$$

не делятся на l^3 .

Проверка условия 2) для современных ЭВМ труда не составляет. Что же касается условия 1), то до сих пор неизвестно ни одного простого числа l , для которого оно не выполнено, хотя были проверены все простые числа $l < 100\,000$. Для этих чисел условие 2) теоремы Вандивера тоже оказалось выполненным. Таким образом, *теорема Ферма справедлива для всех простых показателей $l < 100\,000$.*

Уже Эйлеру было известно, что при исследовании уравнения

$$(4) \quad x^l + y^l = z^l, \quad l \text{ простое} \geq 3,$$

необходимо различать случай, когда ни одно из чисел x, y, z не делится на l , от случая, когда хотя бы одно из этих чисел делится на l .

Допуская определенную небрежность речи, принято называть утверждение, что уравнение (4) не может быть удовлетворено не делящимися на l числами, первым случаем теоремы Ферма, а утверждение, что уравнение (2) не может быть удовлетворено числами, одно из которых делится на l , — вторым случаем теоремы Ферма.

Оказывается, что, в отличие от общего случая теоремы Ферма, ее первый случай допускает для многих l элементарное доказательство. Подход к этому доказательству был нащупан еще в начале XIX века известной Софи Жермен (1776—1831), первой женщиной-математиком нового времени. В частности, она доказала, что *для простого числа l справедлив первый случай теоремы Ферма, если число $2l + 1$ также является простым числом.*

Однако надежды, которые возбудила Жермен, не оправдались, и на предложенном ей пути найти полное доказательство хотя бы первого случая теоремы Ферма не удалось.

Жермен не опубликовала своих результатов, а сообщила их в письме известному французскому математику Лежандру. В 1823 г. Лежандр выпустил в свет обширный мемуар по теореме Ферма, в котором он изложил теорему Жермен и вывел из них ряд следствий. В частности, он показал, что *первый случай теоремы Ферма справедлив для простого показателя l , если хотя бы одно из пяти чисел*

$$4l + 1, \quad 8l + 1, \quad 10l + 1, \quad 14l + 1, \quad 16l + 1$$

является простым числом. Тем самым первый случай теоремы Ферма оказался доказанным для всех простых показателей < 197 . Для показателя 197 теорема Лежандра ответа не дает.

После Лежандра многие математики пытались улучшить его результаты. По-видимому, окончательную (далее существенно не улучшаемую элементарными методами) теорему получил в 1893 г. немецкий математик Вендт.

Для любого $m \geq 1$ Вендт ввел некое целое число D_m и, используя общую технику Жермен, показал, что *первый случай теоремы Ферма справедлив для простого показателя l , если существует такое $m \geq 1$, что*

1) *число $p = 2ml + 1$ является простым числом, не делящим числа D_m ;*

2) *число $l^{2m} - 1$ не делится на p .*

Число D_m допускает три равносильных определения:

$$a) \quad D_m = (-1)^m \prod_{j=1}^{2m-1} [(1 + \zeta^j)^{2m} - 1],$$

где $\zeta = \cos \frac{\pi}{m} + i \sin \frac{\pi}{m}$;

б) D_m является определителем матрицы

$$\begin{vmatrix} \binom{2m}{1} & \binom{2m}{2} & \cdots & \binom{2m}{2m-1} & \binom{2m}{2m} \\ \binom{2m}{2} & \binom{2m}{3} & \cdots & \binom{2m}{2m} & \binom{2m}{1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \binom{2m}{2m} & \binom{2m}{1} & \cdots & \binom{2m}{2m-2} & \binom{2m}{2m-1} \end{vmatrix};$$

в) D_m представляет собой так называемый результат многочленов $x^{2m} - 1$ и $(x + 1)^{2m} - 1$.

Отметим, что, несмотря на усилия не одного десятка математиков, среди которых были чрезвычайно остроумные и изобретательные люди, не удалось найти *никаких других* элементарных и вместе с тем достаточно общих подходов к доказательству теоремы Ферма или хотя бы ее первого случая. (Впрочем, общность результатов Жермен до сих пор до конца не выяснена. Например, неизвестно, существует ли бесконечное число простых показателей l , к которым они применимы.)

Неэлементарные методы к первому случаю теоремы Ферма привлек Куммер. В упоминавшейся выше работе 1858 г. он доказал, что *первый случай теоремы Ферма справедлив для простого показателя l , если на l не делится числитель хотя бы одного из двух чисел Бернулли B_{l-3} и B_{l-5} .*

В 1905 г. Мириманов обобщил этот результат, показав, что *достаточно, чтобы l не делило числителя хотя бы одного из четырех чисел Бернулли B_{l-3} , B_{l-5} , B_{l-7} и B_{l-9} .* Это покрывает все $l < 257$.

Используя метод Мириманова, Виферих в 1909 г. доказал, что *первый случай теоремы Ферма справедлив для всех простых показателей l , для которых $2^{l-1} - 1$ не делится на l^2 .* Этот результат произвел сенсацию. О его силе можно судить, например, по тому, что для простых чисел $\leq 200\,183$ он не дает ответа только для двух чисел 1093 и 3511.

Доказательство Вифериха было впоследствии упрощено Миримановым и Фробениусом, которые также показали, что в условии Вифериха основание 2 можно заменить основанием 3 (так что первый случай теоремы Ферма оказывается справедливым для любого

простого показателя l , для которого хотя бы одно из чисел $2^{l-1} - 1$ или $3^{l-1} - 1$ не делится на l^2).

В 1912 г. Фуртвенглер, обратившись к очень сильным средствам (к так называемому закону взаимности Эйзенштейна), доказал критерии Вифериха и Мириманова — Фробениуса буквально в несколько строк. Эта работа послужила началом целой серии исследований, авторы которых, опираясь на самые новейшие достижения теории чисел (например, так называемую теорию полей классов), смогли к 1941 г. доказать, что в критерии Вифериха основание 2 можно заменить произвольным простым числом $p \leq 43$. Это позволило проверить, что *первый случай теоремы Ферма справедлив для всех показателей $l < 6 \cdot 10^9$* .

В 1934 г. Вандивер доказал, что *для простого показателя l справедлив первый случай теоремы Ферма, если второй множитель h_2 не делится на l* . Эта теорема интересна тем, что, как уже говорилось, до сих пор неизвестно ни одного простого показателя l , который бы этому условию не удовлетворял. Однако тот факт, что l не делит h_2 , проверен пока только для $l < 100\,000$.

§ 1. Теорема Жермен

Как же можно подойти к доказательству теоремы Ферма?

В первую очередь, здесь следует заметить, что если тройка (x, y, z) целых чисел удовлетворяет уравнению

$$(1) \quad x^n + y^n = z^n$$

(случай $n = 2$ мы пока не исключаем), то ему будет удовлетворять и любая тройка вида $(\lambda x, \lambda y, \lambda z)$, где λ — произвольное целое число. Обратно, если тройка $(\lambda x, \lambda y, \lambda z)$ является решением уравнения (1), то решением будет и тройка (x, y, z) . Поэтому, чтобы найти все решения уравнения (1) (состоящие из отличных от нуля чисел), достаточно найти решения (x, y, z) , для которых числа x, y, z взаимно просты (не имеют общего множителя, отличного от единицы), а чтобы доказать, что уравнение (1) неразрешимо в целых числах, достаточно привести к противоречию пред-

положение о существовании решения (x, y, z) , состоящего из взаимно простых чисел.

Более того, ясно, что если в каком-нибудь решении (x, y, z) уравнения (1) два из чисел x, y, z имеют общий множитель $\lambda \neq \pm 1$, то третье число также будет делиться на λ . Поэтому мы можем ограничиться лишь решениями, состоящими из попарно взаимно простых чисел. Такие решения мы будем называть *примитивными*.

Далее, ясно, что если теорема Ферма верна для показателя n , то она автоматически верна и для любого показателя an , кратного n , потому что, если уравнение

$$u^{an} + v^{an} = w^{an}$$

имеет целочисленное решение (u, v, w) , то уравнение (1) будет иметь целочисленное решение (u^a, v^a, w^a) . Поэтому теорему Ферма достаточно доказать для $n = 4$ (это сделал, как было уже сказано, сам Ферма) и для $n = l$, где l — произвольное *простое* число ≥ 3 .

Фундаментальную роль во всех рассуждениях, связанных с теоремой Ферма, играет следующая очевидная лемма:

Л е м м а. Пусть a, b и c — такие натуральные (целые положительные) числа, что

1) имеет место равенство

$$ab = c^n;$$

2) числа a и b взаимно просты.

Тогда существуют такие натуральные числа x и y , что

$$a = x^n, \quad b = y^n.$$

Короче говоря, если произведение двух взаимно простых натуральных чисел является n -й степенью, то каждый из сомножителей также будет n -й степенью.

Если n нечетно, то эта лемма справедлива для любых отличных от нуля целых (положительных или отрицательных) чисел a, b и c .

Приведем для полноты доказательство леммы. Пусть

$$a = p_1^{k_1} \dots p_s^{k_s}, \quad b = q_1^{l_1} \dots q_t^{l_t}$$

— разложения чисел a и b в произведение простых чисел. Здесь $k_1 \geq 1, \dots, k_s \geq 1$ и p_1, \dots, p_s — различные простые числа. Ана-

логично $l_1 \geq 1, \dots, l_t \geq 1$ и q_1, \dots, q_t — различные простые числа. При этом, так как числа a и b по условию взаимно просты, то ни одно из чисел p_1, \dots, p_s не равно ни одному из чисел q_1, \dots, q_t . Следовательно, формула

$$(2) \quad c^n = p_1^{k_1} \dots p_s^{k_s} q_1^{l_1} \dots q_t^{l_t}$$

дает разложение числа $c^n = ab^n$ в произведение степеней различных простых чисел. Но известно (это так называемая основная теорема арифметики), что разложение натурального числа в произведение степеней различных простых чисел единственно (с точностью до порядка множителей). Поэтому разложение (2) должно совпадать с разложением, которое получается, когда мы возьмем разложение числа c и возведем его в n -ю степень. Это доказывает, что все показатели $k_1, \dots, k_s, l_1, \dots, l_t$ делятся на n . Поэтому и a , и b являются n -й степенью. ■

Мы привели это доказательство (безусловно, известное читателю) в основном для того, чтобы подчеркнуть роль, которую играет в нем основная теорема арифметики.

Для любого примитивного решения (x, y, z) уравнения

$$(3) \quad x^l + y^l = z^l, \quad l \text{ простое } \geq 3,$$

число z^l будет произведением ab целых чисел

$$a = x + y$$

и

$$(4) \quad b = \frac{x^l + y^l}{x + y} = \frac{(a - y)^l + y^l}{a} = \\ = a^{l-1} - \binom{l}{1} a^{l-2} y + \dots + (-1)^k \binom{l}{k} a^{l-k-1} y^k + \dots \\ \dots + \binom{l}{l-1} y^{l-1},$$

где

$$\binom{l}{k} = \frac{l!}{k!(l-k)!}$$

— так называемые биномиальные коэффициенты (часто обозначаемые также символом C_l^k).

Из равенства (4) следует, что любой общий простой делитель p чисел a и b делит число

$$\binom{l}{l-1} y^{l-1} = l y^{l-1},$$

и потому, если $p \neq l$, и число y . Но если p делит a и y , то p делит $x = a - y$, что невозможно, ибо, по условию, числа x и y взаимно просты. Если теперь z

не делится на l , то l не делит $z^l = ab$, а значит, ни a , ни b . Таким образом, в этом случае числа a и b взаимно просты и потому, согласно лемме (в которой следует положить $c = z$ и $n = l$), существуют такие целые числа u и v , что

$$x + y = u^l, \quad \frac{x^l + y^l}{x + y} = v^l, \quad z = uv.$$

Заметив теперь, что уравнение (3) может быть переписано в виде

$$x^l + y^l + (-z)^l = 0$$

и, следовательно, что числа x , y , $-z$ играют в нем вполне симметричные роли, мы получим, что аналогичные формулы должны иметь место для тройки $(y, -z, x)$ и для тройки $(-z, x, y)$. Этим доказано следующее предложение:

Предложение 1. Для любых попарно взаимно простых и не делящихся на l целых чисел x, y, z , удовлетворяющих уравнению (3), существуют такие пары целых чисел (u, v) , (u_1, v_1) и (u_2, v_2) , состоящие из взаимно простых чисел, что

$$(5) \quad \begin{aligned} x + y &= u^l, & \frac{x^l + y^l}{x + y} &= v^l, & z &= uv, \\ z - y &= u_1^l, & \frac{z^l - y^l}{z - y} &= v_1^l, & x &= u_1 v_1, \\ z - x &= u_2^l, & \frac{z^l - x^l}{z - x} &= v_2^l, & y &= u_2 v_2. \end{aligned}$$

Формулы (5) известны как формулы Абеля, хотя их знала еще Жермен, а опубликованы они были впервые Лежандром.

Аналогичные (но более сложные) формулы могут быть выведены и в случае, когда одно из чисел x, y, z делится на l . Однако за полтора столетия интенсивных исследований эти формулы никакой реальной пользы не принесли, и поэтому мы их выписывать здесь не будем.

Исследование теоретико-числовых проблем, связанных с делимостью чисел, существенно облегчается удобными обозначениями, предложенными Гауссом.

Пусть n — произвольное натуральное число. Согласно Гауссу, целые числа a и b называются *сравнимыми по модулю n* , если их разность $a - b$ делится на n . В этом случае пишут

$$a \equiv b \pmod{n}.$$

Ясно, что отношение сравнимости является отношением эквивалентности, и потому множество \mathbb{Z} всех целых чисел распадается на классы сравнимых между собой чисел. Множество всех этих классов мы будем обозначать символом \mathbb{Z}/n .

Сравнения, подобно равенствам, можно складывать и умножать. Их можно также сокращать на общий множитель, если только этот множитель взаимно прост с n . На языке современной алгебры это означает, что множество \mathbb{Z}/n всех классов сравнимых чисел является кольцом (ассоциативным, коммутативным и обладающим единицей), причем классы, состоящие из чисел, взаимно простых с n , не являются в этом кольце делителями нуля.

Более того, легко видеть, что эти классы в кольце \mathbb{Z}/n даже обратимы, т. е. для любого числа a , взаимно простого с n , существует такое число b («обратное по модулю n для a »), что

$$(6) \quad ab \equiv 1 \pmod{n}.$$

Действительно, так как числа a и n взаимно просты, то по известной теореме элементарной теории чисел (которую, кстати сказать, мы докажем в § 4), существуют такие целые числа x и y , что

$$nx + ay = 1.$$

Но ясно, что это равенство в точности равносильно сравнению (6) $c \equiv b \pmod{n}$.

В частности, мы видим, что если $n = l$, где l — простое число, то все отличные от нуля элементы кольца \mathbb{Z}/l обратимы, т. е. это кольцо является полем.

Иными словами множество $(\mathbb{Z}/l)^*$ всех отличных от нуля элементов кольца \mathbb{Z}/l является группой по умножению.

С другой стороны, ясно, что любое число сравнимо по модулю l с одним и только одним из чисел

$$(7) \quad 0, 1, 2, \dots, l-1,$$

откуда следует, что поле \mathbb{Z}/l содержит l элементов, а группа $(\mathbb{Z}/l)^*$ содержит $l-1$ элементов, т. е. порядок этой группы равен $l-1$.

Но из элементарной теории групп известно, что, возведя любой элемент конечной группы в степень, равную порядку группы, мы получим единицу группы. Применительно к группе $(\mathbb{Z}/l)^*$ это означает, что

$$(8) \quad a^{l-1} \equiv 1 \pmod{l}$$

для любого целого числа a , не делящегося на l . Это утверждение называется малой теоремой Ферма.

Умножив сравнение (8) на a , мы получим сравнение

$$(9) \quad a^l \equiv a \pmod{l}.$$

Ясно, что это сравнение выполнено и при $a \equiv 0 \pmod{l}$. Таким образом, сравнение (9) имеет место для любых целых чисел a . Это — малая теорема Ферма в формулировке Эйлера.

На более алгебраическом языке сравнение (9) означает, что каждый элемент поля \mathbb{Z}/l является корнем многочлена $X^l - X$.

Доказать сравнение (9) можно, и не обращаясь к теории групп, например, следующим образом.

Из того, что простое число l делит $l!$ и при $0 < k < l$ не делит $k!(l-k)!$, следует, что все биномиальные коэффициенты

$$\binom{l}{k} = \frac{l!}{k!(l-k)!}, \quad 0 < k < l,$$

делятся на l . Поэтому

$$(x_1 + x_2)^l \equiv x_1^l + x_2^l \pmod{l}$$

для любых (целых) x_1 и x_2 .

Очевидной индукцией отсюда вытекает аналогичная формула для любого числа слагаемых:

$$(10) \quad (x_1 + x_2 + \dots + x_n)^l \equiv x_1^l + x_2^l + \dots + x_n^l \pmod{l}.$$

Положив в этой формуле $x_1 = \dots = x_n = 1$, мы и получим (9) (при $a = n$). ■

Более общим образом мы можем рассмотреть произвольный многочлен

$$a(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n$$

с целыми коэффициентами. Тогда, согласно формуле (10),

$$a(X)^l \equiv (a_0 X^n)^l + (a_1 X^{n-1})^l + \dots + a_n^l \pmod{l},$$

а, согласно формуле (9),

$$a_0^l \equiv a_0, \quad a_1^l \equiv a_1, \quad \dots, \quad a_n^l \equiv a_n \pmod{l}.$$

Поэтому

$$a(X)^l \equiv a_0 X^{nl} + a_1 X^{(n-1)l} + \dots + a_n \pmod{l},$$

т. е.

$$(11) \quad a(X)^l \equiv a(X^l) \pmod{l}.$$

Этой формулой (называемой иногда формулой Шенемана) мы часто будем пользоваться.

Теперь мы можем непосредственно приступить к изложению исследований Жермен.

Пусть (x, y, z) — примитивное решение уравнения (3), состоящее из чисел, не делящихся на l . Рассмотрим произвольное простое число p , сравнимое с единицей по модулю l , т. е. имеющее вид

$$p = 2ml + 1,$$

где m — некоторое целое число. Предположим, что ни одно из чисел x, y, z не делится на p . Поскольку $x \not\equiv 0 \pmod{p}$, существует такое целое число x' , что

$$xx' \equiv 1 \pmod{p}.$$

Умножив на $(x')^l$ равенство (3) и перейдя к сравнениям, мы получим, что $1 + (yx')^l \equiv (zx')^l \pmod{p}$, т. е. что

$$1 + a^l \equiv b^l \pmod{p},$$

где $a = yx'$, $b = zx'$ не делятся на p .

Целое число ξ мы будем называть *l -й степенью по модулю p* , если существует такое число $a \not\equiv 0 \pmod{p}$, что

$$\xi \equiv a^l \pmod{p}.$$

Кроме того, две l -е степени ξ и η мы будем называть *соседними по модулю p* , если

$$\xi - \eta \equiv \pm 1 \pmod{p}.$$

В этой терминологии доказанное выше сравнение означает, что, *если ни одно из чисел x , y , z не делится на p , то существуют соседние l -е степени по модулю p* .

Предположим теперь, что одно (и, в силу примитивности, только одно) из чисел x , y , z делится на p . Для определенности будем считать, что на p делится число z . Тогда одно (и только одно) из фигурирующих в формуле Абеля $z = uv$ (см. (5)) взаимно простых чисел u и v будет делиться на p .

Пусть на p делится v . Тогда u на p не делится, и потому существует такое число u' , что

$$uu' \equiv 1 \pmod{p}.$$

С другой стороны, из формул Абеля (5) следует, что

$$2z = u^l + u_1^l + u_2^l.$$

Поэтому

$$u^l + u_1^l \equiv (-u_2)^l \pmod{p}$$

и, значит,

$$1 + (u_1 u')^l \equiv (-u_2 u')^l \pmod{p}.$$

Таким образом, *если v делится на p , то также существуют соседние l -е степени по модулю p* .

Пусть, наконец, на p делится u . Тогда в соотношении (4) (где, напомним, $b = v^l$, $a = u^l$) все слагаемые правой части, кроме последнего $\binom{l}{l-1} u^{l-1} v = l u^{l-1} v$,

будут делиться на p , и, следовательно, будет иметь место сравнение

$$v^l \equiv ly^{l-1} \pmod{p}.$$

Но по тем же формулам Абеля

$$y = z - u_1^l,$$

т. е.

$$y \equiv (-u_1)^l \pmod{p}.$$

Следовательно,

$$v^l \equiv l(-u_1)^{l(l-1)} \pmod{p}$$

и потому

$$l \equiv (vu_1')^l \pmod{p},$$

где u_1' — такое число, что

$$u_1^{l-1} u_1' \equiv 1 \pmod{p}$$

(ясно, что u_1 , а значит, и u_1^{l-1} не делится на p).

Этим доказано, что при $u \equiv 0 \pmod{p}$ число l является l -й степенью по модулю p .

Тем самым доказана следующая теорема:

Теорема Софи Жермен. Пусть для простого числа $l \geq 3$ существует такое целое число m , что

- 1) число $p = 2ml + 1$ является простым числом;
- 2) среди l -х степеней по модулю p нет соседних;
- 3) число l не является l -й степенью по модулю p .

Тогда для показателя l справедлив первый случай теоремы Ферма.

Для проверки в конкретных ситуациях условий 2) и 3) этой теоремы полезно иметь в виду, что любая l -я степень ξ по модулю $p = 2ml + 1$ удовлетворяет сравнению

$$(12) \quad \xi^{2m} \equiv 1 \pmod{p}.$$

Действительно, если $\xi = a^l \pmod{p}$, где $a \not\equiv 0 \pmod{p}$, то по малой теореме Ферма

$$\xi^{2m} \equiv a^{2ml} \equiv a^{p-1} \equiv 1 \pmod{p}. \quad \blacksquare$$

Задача. Докажите, что и, обратно, любое решение ξ сравнения (12) является l -й степенью по модулю p .

(Указание. Воспользуйтесь понятием первообразного корня по модулю p ; см. ниже стр. 60.)

Легко видеть, что для любого простого числа p существует только два несравнимых числа ξ , удовлетворяющих сравнению

$$\xi^2 \equiv 1 \pmod{p},$$

а именно, числа 1 и $-1 \equiv p-1 \pmod{p}$.

Тот факт, что числа 1 и $p-1$ удовлетворяют этому сравнению, очевиден, а то, что других корней это сравнение не имеет, проще всего доказывается ссылкой на теорему алгебры о том, что в произвольном поле многочлен степени n не может иметь более n корней. (Можно также воспользоваться тем, что число $\xi^2 - 1 = (\xi - 1)(\xi + 1)$ тогда и только тогда делится на простое число p , когда $\xi - 1$ или $\xi + 1$ делится на p .)

Так как числа 1 и $p-1$ не являются, очевидно, соседними l -ми степенями по модулю $p = 2l + 1$, этим доказано, что при $m = 1$ условие 2) теоремы Жермен автоматически выполнено.

Поскольку число $l^2 - 1 = (l + 1)(l - 1)$ не может делиться на простое число $2l + 1 > l + 1$, то при $m = 1$ условие 3) также выполнено.

Таким образом, если показатель l (являющийся простым нечетным числом) обладает тем свойством, что число $2l + 1$ также является простым числом, то для l справедлив первый случай теоремы Ферма.

Как уже было сказано на стр. 19, это следствие выведено самой Жермен. Многие авторы именно его называют теоремой Жермен.

Аналогичным образом из общей теоремы Жермен может быть выведена сформулированная на стр. 19 теорема Лежандра.

Мы сделаем это только для $m = 2$, поскольку с увеличением m рассуждения стремительно усложняются.

Пусть при $m = 2$ условие 1) теоремы Жермен выполнено, т. е. число $p = 4l + 1$ является простым числом.

Проверим, что условие 2) этой теоремы также будет выполнено. Согласно сделанному выше замечанию для этого достаточно доказать, что среди корней сравнения

$$(13) \quad \xi^4 \equiv 1 \pmod{p}$$

нет соседних.

Так как $\xi^4 - 1 = (\xi^2 + 1)(\xi^2 - 1)$, то корнями сравнения (13) будут корни сравнения

$$\xi^2 \equiv 1 \pmod{p}$$

и сравнения

$$\xi^2 \equiv -1 \pmod{p}.$$

Первое сравнение имеет, как мы знаем, корни 1 и $-1 \equiv p-1$. Что же касается второго сравнения, то а priori возможны два случая: либо оно не имеет корней, либо обладает точно двумя корнями ξ_0 и $-\xi_0 \equiv p-\xi_0$.

В первом случае сравнение (13) имеет корни 1 и $p-1$, заведомо не соседние. Таким образом, условие 2) теоремы Жермен в этом случае выполнено.

Во втором случае (кстати сказать, как можно без труда показать, единственно, на самом деле, реализующемся) сравнение (13) имеет четыре корня

$$1, \quad p-1, \quad \xi_0, \quad p-\xi_0.$$

Соседними два из этих корней могут быть только при $\xi_0 = \pm 2$ или при $\xi_0 = \pm(p-1)/2 = \pm 2l$. Если $\xi_0 = \pm 2$, то $2^2 + 1 = 5$ делится на $p = 4l + 1$, что при $l > 1$ невозможно. Аналогично, если $\xi_0 = \pm 2l$, то $(2l)^2 + 1 = (4l+1)l - (l-1)$ делится на $p = 4l + 1$, т. е. $l-1$ делится на $4l+1$, что при $l > 1$ также невозможно. Следовательно, условие 2) теоремы Жермен выполнено и в этом случае.

Обратимся теперь к условию 3). Если оно не выполнено, то $l^4 \equiv 1 \pmod{p}$. Но поскольку при $p = 4l + 1$ имеет место сравнение $4l \equiv -1 \pmod{p}$, а потому и сравнение $(4l)^4 \equiv 1 \pmod{p}$, отсюда следует, что

$$4^4 \equiv 1 \pmod{p},$$

т. е. что $4^4 - 1 = 255 = 3 \cdot 5 \cdot 17$ делится на p . Так как мы уже знаем, что $p \neq 5$, это возможно только при $p = 17$. Но уравнение $17 = 4l + 1$ имеет простое решение $l = 4$, и потому этот случай также невозможен. Следовательно, условие 3) должно быть выполнено. ■

Теорема Вендта (см. стр. 19) также сводится к теореме Жермен. Следует лишь доказать, что если простое число $p = 2ml + 1$ не делит число Вендта D_m , то условие 2) теоремы Жермен выполнено.

Это доказательство мы оставляем читателю в качестве несложного упражнения.

§ 2. Теорема Ферма для показателя 4

Случай $n = 4$ — это единственный случай теоремы Ферма, допускающий вполне элементарное доказательство. Как мы уже говорили, это доказательство было придумано еще самим Ферма. Оно использует формулы общего решения уравнения

$$(1) \quad x^2 + y^2 = z^2,$$

которые были известны еще индусам. Мы начнем с того, что докажем эти формулы.

Как мы знаем, достаточно искать примитивные решения уравнения (1). Ясно, что если (x, y, z) — реше-

ние, то (y, x, z) также будет решением. С другой стороны, для любого решения (x, y, z) хотя бы одно из чисел x или y четно. Действительно, если x и y нечетны, то $x^2 + y^2$ имеет вид $4k + 2$ и потому не может быть равно квадрату z^2 никакого целого числа (ибо каждый квадрат z^2 имеет либо вид $4k$ либо вид $4k + 1$). Кроме того, очевидно, что вместе с решением (x, y, z) и $(\pm x, \pm y, \pm z)$ также будут решениями.

Из этих замечаний непосредственно следует, что нам достаточно найти лишь состоящие из положительных чисел примитивные решения (x, y, z) уравнения (1), для которых число x четно.

Л е м м а. Для любых взаимно простых положительных целых чисел m и $n < m$ разной четности формулы

$$(2) \quad \begin{aligned} x &= 2mn, \\ y &= m^2 - n^2, \\ z &= m^2 + n^2 \end{aligned}$$

доставляют состоящее из положительных целых чисел примитивное решение уравнения (1) с четным x . Обратно, любое состоящее из положительных чисел примитивное решение (x, y, z) уравнения (1), для которого x четно, выражается формулами (2), где m и $n < m$ — взаимно простые числа разной четности.

Д о к а з а т е л ь с т в о. Тожество

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

показывает, что числа (2) (очевидно, положительные) составляют решение, для которого x четно. Если эти числа имеют общий множитель $\lambda \geq 2$, то λ будет делить и числа

$$2m^2 = (m^2 + n^2) + (m^2 - n^2),$$

$$2n^2 = (m^2 + n^2) - (m^2 - n^2).$$

Значит, $\lambda = 2$, ибо, по условию, m и n взаимно просты. Но если $\lambda = 2$, то число $y = m^2 - n^2$ четно, и, следовательно, числа m^2 и n^2 одновременно либо четны, либо нечетны, что невозможно, ибо по условию числа m и n имеют разную четность. Это доказывает, что решение (2) примитивно.

Обратно, путь (x, y, z) — произвольное состоящее из положительных чисел примитивное решение

с четным $x = 2a$. Так как числа y и z нечетны, то числа $z + y$ и $z - y$ четны. Пусть

$$z + y = 2b, \quad z - y = 2c,$$

где числа b и c , очевидно, положительны.

Каждый общий делитель λ чисел b и c делит $z = b + c$ и $y = b - c$. Поэтому $\lambda = \pm 1$, так что числа b и c взаимно просты. С другой стороны.

$$4a^2 = x^2 = z^2 - y^2 = 4bc,$$

т. е.

$$a^2 = bc.$$

Следовательно, согласно лемме из § 1 (примененной к случаю $n = 2$), существуют такие (очевидно, взаимно простые и разной четности) положительные числа m и n , что

$$b = m^2, \quad c = n^2.$$

Тогда $a^2 = m^2 n^2$, т. е. $a = mn$ и

$$x = 2a = 2mn, \quad y = b - c = m^2 - n^2,$$

$$z = b + c = m^2 + n^2.$$

Для завершения доказательства остается заметить, что $n < m$. ■

Теперь мы можем перейти к доказательству теоремы Ферма при $n = 4$. Мы докажем даже более общее утверждение:

Предложение 1. Уравнение

$$(3) \quad x^4 + y^4 = z^2$$

не имеет решений в целых отличных от нуля числах.

Доказательство. Предположим, что решение уравнения (3) в целых отличных от нуля числах существует. Ясно, что, не теряя общности, мы можем считать, что оно состоит из попарно взаимно простых положительных чисел. Так как в любом множестве натуральных чисел существует наименьшее число, то среди всех таких решений существует решение (x, y, z) с наименьшим z . Рассмотрим это решение более внимательно.

Так же, как для решений уравнения (1), немедленно доказываем, что одно из чисел x и y должно

быть четным. Мы будем предполагать, что четно число x . Ясно, что это предположение общности не ограничивает.

Так как

$$(x^2)^2 + (y^2)^2 = z^2$$

и так как числа x^2, y^2, z положительны и взаимно просты, а число x^2 четно, то, согласно лемме, существуют такие взаимно простые числа m и $n < m$ разной четности, что

$$\begin{aligned} x^2 &= 2mn, \\ y^2 &= m^2 - n^2, \\ z &= m^2 + n^2. \end{aligned}$$

Если $m = 2k$ и $n = 2l + 1$, то

$$y^2 = 4(k^2 - l^2 - l - 1) + 3,$$

что невозможно, ибо, как выше мы уже отмечали, любой нечетный квадрат должен иметь вид $4k + 1$. Следовательно, число m нечетно, а число n четно.

Пусть $n = 2q$. Тогда $x^2 = 4mq$ и потому

$$mq = \left(\frac{x}{2}\right)^2.$$

Поскольку числа m и q взаимно просты, отсюда вытекает, что

$$m = z_1^2, \quad q = t^2,$$

где z_1 и t — некоторые целые (очевидно, взаимно простые) положительные числа.

В частности, мы видим, что

$$y^2 = (z_1^2)^2 - (2t^2)^2,$$

т. е. что

$$(2t^2)^2 + y^2 = (z_1^2)^2.$$

Так как числа t и z_1 взаимно просты, к этому равенству снова применима доказанная выше лемма. Следовательно, существуют такие положительные взаимно простые числа a и $b < a$ различной четности, что

$$\begin{aligned} 2t^2 &= 2ab, \quad \text{т. е. } t^2 = ab, \\ y^2 &= a^2 - b^2, \\ z_1^2 &= a^2 + b^2. \end{aligned}$$

Так как a и b взаимно просты, из первого равенства вытекает (по лемме из § 1), что существуют целые числа x_1 и y_1 , для которых

$$a = x_1^2, \quad b = y_1^2.$$

Поэтому третье равенство может быть переписано следующим образом:

$$x_1^4 + y_1^4 = z_1^2.$$

Это означает, что числа x_1, y_1, z_1 составляют (очевидно, примитивное) решение уравнения (3), состоящее из положительных чисел. Следовательно, в силу выбора решения (x, y, z) должно иметь место неравенство

$$z_1 \geq z,$$

а потому и неравенство

$$z_1^2 \geq z,$$

т. е. абсурдное неравенство

$$m \geq m^2 + n^2.$$

Таким образом, предположение о существовании у уравнения (3) целочисленных решений приводит к противоречию. Следовательно, это уравнение не имеет решений в целых отличных от нуля числах. ■

§ 3. Теорема Ферма для показателя 3

Как уже говорилось, теорема Ферма при $l = 3$ впервые была доказана Эйлером в 1768 г. Мы воспроизведем сейчас это доказательство Эйлера.

Эйлер основывается на следующей лемме:

Л е м м а. Если взаимно простые целые числа a и b обладают тем свойством, что число $a^2 + 3b^2$ является кубом целого числа, то существуют такие целые числа s и t , что

$$a = s(s^2 - 9t^2), \quad b = 3t(s^2 - t^2).$$

Покажем сначала, как из этой леммы вытекает теорема Ферма.

Предположим, что при $l = 3$ теорема Ферма неверна, т. е. что существуют такие целые отличные от нуля числа x, y и z , что

$$(1) \quad x^3 + y^3 = z^3.$$

Как мы знаем, числа x , y и z мы можем считать попарно взаимно простыми. Поэтому, в частности, только одно из них может быть четным. С другой стороны, ясно, что все три числа нечетными быть не могут (сумма или разность двух нечетных чисел четна). Следовательно, одно и только одно из чисел x , y , z четно.

Без ограничения общности мы можем считать, что четно число x . Действительно, если четно y , то достаточно переименовать x и y , а если четно z , то достаточно переименовать x и z и изменить знаки (ибо $(-z)^3 + y^3 = (-x)^3$).

Среди всех троек (x, y, z) целых чисел, удовлетворяющих уравнению (1) и таких, что x четно, мы выберем тройку, для которой $|x|$ имеет наименьшее возможное значение. Такая «минимальная» тройка существует, ибо в любом непустом множестве целых положительных чисел существует наименьшее число.

Так как y и z нечетны, то числа

$$p = \frac{z+y}{2} \quad \text{и} \quad q = \frac{z-y}{2}$$

целые. Так как

$$(2) \quad z = p + q, \quad y = p - q,$$

то одно из чисел p и q четно, а другое нечетно. Кроме того, эти числа, очевидно, взаимно просты.

Согласно (1) и (2)

$$\begin{aligned} x^3 &= z^3 - y^3 = (p+q)^3 - (p-q)^3 = \\ &= 6p^2q + 2q^3 = 2q(q^2 + 3p^2) \end{aligned}$$

Полагая здесь $x = 2u$, мы получим, что

$$(3) \quad u^3 = \frac{q}{4}(q^2 + 3p^2).$$

Так как p и q — числа разной четности, то число $q^2 + 3p^2$ нечетно. Поэтому из (3) следует, что q делится на 4 (и, значит, q четно, а p нечетно).

Согласно доказанной в § 1 лемме, произведение двух взаимно простых чисел тогда и только тогда является кубом, когда каждое из них является кубом. С другой стороны, числа $q/4$ и $q^2 + 3p^2$ тогда и только тогда взаимно просты, когда взаимно просты числа q

и $3p^2 = (q^2 + 3p^2) - q^2$, что имеет место (в силу взаимной простоты чисел p и q) тогда и только тогда, когда q не делится на 3. Поэтому, если мы предположим, что q не делится на 3, то из (3) будет следовать, что числа $q/4$ и $q^2 + 3p^2$ являются кубами.

Но, согласно лемме, если $q^2 + 3p^2$ — куб, то

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2),$$

где s и t — некоторые целые числа. Так как p нечетно, то из равенства $p = 3t(s^2 - t^2)$ следует, что t нечетно, а s четно. Кроме того, так как p и q взаимно просты, то t и s также взаимно просты.

Так как число $q/4$ — куб, то число $2q = 8 \cdot q/4$ — также куб. Это доказывает, что число

$$2s(s^2 - 9t^2) = 2s(s - 3t)(s + 3t)$$

тоже является кубом.

Числа $2s$, $s - 3t$ и $s + 3t$ взаимно просты. Действительно, если $2s$ и $s \pm 3t$ имеют общий простой множитель λ , то $\lambda \neq 2$, ибо число $s \pm 3t$ нечетно. Следовательно, λ делит s и $\pm 3t = (s \pm 3t) - s$. Но, так как t и s взаимно просты, это возможно только при $\lambda = 3$. Аналогично, если числа $s + 3t$ и $s - 3t$ имеют общий простой множитель λ , то, во-первых, $\lambda \neq 2$, ибо оба эти числа нечетны, а, во-вторых, числа $2s = (s + 3t) + (s - 3t)$ и $6t = (s + 3t) - (s - 3t)$ делятся на λ , что опять возможно только при $\lambda = 3$. Таким образом, в обоих случаях число s , а значит, и число q делятся, вопреки предположению, на $\lambda = 3$.

Так как произведение взаимно простых чисел $2s$, $s - 3t$ и $s + 3t$ является кубом, то, следовательно, кубом будет и каждое из них. Это означает, что существуют такие целые числа x_1 , y_1 и z_1 , что

$$\begin{aligned} x_1^3 &= 2s, \\ y_1^3 &= -(s + 3t), \\ z_1^3 &= s - 3t, \end{aligned}$$

и, следовательно,

$$x_1^3 + y_1^3 = z_1^3.$$

Таким образом, исходя из тройки (x, y, z) , мы получили новую тройку (x_1, y_1, z_1) , также удовлетворяю-

щую уравнению (1) и обладающую тем свойством, что ее первое число x_1 четно.

Так как $x^3 = 2q(q^2 + 3p^2)$, то $|q| < \frac{|x^3|}{2}$, а так как $q = s(s^2 - 9t^2)$, то $|s| \leq |q|$. Следовательно,

$$|x_1^3| = 2|s| < |x^3|$$

и потому $|x_1| < |x|$, что противоречит свойству минимальности тройки (x, y, z) . Полученное противоречие доказывает, что число q должно делиться на 3, т. е. должно иметь место равенство

$$q = 3r,$$

где r — некоторое целое число (делящееся на 4), а потому (см. (3)) и равенство

$$(4) \quad u^3 = \frac{3}{4}r(9r^2 + 3p^2) = \frac{9}{4}r(3r^2 + p^2).$$

Если целые числа $\frac{9}{4}r$ и $3r^2 + p^2$ имеют общий простой множитель λ , то $\lambda \neq 3$, так как в противном случае число p делится на 3 и, значит, не взаимно просто с q . Но если $\lambda \neq 3$, то λ делит r и $p^2 = (3r^2 + p^2) - 3r^2$, а значит, q и p , что невозможно. Следовательно, числа $\frac{9}{4}r$ и $3r^2 + p^2$ взаимно просты.

Поэтому из (4) следует, что оба эти числа являются кубами и потому, согласно лемме (примененной к числу $3r^2 + p^2$), имеют место равенства

$$(5) \quad p = s(s^2 - 9t^2), \quad r = 3t(s^2 - t^2),$$

где s и t — некоторые (очевидно, взаимно простые) целые числа. При этом ясно, что число t четно (ибо r четно), а число s , следовательно, нечетно.

Кроме того, мы видим, что (целое) число

$$\frac{8}{27} \cdot \frac{9}{4}r = \frac{2}{3}r = 2t(s^2 - t^2) = 2t(s + t)(s - t)$$

является кубом.

Так как числа s и t взаимно просты и имеют разную четность, то числа $2t$, $s + t$ и $s - t$ попарно взаим-

но просты. Поэтому каждое из них является кубом, так что существуют такие целые числа x_1 , y_1 и z_1 , что

$$\begin{aligned}x_1^3 &= 2t, \\y_1^3 &= s - t, \\z_1^3 &= s + t.\end{aligned}$$

Но тогда

$$x_1^3 + y_1^3 = z_1^3$$

и

$$|x_1^3| = 2|t| \leq \frac{2}{3}|r| = \frac{2}{9}|q| < 2|q| < |x^3|,$$

т. е. $|x_1| < |x|$.

Таким образом, и в этом случае мы приходим в противоречие с минимальностью тройки (x, y, z) . Поэтому уравнение $x^3 + y^3 = z^3$ решений иметь не может. ■

§ 4. Арифметика кольца D_3

Итак, для завершения доказательства теоремы Ферма при $l = 3$ нам осталось лишь доказать сформулированную выше лемму.

Эйлер доказывает эту лемму, замечая, что ¹⁾

$$a^2 + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3}).$$

Потом он пишет, что, поскольку левая часть является по условию кубом, то и оба множителя правой части должны быть кубами. В частности,

$$a + b\sqrt{-3} = (s + t\sqrt{-3})^3,$$

где s и t — некоторые целые числа. Возводя в куб, мы получаем, что

$$a + b\sqrt{-3} = s^3 - 9st^2 + (3s^2t - 3t^3)\sqrt{-3}$$

и, следовательно, что

$$\begin{aligned}a &= s^3 - 9st^2 = s(s^2 - 9t^2), \\b &= 3s^2t - 3t^3 = 3t(s^2 - t^2).\end{aligned}\quad \blacksquare$$

¹⁾ Здесь и далее под $\sqrt{-3}$ понимается корень уравнения $x^2 + 3 = 0$, лежащий в верхней полуплоскости.

Нельзя не отдать должное остроумию и смелости Эйлера, бесстрашно перешедшего от целых чисел к числам вида $a + b\sqrt{-3}$. Но, конечно, чтобы сделать его доказательство безупречным, надо предварительно построить арифметику таких чисел. В частности, поскольку утверждение о произведениях, являющихся кубами, существенно зависит, как мы знаем, от основной теоремы арифметики, нужно для чисел вида $a + b\sqrt{-3}$ доказать аналог этой теоремы (мы не говорим уже о том, что требует доказательства «взаимная простота» чисел $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$).

Однако оказывается, что для чисел вида $a + b\sqrt{-3}$ основная теорема арифметики неверна: единственности разложения на «простые» (далее неразложимые) множители нет. Например,

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

и, вместе с тем, числа 2 и $1 \pm \sqrt{-3}$ неразложимы.

Доказательство. Имеем

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = ac - 3bd + (ad + bc)\sqrt{-3}.$$

Поэтому, если

$$2 = (a + b\sqrt{-3})(c + d\sqrt{-3}),$$

то

$$\begin{cases} ac - 3bd = 2, \\ ad + bc = 0. \end{cases}$$

Можно непосредственно доказать, что эти уравнения не имеют решений в целых числах, но лучше поступить по-другому, заметив, что они не меняются при одновременном изменении знака у b и d . Поэтому

$$2 = (a - b\sqrt{-3})(c - d\sqrt{-3})$$

и, значит,

$$2 \cdot 2 = (a + b\sqrt{-3})(a - b\sqrt{-3}) \cdot (c + d\sqrt{-3})(c - d\sqrt{-3}),$$

т. е.

$$(1) \quad 4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

Аналогично, если

$$1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3}),$$

то

$$1 - \sqrt{-3} = (a - b\sqrt{-3})(c - d\sqrt{-3}),$$

и потому мы снова получаем уравнение (1).

Поскольку в этом уравнении участвуют только натуральные числа, то либо один из множителей правой части равен 4, а другой 1, т. е., скажем,

$$a^2 + 3b^2 = 4,$$

$$c^2 + 3d^2 = 1,$$

либо оба они равны 2, т. е.

$$a^2 + 3b^2 = 2,$$

$$c^2 + 3d^2 = 2.$$

Но ясно, что уравнение вида $a^2 + 3b^2 = 2$ не имеет решения в целых числах. Поэтому второй случай невозможен. Что же касается первого, то уравнение

$$a^2 + 3b^2 = 4$$

удовлетворяется только при $a = \pm 1$, $b = \pm 1$ и $a = \pm 2$, $b = 0$, а уравнение

$$c^2 + 3d^2 = 1$$

— только при $c = \pm 1$, $d = 0$.

Это доказывает неразложимость как числа 2, так и чисел $1 \pm \sqrt{-3}$. ■

Тем не менее рассуждение Эйлера можно спасти, если чуть глубже вникнуть в предмет.

Поставим вопрос, закономерно ли у Эйлера появились числа вида $a + b\sqrt{-3}$, или это было случайным эффектом, обязанным изобретательности Эйлера?

Если вообще прибегать к каким-нибудь нецелым числам, то в первую очередь следует, конечно, привлечь числа, участвующие в разложении левой части уравнения Ферма на линейные множители. Такое разложение имеет вид

$$x^3 + y^3 = (x + y)(x + \xi y)(x + \bar{\xi} y),$$

где ξ и $\bar{\xi}$ — комплексные числа, являющиеся вместе с 1 корнями уравнения

$$(2) \quad x^3 = 1.$$

Это соображение подсказывает, что естественной областью, в которой следует рассматривать уравнение Ферма при $l = 3$, являются числа вида

$$(3) \quad a + b\xi + c\bar{\xi},$$

где a , b и c — целые числа.

Но легко видеть, что вместе с числом ξ корнем уравнения (2) будет и число ξ^2 , ибо

$$(\xi^2)^3 = (\xi^3)^2 = 1^2 = 1.$$

Поэтому $\xi^2 = \bar{\xi}$, и, значит, число (3) мы можем записывать в виде

$$(3') \quad a + b\xi + c\xi^2.$$

Более того, число ξ (вместе с числом $\bar{\xi} = \xi^2$) является корнем уравнения

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1 = 0,$$

откуда следует, что

$$(4) \quad \xi^2 = -1 - \xi.$$

Поэтому любое число вида (3') имеет вид

$$(5) \quad A + B\xi,$$

где $A = a - c$, $B = b - c$.

Итак, мы видим, что нам следует ввести в рассмотрение множество всех чисел вида (5), где A и B — произвольные целые числа. Это множество мы будем обозначать символом D_3 .

Ясно, что сумма и разность чисел из D_3 является числом из D_3 . Более того, произведение любых двух чисел из D_3 также будет числом из D_3 , поскольку появляющийся после перемножения член с ξ^2 мы можем преобразовать с помощью соотношения (4). (Таким образом, $(A + B\xi)(A_1 + B_1\xi) = (AA_1 - BB_1) + (AB_1 + BA_1 - BB_1)\xi$.)

На языке современной алгебры все это означает, что D_3 является *кольцом* (числовым).

Для удобства вычислений целесообразно рассматривать также числа вида (5) с произвольными рациональными A и B . Множество таких чисел мы обозначим через K_3 .

Ясно, что сумма, разность и произведение чисел из K_3 также будет числом из K_3 . Однако теперь и частное любых двух чисел из K_3 будет числом из K_3 . Действительно, любое число вида $\frac{C + D\xi}{A + B\xi}$, где, конечно, $A + B\xi \neq 0$, мы можем преобразовать следующим

образом (в элементарной алгебре это называется «освобождением знаменателя от иррациональности»):

$$\begin{aligned}\frac{C + D\xi}{A + B\xi} &= \frac{(C + D\xi)(A + B\bar{\xi})}{(A + B\xi)(A + B\bar{\xi})} = \frac{(C + D\xi)(A + B\xi^2)}{A^2 + AB(\xi + \bar{\xi}) + B^2\xi\bar{\xi}} = \\ &= \frac{CA + DA\xi + CB\xi^2 + DB\xi^3}{A^2 - AB + B^2} = \\ &= \frac{CA + DB - CB}{A^2 - AB + B^2} + \frac{DA - CB}{A^2 - AB + B^2} \xi.\end{aligned}$$

Все это означает, что K_3 является полем. Оно называется *3-круговым полем* (это название возникло из-за тесной связи корней уравнения (2) с задачей деления круга на 3 части). Числа из D_3 называются, естественно, *целыми числами поля K_3* ; соответственно этому, D_3 называется *кольцом целых чисел* поля K_3 . Оно содержит все обычные целые числа (они получаются при $B = 0$).

Заметим, что запись числа из D_3 (или из K_3) в форме (5) единственна. Действительно, если

$$A + B\xi = A_1 + B_1\xi$$

и $B \neq B_1$, то

$$\xi = -\frac{A - A_1}{B - B_1},$$

что невозможно, ибо ξ не является вещественным и, тем более, рациональным числом. Следовательно, $B = B_1$ и потому $A = A_1$. ■

Выше при вычислении частного в K_3 мы фактически ввели для любого числа

$$\alpha = A + B\xi \in K_3$$

число

$$N\alpha = \alpha\bar{\alpha} = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4}.$$

Это неотрицательное рациональное число (целое, когда $\alpha \in D_3$) называется *нормой* числа α . Оно равно нулю только при $\alpha = 0$.

Замечательное свойство нормы состоит в том, что *норма произведения равна произведению норм*:

$$(6) \quad N(\alpha\beta) = N\alpha \cdot N\beta, \quad \alpha, \beta \in K_3.$$

Действительно,

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta \cdot \bar{\alpha}\bar{\beta} = \alpha\bar{\alpha} \cdot \beta\bar{\beta} = N\alpha \cdot N\beta. \quad \blacksquare$$

В раскрытом виде соотношение (6) имеет вид

$$(AA_1 - BB_1)^2 - (AA_1 - BB_1)(AB_1 + BA_1 - BB_1) + \\ + (AB_1 + BA_1 - BB_1)^2 = (A^2 - AB + B^2)(A_1^2 - A_1B_1 + B_1^2)$$

Оно является простейшим примером алгебраических тождеств, возникающих из соотношений вида (6) для других полей алгебраических чисел.

Числа из K_3 (и D_3) можно записать в более явной форме, заметив, что квадратное уравнение

$$x^2 + x + 1 = 0$$

имеет корни

$$\frac{-1 \pm \sqrt{-3}}{2}.$$

Любой из этих корней можно принять за ζ . Для определенности мы положим

$$\zeta = \frac{-1 + \sqrt{-3}}{2}.$$

Тогда

$$A + B\zeta = \frac{(2A - B) + B\sqrt{-3}}{2}.$$

Таким образом, получается, что числа из K_3 имеют вид $a + b\sqrt{-3}$, где a и b — рациональные числа, а числа из D_3 (целые числа из K_3) — вид

$$(7) \quad \frac{p + q\sqrt{-3}}{2},$$

где p и q — целые числа одинаковой четности.

В частности, при p и q четных мы получаем числа Эйлера

$$a + b\sqrt{-3}.$$

Таким образом, ограничение только такими числами с общей точки зрения ничем не оправдано, и поэтому можно надеяться, что при переходе к более естественно возникающим числам (7) все наши трудности исчезнут. Оказывается, что это и на самом деле так.

Чтобы избежать кустарности в исследовании этой проблематики, целесообразно ввести простейшие основные понятия арифметики в кольцах. Хотя сейчас нам нужно только кольцо D_3 , а в дальнейшем понадобится лишь его непосредственные обобщения D_l , $l \geq 3$, мы дадим определения этих понятий в их естественной общности. Читатель, безразличный к эстетическим сторонам теории и не желающий вникать в абстрактные определения, может пока игнорировать несколько следующих строк и во всем дальнейшем понимать под D кольцо D_3 .

Мы будем считать известным понятие кольца (коммутативного, ассоциативного и с единицей 1). Напомним, что такое кольцо называется *целым кольцом* (традиционное название — «область целостности»), если оно не имеет делителей нуля, т. е. произведение любых его двух отличных от нуля элементов отлично от нуля. *В дальнейшем под кольцом мы будем всегда иметь в виду целое кольцо.*

Каждое целое число $a \in \mathbb{Z}$ мы будем отождествлять с элементом $a \cdot 1$, где 1 — единичный элемент кольца D . Тем самым кольцо целых рациональных чисел \mathbb{Z} окажется подкольцом кольца D .

Основное свойство целых колец, которым мы будем постоянно пользоваться, состоит в том, что в них (и только в них) справедливо *правило сокращения*, т. е. из равенства $\alpha\beta = \alpha\gamma$, где $\alpha \neq 0$, следует, что $\beta = \gamma$.

Элемент ε кольца D называется *единицей* (или *обратимым элементом*; последний термин используется теперь все чаще, а употребление термина «единица» постепенно сходит на нет), если существует такой элемент $\varepsilon^{-1} \in D$, что

$$\varepsilon\varepsilon^{-1} = 1.$$

Ясно, что произведение и частное двух единиц также является единицей.

Пример 1. Кольцо \mathbb{Z} целых рациональных чисел имеет две единицы $+1$ и -1 .

Пример 2. Элемент $\varepsilon \in D$ называется *корнем из единицы степени n* , если

$$\varepsilon^n = 1$$

(первообразным, если $\varepsilon^m \neq 1$ при $0 < m < n$). Ясно, что каждый корень из единицы (содержащийся в D) будет единицей кольца D (для которой $\varepsilon^{-1} = \varepsilon^{n-1}$).

Пример 3. Найдем единицы кольца D_3 . С этой целью мы заметим сначала, что число $\alpha \in D_3$ тогда и только тогда является единицей, когда $N\alpha = 1$.

Действительно, если $\alpha\alpha^{-1} = 1$, то

$$N\alpha \cdot N\alpha^{-1} = N(\alpha\alpha^{-1}) = N1 = 1,$$

и потому $N\alpha = 1$. Обратно, если $N\alpha = 1$, т. е. $\alpha\bar{\alpha} = 1$, то α является единицей (с $\alpha^{-1} = \bar{\alpha}$). ■

Так как для числа $\alpha = A + B\zeta$ норма $N\alpha$ выражается формулой

$$N\alpha = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4},$$

то $N\alpha = 1$ тогда и только тогда, когда либо $B = 0$ и $A = \pm 1$, либо $B = \pm 1$ и $(2A - B)^2 = 1$, т. е. $A = \pm B = \pm 1$ или $A = 0$, $B = \pm 1$. Таким образом, кольцо D_3 имеет шесть единиц:

$$\begin{aligned} +1, \quad +\zeta, \quad 1+\zeta &= -\zeta^2, \\ -1, \quad -\zeta, \quad -1-\zeta &= \zeta^2. \end{aligned}$$

Все они являются корнями из единицы степени 6. При этом каждая единица является степенью единицы

$$1 + \zeta = \frac{1 + \sqrt{-3}}{2}$$

(первообразного корня из единицы степени 6). Именно,

$$\begin{aligned} (1 + \zeta)^1 &= 1 + \zeta, & (1 + \zeta)^2 &= \zeta, & (1 + \zeta)^3 &= -1, \\ (1 + \zeta)^4 &= -1 - \zeta, & (1 + \zeta)^5 &= -\zeta, & (1 + \zeta)^6 &= 1. \end{aligned}$$

Пусть D^* — множество $D \setminus \{0\}$ всех отличных от нуля элементов кольца D .

Два элемента $\alpha, \beta \in D^*$ называются *ассоциированными* (обозначение $\alpha \sim \beta$), если существует такая единица ε , что $\beta = \varepsilon\alpha$. Очевидно, что отношение ассоциированности является отношением эквивалентности и потому множество D^* распадается на классы ассоциированных элементов.

Пусть $D' \subset D^*$ — множество всех отличных от нуля элементов кольца D , не являющихся единицами.

Элемент $\alpha \in D'$ называется *разложимым*, если существуют такие элементы $\beta, \gamma \in D'$, что $\alpha = \beta\gamma$. Неразложимый элемент $\alpha \in D'$ называется также *простым элементом*.

Функция $\alpha \mapsto \|\alpha\|$, определенная на D^* и принимающая значения в множестве \mathbb{N} целых положительных чисел, называется *псевдонормой*, если из того, что $\alpha \in D^*$ делится на $\beta \in D^*$ (т. е. $\alpha = \beta\gamma$, где $\gamma \in D$), следует, что $\|\alpha\| \geq \|\beta\|$.

Если γ — единица, то $\beta = \alpha\gamma^{-1}$, где $\gamma^{-1} \in D$, и потому $\|\beta\| \geq \|\alpha\|$. Следовательно, *если элементы α и β ассоциированы, то $\|\alpha\| = \|\beta\|$* . Если обратное тоже верно, т. е. если $\|\alpha\| > \|\beta\|$, когда α делится на β , но частное γ не является единицей, то псевдонорма называется *строгой*.

Примером строгой псевдонормы является, очевидно, норма в D_3 .

Предложение 1. *Если в кольце D существует строгая псевдонорма, то любой элемент $\alpha \in D'$ разлагается в произведение простых элементов, т. е.*

$$(8) \quad \alpha = \pi_1 \pi_2 \dots \pi_k,$$

где $\pi_1, \pi_2, \dots, \pi_k$ — *простые элементы*.

Доказательство. Значения псевдонормы на элементах $\alpha \in D'$ являются целыми положительными числами. Поэтому среди них существует наименьшее. Пусть p_0 — это наименьшее значение. Ясно, что любой элемент $\alpha \in D'$, для которого $\|\alpha\| = p_0$, будет простым. Поэтому разложение (8) для него имеет место (с $k = 1$ и $\pi_1 = \alpha$). Пусть теперь $p > p_0$ и пусть существование разложения (8) доказано для всех элементов $\alpha \in D'$ с $\|\alpha\| < p$. Рассмотрим произвольный элемент $\alpha \in D'$, для которого $\|\alpha\| = p$. Если α прост, то доказывать нечего. Пусть $\alpha = \alpha_1 \alpha_2$, где $\alpha_1, \alpha_2 \in D'$. Тогда $\|\alpha_1\| < \|\alpha\| = p$ и $\|\alpha_2\| < \|\alpha\| = p$. Поэтому для элементов α_1 и α_2 существуют разложения (8). Перемножив их, мы и получим разложение элемента α . Тем самым предложение 1 по индукции полностью доказано. ■

Вообще говоря, разложение (8) не единственно. Например, можно менять порядок простых множителей и заменять их на ассоциированные (с тем, конеч-

но, чтобы произведение всех дополнительных множителей-единиц было равно 1). Назовем два разложения

$$\alpha = \pi_1 \dots \pi_r \quad \text{и} \quad \alpha = \pi'_1 \dots \pi'_s$$

элемента $\alpha \in D'$ в произведение простых множителей *ассоциированными*, если $r = s$ и, после возможной перенумерации, элемент π'_i для каждого $i = 1, \dots, r$ ассоциирован с элементом π_i . Если любой элемент $\alpha \in D'$ разлагается в произведение простых элементов и если каждые два таких разложения ассоциированы, то говорят, что *в кольце D выполнена основная теорема арифметики*, или (допуская определенную неточность) что D является *кольцом с однозначным разложением на множители*.

В таком кольце имеют смысл все основные понятия теории делимости целых чисел, и их свойства аналогичны свойствам, известным из элементарной арифметики.

Например, по аналогии с натуральными числами назовем элементы кольца D *взаимно простыми*, если у них нет общих простых множителей. Тогда то же рассуждение, что и для натуральных чисел (см. лемму в § 1) покажет, что *если в кольце D выполнена основная теорема арифметики, то взаимно простые элементы α и β являются с точностью до единиц n -ми степенями, когда n -й степенью является их произведение $\alpha\beta$* .

Элемент $\delta \in D^*$ называется *наибольшим общим делителем* элементов $\alpha, \beta \in D^*$, если он делит эти элементы и делится на любой другой общий делитель элементов α и β . Ясно, что наибольший общий делитель однозначно определен с точностью до ассоциированности. Однако, вообще говоря, для элементов произвольного кольца он может и не существовать. В кольце же с однозначным разложением на множители наибольший общий делитель существует, очевидно, для любых элементов α и β . Чтобы его найти, следует разложить эти элементы в произведение простых множителей и отобрать в обоих разложениях одинаковые (ассоциированные) множители. Если таких множителей нет (т. е. элементы α и β взаимно просты), — в частности, так будет, если хотя бы один из элементов α и β является единицей, — то наибольшим общим

делителем является элемент 1 (а также произвольная единица).

Из основной теоремы арифметики непосредственно вытекает также следующее утверждение:

(*) Если простой элемент π делит произведение $\alpha\beta$, то он делит либо α , либо β .

Легко видеть, что и обратно, если в кольце D любой элемент $\alpha \in D'$ разлагается в произведение простых элементов (например, если в D есть строгая псевдонорма) и если D обладает свойством (*), то в D имеет место основная теорема арифметики.

Действительно, если

$$\pi_1 \dots \pi_r = \pi'_1 \dots \pi'_s,$$

где $\pi_1, \dots, \pi_r, \pi'_1, \dots, \pi'_s$ — простые элементы, то π_1 делит произведение $\pi'_1 \dots \pi'_s$. Поэтому π_1 делит хотя бы один из сомножителей (это получается из (*) посредством очевидной индукции). Мы можем считать, что π_1 делит π'_1 , т. е. что $\pi'_1 = \pi_1 \varepsilon_1$, где, поскольку элемент π'_1 также прост, элемент ε_1 является единицей. Сократив на π_1 , мы получим, таким образом, что $\pi_2 \dots \pi_r = \varepsilon_1 \pi'_2 \dots \pi'_s$. Аналогично доказывается, что π_2 (после соответствующей перенумерации) делит π'_2 и (после сокращения π_2) что π_3 делит π'_3 и т. д. После r шагов мы получим, во-первых, что $r \leq s$, а во-вторых, что при $r < s$ имеет место равенство

$$1 = \varepsilon_1 \dots \varepsilon_r \pi'_{r+1} \dots \pi'_s.$$

Поскольку это равенство невозможно (элементы $\pi'_{r+1}, \dots, \pi'_s$ единицами, по условию, не являются), этим доказано, что $r = s$ и что для любого $i = 1, \dots, r$ элемент π'_i ассоциирован с элементом π_i . ■

Известно (мы покажем это ниже), что в кольце целых чисел наибольший общий делитель d любых двух чисел a и b может быть представлен в виде

$$(9) \quad ax + by = d,$$

где x и y — целые числа (т. е., иначе говоря, уравнение (9) всегда имеет решение в целых числах). Оказывается, что аналогичное свойство для произвольных колец не вытекает из основной теоремы арифметики. Поэтому приходится вводить еще один класс колец.

Кольцо D называется *кольцом главных идеалов* (происхождение этого названия станет ясным в § 11), если для любых элементов $\alpha, \beta \in D^*$

- а) существует их наибольший общий делитель δ ;
 б) можно найти такие элементы $x, y \in D$, что

$$\alpha x + \beta y = \delta.$$

Легко видеть, что *любое кольцо главных идеалов обладает свойством (*)*.

Действительно, если π не делит α , то π и α взаимно просты, и потому существуют такие элементы $x, y \in D$, что $\alpha x + \pi y = 1$. Умножив это равенство на β , мы получим, что

$$\beta = (\alpha\beta)x + \pi(y\beta).$$

Оба слагаемых справа делятся на π . Поэтому на π делится и элемент β . ■

Говоря, что в кольце D с псевдонормой имеет место *алгоритм деления с остатком* (такое кольцо называется также *евклидовым кольцом*), если для любых элементов $\alpha, \beta \in D^*$ существуют такие элементы γ и ρ , что $\alpha = \beta\gamma + \rho$, причем либо $\rho = 0$, либо $\|\rho\| < \|\beta\|$.

Интересно, что *в евклидовом кольце псевдонорма обязательно является строгой*. Действительно, если $\alpha = \beta\gamma$ и $\|\alpha\| = \|\beta\|$, то, разделив с остатком β на α , мы получим равенство вида

$$\beta = \alpha\delta + \rho,$$

где $\delta \in D$, и либо $\rho = 0$, либо $\|\rho\| < \|\alpha\|$. Но $\rho = \beta(1 - \gamma\delta)$, и потому при $\rho \neq 0$ имеет место неравенство $\|\rho\| \geq \|\beta\| = \|\alpha\|$. Следовательно, $\rho = 0$ и потому $\beta = (\beta\gamma)\delta$, т. е. $\gamma\delta = 1$. ■

С другой стороны, *любое евклидово кольцо является кольцом главных идеалов* (и, следовательно, обладает свойством (*)). Действительно, для любых элементов $\alpha, \beta \in D^*$ в множестве всех отличных от нуля элементов вида

$$(10) \quad \alpha x + \beta y, \quad x, y \in D,$$

существуют элементы с наименьшей псевдонормой. Пусть $\delta = \alpha x_0 + \beta y_0$ — один из таких элементов. Все будет доказано, если мы покажем, что δ является наибольшим общим делителем элементов α и β . Но ясно, что δ делится на любой общий делитель элементов α и β . Поэтому нужно только доказать, что δ делит α и β . Докажем, что δ делит α (для β доказательство аналогично).

Пусть $\alpha = \delta\gamma + \bar{\rho}$, где либо $\rho = 0$, либо $\|\rho\| < \|\delta\|$. Тогда

$$\rho = \alpha - \delta\gamma = \alpha - (\alpha x_0 + \beta y_0)\gamma = \alpha(1 - x_0\gamma) + \beta(-y_0\gamma),$$

так как ρ также имеет вид (10). Следовательно, неравенство $\|\rho\| < \|\delta\|$ невозможно, и, значит, $\rho = 0$. ■

Сопоставляя все доказанное, мы видим, что справедливо следующее предложение:

Предложение 2. *Любое евклидово кольцо является кольцом главных идеалов, в котором выполнена основная теорема арифметики.*

Заметим, что существуют кольца, в которых выполнена основная теорема арифметики, но которые не допускают алгоритма деления с остатком (ни по отношению ни к какой псевдонорме).

Таким кольцом является, например, кольцо всех чисел вида

$$\frac{a + b\sqrt{-19}}{2},$$

где a и b — целые числа одинаковой четности, но доказать это не так-то просто.

Как мы уже говорили, чтобы подвести прочную базу под доказательство Эйлера, достаточно доказать, что в кольце D_3 выполнена основная теорема арифметики. Согласно предложению 2 для этого достаточно доказать следующее предложение:

Предложение 3. *По отношению к норме в кольце D_3 имеет место алгоритм деления с остатком.*

Доказательство. Нужно доказать, что для любых элементов α и $\beta \neq 0$ кольца D_3 существуют такие элементы γ и ρ , что $\alpha = \beta\gamma + \rho$ и $N\rho < N\beta$.

Лемма. *Для любого числа $\xi \in K_3$ существует такое число $\gamma \in D_3$, что*

$$N(\xi - \gamma) \leq \frac{3}{4}.$$

Предложение 3 из этой леммы следует непосредственно. Действительно, применив лемму к числу $\xi = \frac{\alpha}{\beta}$ и положив $\rho = \alpha - \beta\gamma$, мы немедленно получим, что $\alpha = \beta\gamma + \rho$ и что

$$N\rho = N(\alpha - \beta\gamma) = N\beta \cdot N(\xi - \gamma) \leq \frac{3}{4} N\beta < N\beta. \quad \blacksquare$$

Таким образом, нам нужно лишь доказать лемму.

Доказательство леммы. Пусть

$$\xi = A + B\xi,$$

и пусть a и b — такие целые числа, что

$$|A - a| \leq \frac{1}{2}, \quad |B - b| \leq \frac{1}{2}.$$

Тогда для числа

$$\gamma = a + b\xi \in D_3$$

мы получаем

$$\begin{aligned} N(\xi - \gamma) &= (A - a)^2 - (A - a)(B - b) + (B - b)^2 \leq \\ &\leq |A - a|^2 + |A - a| \cdot |B - b| + |B - b|^2 \leq \\ &\leq \left(\frac{1}{2}\right)^2 + \frac{1}{2} \cdot \frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4}. \quad \blacksquare \end{aligned}$$

С л е д с т в и е. В кольце D_3 выполнена основная теорема арифметики.

Существование двух разложений

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

этому не противоречит, так как в D_3 числа 2 и $1 + \sqrt{-3}$ ассоциированы (число $\frac{1 + \sqrt{-3}}{2}$ принадлежит D_3 и является в D_3 единицей).

Теперь для завершения доказательства Эйлера осталось лишь заполнить в нем два незначительных пробела.

Во-первых, надо доказать, что в условиях леммы Эйлера элементы $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ кольца D_3 взаимно просты. Для этого сначала покажем, что число a не делится на 3. Действительно, в противном случае на 3 будет делиться число $a^2 + 3b^2$, которое, являясь кубом, будет делиться поэтому на 27. Следовательно, положив $a = 3a_1$ и $a^2 + 3b^2 = 27N$, мы получим, что $9a_1^2 + 3b^2 = 27N$ и, значит, что $b^2 = 3(3N - a_1^2)$. Таким образом, число b^2 , а потому и число b будут делиться на 3, что противоречит взаимной простоте чисел a и b . \blacksquare

Если теперь элементы $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ делятся на элемент $\gamma \in D_3$, то на γ делятся и элементы

$$2a = (a + b\sqrt{-3}) + (a - b\sqrt{-3}),$$

$$2b\sqrt{-3} = (a + b\sqrt{-3}) - (a - b\sqrt{-3}),$$

откуда, перейдя к нормам, мы немедленно получим, что число $N\gamma$ делит числа $N(2a) = 4a^2$ и $N(2b\sqrt{-3}) = 12b^2$, т. е. делит их наибольший общий делитель. Поскольку же числа a и b взаимно просты и число a не делится на 3, этот наибольший общий делитель равен 4 и, значит, для нормы $N\gamma$ элемента γ имеется только три возможности: $N\gamma = 4$, $N\gamma = 2$ и $N\gamma = 1$.

Если $N\gamma = 4$, то $N\left(\frac{\gamma}{2}\right) = 1$, т. е. $\gamma = 2\varepsilon$, где ε — единица. Таким образом, в этом случае с точностью до ассоциированности имеется единственное решение $\gamma = 2$. Но это решение нам не годится, потому что число $a + b\sqrt{-3}$ тогда и только тогда делится в D_3 на 2, когда оба числа a и b делятся на 2.

Случай $N\gamma = 2$ вообще невозможен, ибо уравнение $x^2 - xy + y^2 = 2$ не имеет целочисленных решений.

Таким образом, обязательно $N\gamma = 1$, т. е. γ является единицей. Следовательно, элементы $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ взаимно просты. ■

Второй пробел, которого не было у Эйлера, но который возник, когда мы перешли к кольцу D_3 , состоит в том, что в равенстве

$$(11) \quad a + b\sqrt{-3} = (s + t\sqrt{-3})^3$$

числа s и t могут, вообще говоря, оказаться нецелыми, поскольку, как мы знаем, числа из D_3 имеют вид

$$(12) \quad \frac{p + q\sqrt{-3}}{2},$$

где p и q — целые числа одинаковой четности.

Чтобы преодолеть эту трудность, мы заметим, что если число (12) записать в форме $A + B\zeta$, то будут иметь место равенства

$$p = 2A - B, \quad q = B.$$

Поэтому числа p и q тогда и только тогда четны (и, значит, число (12) имеет нужный нам вид $s + t\sqrt{-3}$, где s и t целые), когда четно число B . Но формулы

$$(A + B\zeta)\zeta = -B + (A - B)\zeta, \quad (A + B\zeta)\zeta^2 = (B - A) - A\zeta$$

показывают, что хотя бы у одного из трех ассоцииро-

ванных чисел $A + B\xi$, $(A + B\xi)\xi$, $(A + B\xi)\xi^2$ коэффициент при ξ четен. Следовательно, умножив в равенстве (11) число $s + t\sqrt{-3}$ на ξ или на ξ^2 (отчего равенство, очевидно, не нарушится), мы всегда сможем добиться, чтобы числа s и t стали целыми.

Тем самым лемма Эйлера полностью доказана, и вместе с ней наконец-то доказана и теорема Ферма для показателя 3.

П р и л о ж е н и е. Об арифметике многочленов

Пусть K — произвольное поле и $K[X]$ — кольцо многочленов от одной переменной над полем K (т. е. с коэффициентами из K). Из элементарной алгебры известно, что для многочленов имеет место алгоритм деления с остатком (с псевдонормой — степенью многочлена). Следовательно, в кольце $K[X]$ выполнена основная теорема арифметики.

При этом единицами кольца $K[X]$ являются, очевидно, лишь многочлены нулевой степени, т. е. отличные от нуля элементы поля K .

Простые элементы кольца $K[X]$ называются обыкновенно *неприводимыми многочленами*. Таким образом, можно сказать, что любой многочлен разлагается в произведение неприводимых многочленов и с точностью до постоянных множителей это разложение единственно.

Более того, являясь евклидовым кольцом, кольцо $K[X]$ является также *кольцом главных идеалов*. Поэтому, в частности, для любых взаимно простых многочленов $f(X)$ и $g(X)$ существуют такие многочлены $u(X)$ и $v(X)$, что

$$f(X)u(X) + g(X)v(X) = 1.$$

Следовательно, ни при одном значении X многочлены $f(X)$ и $g(X)$ не могут одновременно обращаться в нуль. Этим доказано, что *многочлены, имеющие общий корень, не взаимно просты*.

Поскольку неприводимый многочлен взаимно прост с каждым многочленом меньшей степени, отсюда, в частности, вытекает, что *никакой корень неприводимого многочлена не может быть корнем многочлена меньшей степени*.

§ 5. Поле K_l и кольцо D_l

Единственный известный к настоящему времени общий метод доказательства теоремы Ферма для любых простых $l \geq 3$ (к сожалению, увенчивающийся успехом не для всех l) восходит, как уже говорилось, к Куммеру и основывается на дальнейшем развитии и обобщении идей Эйлера. Естественно, что основную роль в нем играет некое поле K_l , аналогичное полю K_3 . Поэтому мы начнем с описания и изучения этого поля.

Рассмотрим многочлен

$$(1) \quad X^l - 1$$

или, лучше, многочлен

$$(2) \quad \varphi(X) = X^{l-1} + X^{l-2} + \dots + X + 1,$$

получающийся из многочлена (1) делением на $X - 1$. Корни многочлена (1) выражаются формулой

$$(3) \quad \cos \frac{2\pi k}{l} + i \sin \frac{2\pi k}{l},$$

где $k = 0, 1, \dots, l-1$. На плоскости комплексных чисел эти корни изображаются вершинами правильного l -угольника, вписанного в единичную окружность. На этом основании многочлен (1), а также многочлен (2), называется *многочленом деления круга на l частей*.

Следующее предложение объясняет, почему многочлену (1) мы предпочитаем многочлен $\varphi(X)$.

Предложение 1. *Многочлен $\varphi(X)$ неприводим (над полем \mathbb{Q} рациональных чисел).*

Мы предположим доказательству этого предложения две леммы.

Для любого многочлена

$$F(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n$$

с целыми коэффициентами мы будем символом $[F]$ обозначать наибольший общий делитель его коэффициентов:

$$[F] = \text{НОД}(a_0, a_1, \dots, a_n).$$

Лемма 1 (лемма Гаусса). Для любых двух многочленов с целыми коэффициентами

$$F(X) = a_0X^n + a_1X^{n-1} + \dots + a_n$$

и

$$G(X) = b_0X^m + b_1X^{m-1} + \dots + b_m$$

имеет место равенство

$$[FG] = [F] \cdot [G].$$

Доказательство. Достаточно для любого простого числа p доказать, что если $[F]$ делится на p^a , но не делится на p^{a+1} , а $[G]$ делится на p^b , но не делится на p^{b+1} , то $[FG]$ делится на p^{a+b} , но не делится на p^{a+b+1} . Мы сначала докажем это утверждение при $a = 0$ и $b = 0$, т. е. докажем, что если простое число p не делит чисел $[F]$ и $[G]$, то оно не делит и число $[FG]$.

Если p не делит $[F]$, то существуют коэффициенты a_i многочлена $F[X]$, не делящиеся на p .

Пусть a_{i_0} — обладающий этим свойством коэффициент с наименьшим индексом, т. е. такой, что коэффициент a_{i_0} не делится на p , но (при $i_0 > 0$) все коэффициенты a_0, \dots, a_{i_0-1} делятся на p . Аналогично, если p не делит $[G]$, то существует такой не делящийся на p коэффициент b_{j_0} многочлена $G(X)$, что (при $j_0 > 0$) все коэффициенты b_0, \dots, b_{j_0-1} делятся на p .

По правилу умножения многочленов коэффициент

$$FG = c_0X^{n+m} + c_1X^{n+m-1} + \dots + c_{n+m}$$

выражаются формулой

$$c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0, \quad k = 0, 1, \dots, n+m$$

(мы условно считаем, что $a_i = 0$ при $i > n$ и $b_j = 0$ при $j > m$). При $k = i_0 + j_0$ эта формула содержит слагаемое $a_{i_0}b_{j_0}$, не делящееся на p , а все остальные слагаемые a_ib_j будут делиться на p (ибо либо $i < i_0$, либо $j < j_0$). Поэтому коэффициент $c_{i_0+j_0}$ не делится на p и, значит, $[FG]$ также не делится на p .

Пусть теперь a и b произвольны. Рассмотрим многочлены $\frac{1}{p^a}F$ и $\frac{1}{p^b}G$. По условию числа

$$\left[\frac{1}{p^a} F \right] = \frac{1}{p^a} [F] \quad \text{и} \quad \left[\frac{1}{p^b} G \right] = \frac{1}{p^b} [G]$$

не делятся на p . Следовательно, по доказанному число

$$\frac{1}{p^{a+b}} [FG] = \left[\frac{1}{p^a} F \cdot \frac{1}{p^b} G \right]$$

также не делится на p . Таким образом, число $[FG]$, делясь на p^{a+b} , не делится на p^{a+b+1} . ■

С л е д с т в и е. Если многочлен $H(X)$ с целыми коэффициентами приводим над полем \mathbb{Q} , то существуют такие многочлены $F(X)$ и $G(X)$ положительных степеней с целыми коэффициентами, что

$$(4) \quad H(X) = F(X) G(X).$$

Д о к а з а т е л ь с т в о. По условию разложение (4) имеет место для многочленов $F(X)$ и $G(X)$ с рациональными коэффициентами. Умножив эти многочлены на наименьший общий знаменатель их коэффициентов, мы из разложения (4) получим разложение вида

$$d \cdot H(X) = F_1(X) G_1(X),$$

где d — некоторое целое положительное число, а $F_1(X)$ и $G_1(X)$ — такие многочлены с целыми коэффициентами, что $[F_1] = 1$ и $[G_1] = 1$. Но тогда по лемме 1

$$d \cdot [H] = [d \cdot H] = [F_1] \cdot [G_1] = 1,$$

что возможно только при $d = 1$. ■

Это следствие также часто называется леммой Гаусса.

Л е м м а 2 (к р и т е р и й Э й з е н ш т е й н а). Если существует такое простое число p , что в многочлене

$$(5) \quad H(X) = c_0 X^N + c_1 X^{N-1} + \dots + c_N$$

с целыми коэффициентами:

- i) коэффициент c_0 не делится на p ;
- ii) все коэффициенты c_1, \dots, c_N делятся на p ;
- iii) коэффициент c_N не делится на p^2 ,

то многочлен $H(X)$ неприводим (над полем \mathbb{Q}).

Д о к а з а т е л ь с т в о. Пусть, вопреки утверждению,

$$H(X) = F(X) G(X),$$

где

$$F(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n,$$

$$G(X) = b_0 X^m + b_1 X^{m-1} + \dots + b_m$$

— некоторые многочлены положительных степеней. При этом, согласно доказанному выше следствию, мы, без ограничения общности, можем все коэффициенты многочленов $F(X)$ и $G(X)$ считать целыми числами.

Пусть i_0 и j_0 — наибольшие индексы такие, что коэффициенты a_{i_0} и b_{j_0} не делятся на p . Так как $c_0 = a_0 b_0$ и потому ни a_0 , ни b_0 не делятся на p , то такие индексы существуют. При этом, так как $c_n = a_n b_m$ делится на p , то либо $i_0 < n$, либо $j_0 < m$, а так как c_n не делится на p^2 , то либо $i_0 = n$, либо $j_0 = m$.

Пусть для определенности $j_0 = m$, и потому $i_0 < n$. Тогда в формуле

$$c_{i_0+m} = a_{i_0} b_m + a_{i_0+1} b_{m-1} + \dots + a_n b_{m-n+i_0}$$

для коэффициента c_{i_0+m} первое слагаемое $a_{i_0} b_m$ не будет делиться на p , а все остальные слагаемые будут (ибо по условию все коэффициенты a_i при $i > i_0$ делятся на p). Следовательно, вопреки предположению, коэффициент c_{i_0+m} многочлена $H(X)$ не делится на p . ■

Доказательство предложения 1. Сделав в многочлене $\varphi(X)$ замену $X = Y + 1$, мы получим многочлен

$$\begin{aligned} \varphi(Y+1) &= \frac{(Y+1)^l - 1}{Y} = \\ &= Y^{l-1} + \binom{l}{1} Y^{l-2} + \dots + \binom{l}{l-1}, \end{aligned}$$

приводимый или неприводимый одновременно с многочленом $\varphi(X)$. Но, согласно свойству делимости биномиальных коэффициентов (см. стр. 26), все коэффициенты многочлена $\varphi(Y+1)$ делятся на простое число l , а свободный член

$$\binom{l}{l-1} = l$$

на l^2 не делится. Следовательно, по критерию Эйзенштейна многочлен $\varphi(Y+1)$, а значит и многочлен $\varphi(X)$, неприводим. ■

Пусть теперь ξ — произвольный фиксированный корень многочлена (2). Для определенности можно считать, что

$$(6) \quad \xi = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l},$$

но на самом деле этот выбор не имеет никакого значения (при l простом!) и в дальнейшем не используется. Достаточно знать, что ξ представляет собой комплексное число, удовлетворяющее соотношению

$$(7) \quad \xi^{l-1} = -1 - \xi - \dots - \xi^{l-2},$$

равносильному утверждению, что ξ является корнем многочлена (2). Только этим его свойством мы и будем пользоваться.

По аналогии со случаем $l = 3$ мы введем в рассмотрение множество K_l всевозможных чисел вида

$$(8) \quad \alpha = a_0 + a_1\xi + \dots + a_{l-2}\xi^{l-2},$$

где a_0, a_1, \dots, a_{l-2} — произвольные рациональные числа.

Легко видеть, что представление каждого числа $\alpha \in K_l$ в виде (8) единственно.

Действительно, если это не так, то будет иметь место равенство вида

$$a_0 + a_1\xi + \dots + a_{l-2}\xi^{l-2} = 0,$$

где не все числа a_0, a_1, \dots, a_{l-2} отличны от нуля. Другими словами, число ξ будет корнем некоторого многочлена с рациональными коэффициентами степени, меньшей $l - 1$, что невозможно, ибо многочлен (2) неприводим.

Так как, согласно (7), имеет место равенство

$$1 = -\xi - \xi^2 - \dots - \xi^{l-1},$$

то любой элемент $\alpha \in K_l$ может быть (очевидно, единственным образом) представлен в виде

$$(9) \quad \alpha = b_1\xi + b_2\xi^2 + \dots + b_{l-1}\xi^{l-1},$$

где b_1, b_2, \dots, b_{l-1} — рациональные числа (целые, если числа a_0, \dots, a_{l-2} были целыми).

Такое представление иногда бывает полезно.

Для записи числа (8) удобно ввести в рассмотрение многочлен

$$a(X) = a_0 + a_1X + \dots + a_{l-2}X^{l-2}.$$

Тогда формула (8) приобретет вид

$$(10) \quad \alpha = a(\xi).$$

В таком же виде можно, конечно, записать и формулу (9). Отличие будет состоять в том, что многочлен $a(X)$ будет тогда иметь степень $l-1$, а его свободный член будет равен нулю (т. е. будет иметь место равенство $a(0) = 0$).

Вообще, для любого многочлена $a(X)$ с рациональными коэффициентами число $a(\xi)$ принадлежит K_l , ибо любую степень ξ^k числа ξ с $k \geq l-1$ можно представить в виде (8), воспользовавшись несколько раз соотношением (7). При этом равенство

$$(11) \quad a(\xi) = b(\xi)$$

имеет место тогда и только тогда, когда многочлен $b(X) - a(X)$ делится на многочлен $\varphi(X)$, т. е. когда

$$(12) \quad b(X) = a(X) + \varphi(X)F(X),$$

где $F(X)$ — некоторый многочлен. Действительно, равенство (11) означает, что многочлен $b(X) - a(X)$ имеет корень ξ и потому не взаимно прост с многочленом $\varphi(X)$. Но в силу неприводимости многочлена $\varphi(X)$ это возможно только тогда, когда $b(X) - a(X)$ делится на $\varphi(X)$. ■

Заметим, что, как непосредственно следует из леммы Гаусса, если в соотношении (12) коэффициенты многочленов $a(X)$ и $b(X)$ целые, то коэффициенты многочлена $F(X)$ также целые. ■

Теперь ясно, что сумма и произведение любых двух чисел из K_l также лежит в K_l (если $\alpha = a(\xi)$ и $\beta = b(\xi)$, то $\alpha + \beta = c(\xi)$ и $\alpha\beta = d(\xi)$, где соответственно $c(X) = a(X) + b(X)$ и $d(X) = a(X)b(X)$), т. е. что K_l является кольцом. Более того, легко видеть, что K_l является полем, т. е. для любого отличного от нуля элемента $\alpha \in K_l$ число α^{-1} также лежит в K_l . Действительно, так как $\alpha \neq 0$, то в представлении $\alpha = a(\xi)$ многочлен $a(X)$ не делится на многочлен $\varphi(X)$, и, значит (поскольку многочлен $\varphi(X)$ неприводим), существуют такие многочлены $u(X)$ и $v(X)$, что

$$a(X)u(X) + \varphi(X)v(X) = 1.$$

Полагая здесь $X = \xi$ и учитывая равенство $\varphi(\xi) = 0$, мы немедленно получим, что

$$\alpha^{-1} = u(\xi) \in K. \quad \blacksquare$$

Обратим внимание, что при $l = 3$ мы тот факт, что K_l является полем, доказывали на основе совсем дру-

Корень ξ является лишь одним из $l - 1$ различных корней

многочлена (2). Оказывается, что все эти корни очень просто выражаются через корень ξ .

$$(14) \quad \xi^{(1)} = \xi, \quad \xi^{(2)} = \xi^2, \quad \xi^{(3)} = \xi^3, \quad \dots, \quad \xi^{(l-1)} = \xi^{l-1}.$$

Часто бывает удобна другая нумерация корней (13) многочлена $\varphi(X)$. Чтобы ввести эту нумерацию, мы напомним, что, согласно малой теореме Ферма, для любого целого числа g имеет место сравнение $g^{l-1} \equiv 1 \pmod{l}$. Если же $g^k \not\equiv 1 \pmod{l}$ при $1 \leq k \leq l-2$, то число g называется *первообразным корнем по модулю l* . В этом случае числа g_k , $0 \leq k \leq l-2$, определенные условиями $0 < g_k < l$ и $g_k \equiv g^k \pmod{l}$, все различные и потому совпадают с числами $1, \dots, l-1$, но в другом порядке. Поэтому для любого фиксированного первообразного корня g числа

являются корнями (13) многочлена $\varphi(X)$.

$$\sigma\alpha = a(\zeta^g).$$

60

тельно, любой другой многочлен $b(X)$, для которого $b(\xi) = \alpha$ имеет вид (12), и потому $b(\xi^g) = a(\xi^g)$, так как $\varphi(\xi^g) = 0$. ■

Пользуясь отображением σ мы можем формулы (15) записать и в следующем виде:

$$(16) \quad \xi^{(1)} = \xi, \quad \xi^{(2)} = \sigma\xi, \quad \dots, \quad \xi^{(l-1)} = \sigma^{l-2}\xi.$$

Ясно, что отображение $\sigma: K_l \rightarrow K_l$ биективно. Кроме того, оно сумму переводит в сумму, а произведение — в произведение, т. е. является *автоморфизмом* поля K_l . При этом $(l-1)$ -кратная композиция σ^{l-1} этого автоморфизма является тождественным автоморфизмом (оставляющим все элементы поля K_l на месте. В соответствии с общепринятой практикой мы будем этот факт записывать формулой

$$\sigma^{l-1} = 1.$$

Заметим, что $l-1$ *автоморфизмов*

$$(17) \quad \sigma^0 = 1, \sigma, \sigma^2, \dots, \sigma^{l-2}$$

поля K_l различны (ибо различны $l-1$ корней (16)).

Задача. Покажите, что любой автоморфизм поля K_l является одним из автоморфизмов (17).

Пусть $m = \frac{l-1}{2}$. Тогда $(g^m)^2 = g^{l-1} \equiv 1 \pmod{l}$, и потому $g^m \equiv -1 \pmod{l}$. Следовательно, $\sigma^m \xi = \xi^{-1} = \bar{\xi}$ и, значит,

$$(18) \quad \sigma^m \alpha = \bar{\alpha}$$

для любого $\alpha \in K_l$. Поэтому

$$\sigma^{m+k} \alpha = \overline{\sigma^k \alpha} \quad \text{для любого } k = 0, 1, \dots, m-1.$$

Кроме того, мы видим, что

$$(19) \quad |\alpha|^2 = \alpha \cdot \sigma^m \alpha,$$

откуда, в частности, следует, что если $|\alpha| = 1$, то $|\sigma^k \alpha| = 1$ для любого $k = 1, \dots, l-1$. Действительно,

$$\begin{aligned} |\sigma^k \alpha|^2 &= \sigma^k \alpha \cdot \sigma^{m+k} \alpha = \\ &= \sigma^k (\alpha \cdot \sigma^m \alpha) = \sigma^k (|\alpha|^2) = \sigma^k (1) = 1. \quad \blacksquare \end{aligned}$$

Поскольку числа $\xi, \sigma\xi, \dots, \sigma^{l-2}\xi$ с точностью до порядка совпадают с числами $\xi, \xi^2, \dots, \xi^{l-1}$, мы вместо (9) можем писать

$$(20) \quad \alpha = c_0\xi + c_1\sigma\xi + \dots + c_{l-2}\sigma^{l-2}\xi,$$

где c_0, c_1, \dots, c_{l-2} — те же коэффициенты b_0, b_1, \dots, b_{l-2} , но в другом порядке. Это представление чисел $\alpha \in K_l$ также, конечно, единственно.

Ясно, что автоморфизм σ (а потому и все автоморфизмы (17)) оставляет на месте каждое рациональное число, т. е. $\sigma a = a$ для любого $a \in \mathbb{Q}$. Обратно, если $\sigma\alpha = \alpha$, $\alpha \in K_l$, то в формуле (20) должны иметь место равенства

$$c_0 = c_1 = \dots = c_{l-2}.$$

Поэтому

$$\begin{aligned} \alpha &= c_0(\xi + \sigma\xi + \dots + \sigma^{l-2}\xi) = \\ &= c_0(\xi^{(1)} + \xi^{(2)} + \dots + \xi^{(l-1)}) = -c_0 \in \mathbb{Z}, \end{aligned}$$

ибо по формулам Вьета сумма $\xi^{(1)} + \xi^{(2)} + \dots + \xi^{(l-1)}$ корней многочлена (2) равна взятому с обратным знаком коэффициенту при X^{l-2} , т. е. равна -1 .

Таким образом, $\sigma\alpha = \alpha$ тогда и только тогда, когда $\alpha \in \mathbb{Q}$. ■

Для любого многочлена

$$a(X) = a_0 + a_1X + \dots + a_nX^n$$

и любого элемента $\alpha \in K_l$ мы положим

$$(21) \quad a(\sigma)\alpha = a_0\alpha + a_1\sigma\alpha + \dots + a_n\sigma^n\alpha.$$

В этих обозначениях формулу (20) мы можем записать в следующем виде:

$$(22) \quad \alpha = c(\sigma)\xi,$$

$$\text{где } c(X) = c_0 + c_1(X) + \dots + c_{l-2}X^{l-2}.$$

В то время как запись (22) (или, что равносильно, запись (20)) является лишь иной формой записи (9), аналогичное преобразование записи (8) невозможно.

Определенное формулой (21) отображение $a(\sigma): K_l \rightarrow K_l$ (вообще говоря, не биективное) обладает, очевидно, тем свойством, что

$$a(\sigma)(\alpha + \beta) = a(\sigma)\alpha + a(\sigma)\beta, \quad \alpha, \beta \in K_l,$$

т. е. по отношению к сложению оно является гомоморфизмом. Если $\alpha \in \mathbb{Z}$, то, как нетрудно видеть,

$$(23) \quad a(\sigma)\alpha = a(1)\alpha, \quad \alpha \in \mathbb{Z},$$

откуда, в частности, следует, что равенство $a(\sigma)(\alpha\beta) = a(\sigma)\alpha \cdot a(\sigma)\beta$ может иметь место для всех $\alpha, \beta \in K_l$ только тогда, когда $a(1) = 0$ или 1, так что, вообще говоря, отображение $a(\sigma)$ гомоморфизмом по отношению к умножению не является.

Вместе с тем автоматическая проверка показывает, что

$$\begin{aligned} (a(\sigma) + b(\sigma))\alpha &= a(\sigma)\alpha + b(\sigma)\alpha, \\ (a(\sigma)b(\sigma))\alpha &= a(\sigma)(b(\sigma)\alpha) \end{aligned}$$

для любых многочленов $a(X), b(X)$ и любого элемента $\alpha \in K_l$. Кроме того, легко видеть, что $b(\sigma) = a(\sigma)$ тогда и только тогда, когда многочлен $b(X) - a(X)$ делится на $X^{l-1} - 1$, т. е. когда

$$(24) \quad b(X) - a(X) = (X^{l-1} - 1)F(X).$$

Действительно, если соотношение (24) выполнено, то ввиду тождества $\sigma^{l-1} = 1$ для любого элемента $\alpha \in K_l$ будет иметь место равенство

$$(b(\sigma) - a(\sigma))\alpha = (\sigma^{l-1} - 1)(F(\sigma)\alpha) = 0.$$

Обратно, пусть $b(\sigma)\alpha = a(\sigma)\alpha$ для любого $\alpha \in K_l$. Разделив с остатком многочлен $b(X) - a(X)$ на многочлен $X^{l-1} - 1$, т. е. найдя такие многочлены $F(X)$ и $r(X)$, что

$$b(X) - a(X) = (X^{l-1} - 1)F(X) + r(X),$$

где степень многочлена $r(X)$ не превосходит $l-2$, мы для любого $\alpha \in K_l$ получим, что

$$\begin{aligned} r(\sigma)\alpha &= (b(\sigma) - a(\sigma) - (\sigma^{l-1} - 1)F(\sigma))\alpha = \\ &= b(\sigma)\alpha - a(\sigma)\alpha = 0. \end{aligned}$$

В частности, $r(\sigma)\xi = 0$, что в силу единственности представления (22) возможно только при $r(X) = 0$. \square

Отсюда, в частности, следует, что $a(\sigma) = b(\sigma)$ тогда и только тогда, когда $a(\sigma)\xi = b(\sigma)\xi$.

Внимательный читатель должен заметить во всем сказанном выше существенный пробел, состоящий в

том, что факт существования первообразного корня g требует доказательства. Мы проведем это доказательство, пользуясь простейшими понятиями и теоремами теории групп. Чтобы получить «прямое» доказательство, достаточно все рассуждения провести не в общем теоретико-групповом виде, а применительно к конкретной группе $(\mathbb{Z}/l)^*$.

Известно, что если элемент a группы имеет порядок m , то для любого k , взаимно простого с m , элемент a^k также имеет порядок m . Действительно, поскольку $(a^k)^m = a^{km} = (a^m)^k = 1$, порядок m' элемента a^k делит m . Пусть $m = m't$, где $t \geq 1$. Так как t и k взаимно просты, то t и k также взаимно просты, и потому существуют такие целые числа u и v , что $tu + kv = 1$ и, значит, $m' = m'tu + m'kv = tu + m'kv$. Следовательно,

$$a^{m'} = (a^m)^u ((a^k)^{m'})^v = 1,$$

и, значит, m делит m' . Таким образом, $m' = m$. ■

Отсюда следует, что если a и b — элементы абелевой группы A взаимно простых порядков m и n , то их произведение ab имеет порядок mn . Действительно, так как $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n \cdot (b^n)^m = 1$, то порядок r элемента ab делит mn . Если $r \neq mn$, то r делит либо $m'n$, либо mn' , где m' и n' — некоторые собственные делители чисел m и n соответственно. В первом случае $(a^n)^{m'} = a^{m'n}b^{m'n} = (ab)^{m'n} = 1$, что невозможно, ибо по доказанному порядок элемента a^n равен m , а во втором случае, аналогично $(b^m)^{n'} = 1$, что также невозможно. Следовательно, $r = mn$. ■

Напомним, что экспонентой конечной абелевой группы A называется наибольший из порядков ее элементов. Таким образом, если m_0 — экспонента группы A , то существует элемент $a_0 \in A$ порядка m_0 и порядок m любого элемента $a \in A$ не превосходит m_0 . Легко видеть, что на самом деле порядок m делит экспоненту m_0 . Действительно, если m не делит m_0 , то существует такое простое число p и такой показатель $r \geq 1$, что p^r делит m , но не делит m_0 . Пусть $m_0 = p^s m_1$, где $0 \leq s < r$, а m_1 не делится на p . Тогда элемент $a^{m'p^r}$ имеет порядок p^r , а элемент $a_0^{p^s}$ — порядок m_1 , взаимно простой с p^r . Поэтому по доказанному выше элемент $a^{m/p^r} a_0^{p^s}$ имеет порядок $p^r m_1$, что невозможно, так как $p^r m_1 > p^s m_1 = m_0$. ■

В частности, этим доказано, что

$$(25) \quad a^{m_0} = 1 \quad \text{для любого элемента } a \in A.$$

Если группа A циклична (т. е. исчерпывается степенями некоторого элемента a — ее образующей), то ее экспонента m_0 совпадает, очевидно, с ее порядком n . Обратно, если $m_0 = n$, то степени элемента a порядка m_0 исчерпывают всю группу (их m_0 различных), и потому эта группа циклична. Поскольку всегда $m_0 \leq n$, мы получаем, таким образом, что если $m_0 \geq n$, то группа A циклична. ■

Но именно это неравенство имеет место, если A является группой всех отличных от нуля элементов произвольного конеч-

ного поля. Действительно, равенство (25) в этом случае утверждает, что все элементы группы A , т. е. все отличные от нуля элементы поля, являются корнями многочлена $X^m - 1$, который таким образом, имеет по меньшей мере m_0 корней. Поскольку же число корней уравнения над произвольным полем не может превышать его степени, то $n \leq m_0$.

Тем самым доказано, что группа по умножению всех отличных от нуля элементов конечного поля циклическа. ■

Таким образом, в частности, циклической группой является группа $(\mathbb{Z}/l)^*$.

Поскольку утверждение, что число g является первообразным корнем по модулю l в точности равносильно утверждению, что класс этого числа по модулю l служит образующей группы $(\mathbb{Z}/l)^*$, существование первообразных корней по модулю l тем самым полностью доказано. ■

Подставив в (8) вместо $\xi = \xi^{(1)}$ произвольный корень $\xi^{(k)}$, $k = 1, \dots, l-1$, многочлена $\Phi(X)$, мы получим некоторое число

$$\alpha^{(k)} = a(\xi^{(k)}) = a_0 + a_1 \xi^{(k)} + \dots + a_{l-2} (\xi^{(k)})^{l-2},$$

также лежащее в поле K_l . (Например, если $\xi^{(k)} = \xi^{g^k} = \sigma^k \xi$ — см. формулы (15) и (16), — то $\alpha^{(k)}$ есть не что иное, как $\sigma^k \alpha$. Однако мы не будем сейчас связывать себя определенной нумерацией корней $\xi^{(k)}$.)

Предложение 2. Для любого $\alpha \in K_l$ число

$$N\alpha = \alpha^{(1)} \alpha^{(2)} \dots \alpha^{(l-1)}$$

лежит в поле \mathbb{Q} (является рациональным числом).

Докажем предварительно следующую общую лемму:

Лемма 3. Пусть β_1, \dots, β_n — корни некоторого многочлена $\Phi(X)$ с целыми рациональными коэффициентами, и пусть $p(X)$ — произвольный многочлен с рациональными коэффициентами. Тогда число

$$(26) \quad p(\beta_1) \dots p(\beta_n)$$

является рациональным числом.

Если старший коэффициент многочлена $\Phi(X)$ равен единице, а все коэффициенты многочлена $p(X)$ являются целыми числами, то произведение (26) также является целым числом.

Доказательство. Рассмотрим многочлен

$$(27) \quad F(X_1, \dots, X_n) = p(X_1) \dots p(X_n)$$

от n переменных X_1, \dots, X_n . Он, очевидно, не меняется при любой перестановке этих переменных, т. е.

является *симметрическим* многочленом от X_1, \dots, X_n . Но известно (см., например, книгу: Болтянский В. Г., Виленик Н. Я. Симметрия в алгебре. — М.: Наука, 1967), что любой симметрический многочлен $F(X_1, \dots, X_n)$ может быть представлен в виде многочлена от так называемых *элементарных симметрических* многочленов

$$(28) \quad \begin{array}{rcl} \sigma_1 & = & X_1 + \dots + X_n, \\ & \cdot & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ & \cdot & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ \sigma_n & = & X_1 \dots X_n, \end{array}$$

т. е., иными словами, существует такой многочлен $G(Y_1, \dots, Y_n)$ (кстати сказать, единственный), что имеет место тождество

$$(29) \quad F(X_1, \dots, X_n) = G(\sigma_1, \dots, \sigma_n).$$

При этом коэффициенты многочлена $G(Y_1, \dots, Y_n)$ выражаются посредством действий сложения, вычитания и умножения через коэффициенты многочлена $F(X_1, \dots, X_n)$ и, значит, — в нашем случае — через коэффициенты многочлена $p(X)$, т. е. являются рациональными числами (целыми, если коэффициенты многочлена $p(X)$ были целыми числами).

С другой стороны, согласно так называемым формулам Вьета, значения

$$\begin{aligned}\sigma_1^{(0)} &= \sigma_1(\beta_1, \dots, \beta_n) = \beta_1 + \dots + \beta_n, \\&\vdots \\ \sigma_n^{(0)} &= \sigma_n(\beta_1, \dots, \beta_n) = \beta_1 \dots \beta_n\end{aligned}$$

симметрических многочленов (28) при $X_1 = \beta_1, \dots, X_n = \beta_n$, где β_1, \dots, β_n — корни многочлена

$$\Phi(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n,$$

выражаются формулами

$$\sigma_1^{(0)} = -\frac{a_1}{a_0}, \dots, \sigma_n^{(0)} = (-1)^n \frac{a_n}{a_0}.$$

Поэтому после подстановки $X_1 = \beta_1, \dots, X_n = \beta_n$ мы из (29) получим равенство

$$F(\beta_1, \dots, \beta_n) = G\left(-\frac{a_1}{a_0}, \dots, (-1)^n \frac{a_n}{a_0}\right),$$

доказывающее, очевидно, лемму. ■

Ясно, что утверждение этой леммы останется верным, если произведение (26) мы заменим произвольным симметрическим многочленом от $p(\beta_1), \dots, p(\beta_n)$.

Доказательство предложения 2. Достаточно применить лемму 3 к многочлену $p(X) = a(X)$ и корням $\zeta^{(1)}, \dots, \zeta^{(l-1)}$ многочлена $\varphi(X)$. ■

Согласно сделанному выше замечанию утверждение предложения 2 останется справедливым, если произведение $N\alpha$ мы заменим любым симметрическим многочленом от $\alpha^{(1)}, \dots, \alpha^{(l-1)}$, скажем, элементарным. В силу формул Вьета это доказывает, что для любого элемента $\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2} \in K_l$ коэффициенты многочлена $(x - \alpha^{(1)}) \dots (x - \alpha^{(l-1)})$ являются рациональными числами (целыми, если все числа a_0, a_1, \dots, a_{l-2} целые):

Рациональное число $N\alpha$ называется *нормой* элемента $\alpha \in K_l$. Оно обладает следующими свойствами:

1) $N\alpha \geq 0$, причем $N\alpha = 0$ тогда и только тогда, когда $\alpha = 0$;

2) для любых чисел $\alpha, \beta \in K_l$ имеет место равенство

$$(30) \quad N(\alpha\beta) = N\alpha \cdot N\beta;$$

3) если число $\alpha \in K_l$ рационально (т. е. $a_1 = \dots = a_{l-2} = 0$ и, значит, $\alpha = a_0$), то

$$N\alpha = \alpha^{l-1}.$$

Эти свойства очевидны (ср. со случаем $l = 3$), за исключением, возможно, неравенства $N\alpha \geq 0$, для доказательства которого надо вспомнить, что числа (13) (являясь невещественными корнями уравнения с вещественными коэффициентами) попарно комплексно сопряжены. (Например, можно считать, что $\zeta^{(l-k)} = \overline{\zeta^{(k)}}$.) Поэтому числа $\alpha^{(1)}, \dots, \alpha^{(l-1)}$ также попарно комплексно сопряжены (скажем, $\alpha^{(l-k)} = \overline{\alpha^{(k)}}$) и, значит, $N\alpha \geq 0$ (при указанной нумерации корней имеет место формула $N\alpha = |\alpha^{(1)}|^2 \dots |\alpha^{(m)}|^2$, где $m = \frac{l-1}{2}$).

С помощью нормы доказательство того, что K_l является полем, сводится к тривиальной выкладке:

$$\frac{\beta}{\alpha} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{\alpha^{(1)}\alpha^{(2)} \dots \alpha^{(l-1)}} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{N\alpha} \in K_l,$$

аналогичной соответствующей выкладке при $l = 3$.

Число (8) поля K_l называется *целым*, если все коэффициенты a_0, a_1, \dots, a_{l-2} являются целыми рациональными числами (принадлежат кольцу \mathbb{Z}). Как уже

отмечалось, норма $N\alpha$ целого числа α является (неотрицательным) целым рациональным числом. Все целые числа поля K_l составляют, очевидно, кольцо. Мы будем обозначать это кольцо символом D_l .

Число поля K_l , представленное в виде (22), тогда и только тогда принадлежит кольцу D_l , когда все коэффициенты многочлена $c(X)$ являются целыми числами. Кроме того, для любого многочлена $a(X)$ с целыми коэффициентами отображение $a(\sigma)$ переводит D_l в D_l и потому может рассматриваться как отображение кольца D_l в себя.

Оно, вообще говоря, не биективно и является гомоморфизмом только по отношению к сложению. Однако в частном случае, когда $a(X) = X^k$, каждое отображение вида σ^k , т. е. каждый автоморфизм (17), рассматриваемое как отображение $D_l \rightarrow D_l$, представляет собой автоморфизм кольца D_l .

Так же, как и в случае $l = 3$, число $\alpha \in D_l$ тогда и только тогда является единицей кольца D_l , когда $N\alpha = 1$.

Действительно, если $\alpha\alpha^{-1} = 1$, то $N\alpha \cdot N\alpha^{-1} = 1$ и потому $N\alpha = 1$. Обратно, если $N\alpha = 1$, то $\alpha\alpha^{-1} = 1$, где $\alpha^{-1} = \alpha^{(2)} \dots \alpha^{(l-1)}$. ■

Отсюда (и из (30)) следует, что функция $\alpha \mapsto N\alpha$ является (на D_l^*) строгой псевдонормой. Поэтому (см. § 4, предложение 1) в кольце D_l любой не являющийся единицей элемент разлагается в произведение простых элементов.

Однако, как показывают примеры, кольцо D_l , вообще говоря, не является кольцом с однозначным разложением на множители.

Например, можно показать, что кольцо D_{23} не будет кольцом с однозначным разложением на множители. Напротив, в кольцах D_l с $l < 23$ разложение на множители однозначно.

Задача. Изучите кольцо D_5 . Найдите его единицы. Покажите, что кольцо D_5 евклидово и потому является кольцом с однозначным разложением на множители.

Аналогичное исследование колец D_l при $5 < l < 23$ является уже очень трудной задачей.

Переносим на случай кольца D_l обозначения Гаусса (см. § 1), мы будем писать

$$(31) \quad \alpha = \beta \bmod \gamma,$$

где $\alpha, \beta, \gamma \in D_l$, если разность $\alpha - \beta$ делится в кольце

D_l на γ . Так же как и для целых рациональных чисел, эти сравнения в отношении действий сложения и умножения ведут себя как обыкновенные равенства (их можно складывать, перемножать, и, в частности, возводить в степень с натуральным показателем).

Особо интересен случай, когда в сравнении (31) число γ является целым рациональным числом $t \in \mathbb{Z}$. Пусть

$$\begin{aligned}\alpha &= a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}, \\ \beta &= b_0 + b_1\zeta + \dots + b_{l-2}\zeta^{l-2}.\end{aligned}$$

Предложение 3. Сравнение $\alpha \equiv \beta \pmod{t}$ имеет место тогда и только тогда, когда $a_i \equiv b_i \pmod{t}$ для любого $i = 0, 1, \dots, l-2$.

Доказательство. Сравнение $\alpha \equiv \beta \pmod{t}$ означает, что $\alpha - \beta = t\delta$, где $\delta = d_0 + d_1\zeta + \dots + d_{l-2}\zeta^{l-2}$ — некоторый элемент кольца D_l . С другой стороны, в силу единственности представления чисел из D_l в виде (8) равенство $\alpha - \beta = t\delta$ равносильно равенствам $a_0 - b_0 = td_0$, $a_1 - b_1 = td_1$, ..., $a_{l-2} - b_{l-2} = td_{l-2}$, т. е. сравнениям $a_0 \equiv b_0 \pmod{t}$, $a_1 \equiv b_1 \pmod{t}$, ..., $a_{l-2} \equiv b_{l-2} \pmod{t}$. ■

В частности, мы видим, что число $\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}$ тогда и только тогда делится в кольце D_l на целое рациональное число t , когда коэффициенты a_0, a_1, \dots, a_{l-2} делятся на t (в кольце \mathbb{Z}).

Предложение 4. Для любого числа $\alpha \in D_l$ существует такое целое рациональное число $c_0 \in \mathbb{Z}$, что

$$(32) \quad \alpha^l = c_0 \pmod{l}.$$

Доказательство. Пусть $\alpha = a(\zeta)$. Тогда по формуле Шенемана (см. формулу (11) § 1)

$$\alpha^l = a(\zeta^l) \pmod{l}$$

и, значит, $\alpha^l \equiv a(1) \pmod{l}$. ■

В дальнейшем важную роль будет играть число

$$\lambda = 1 - \zeta.$$

Предложение 5. Число λ является простым элементом кольца D_l . Его норма равна l :

$$(33) \quad N\lambda = l.$$

Его $(l-1)$ -я степень λ^{l-1} ассоциирована с числом l , т. е. существует такая единица $\varepsilon \in D_l$, что

$$(34) \quad l = \varepsilon \lambda^{l-1}.$$

Кроме того, для любого числа $\alpha \in D_l$ существует такое целое рациональное число b_0 , что

$$(35) \quad \alpha \equiv b_0 \pmod{\lambda}.$$

Наконец, если целое рациональное число $a \in \mathbb{Z}$ делится (в кольце D_l) на λ , то оно делится (в кольце \mathbb{Z}) на l .

Доказательство. Так как числа $\zeta, \zeta^2, \dots, \zeta^{l-1}$ являются корнями многочлена $\varphi(X)$, то

$$\varphi(X) = (X - \zeta)(X - \zeta^2) \dots (X - \zeta^{l-1}),$$

и потому

$$(36) \quad l = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{l-1}),$$

ибо $\varphi(1) = l$. Но так как $\zeta^k = \zeta^{(k)}$, $k = 1, \dots, l-1$, (см. формулу (14)), и $1 - \zeta = \lambda$, то $1 - \zeta^k = \lambda^{(k)}$. Это доказывает, что $l = \lambda^{(1)}\lambda^{(2)} \dots \lambda^{(l-1)}$, т. е. что $l = N\lambda$.

Если теперь $\lambda = \alpha\beta$, то $N\lambda = N\alpha \cdot N\beta$, т. е. $N\alpha \cdot N\beta = l$. Поэтому либо $N\alpha = 1$, либо $N\beta = 1$, т. е. одно из чисел α и β является единицей. Следовательно, число λ неразложимо в кольце D_l (является простым элементом).

Кроме того, если $a = \lambda\alpha$, где $a \in \mathbb{Z}$ и $\alpha \in D_l$, то, переходя к нормам, мы получим, что $a^{l-1} = l \cdot N\alpha$ и, следовательно, что a делится на l .

Поскольку автоморфизм $\alpha \mapsto \alpha^{(k)}$ переводит $\lambda = 1 - \zeta$ в $\lambda^{(k)} = 1 - \zeta^{(k)} = 1 - \zeta^k$, числа λ и $\lambda^{(k)}$ имеют одну и ту же норму. Значит, $N(1 - \zeta^k) = l$.

Другое доказательство:

$$N(1 - \zeta^k) = \prod_{s=1}^{l-1} (1 - \zeta^{sk}) = \prod_{s=1}^{l-1} (1 - \zeta^s) = N(1 - \zeta) = l,$$

ибо числа $k, 2k, \dots, (l-1)k$ с точностью до порядка и слагаемых, кратных l , совпадают с числами $1, 2, \dots, l-1$.

Но

$$1 - \zeta^k = (1 - \zeta)\varepsilon_k,$$

где

$$\varepsilon_k = 1 + \zeta + \dots + \zeta^{k-1},$$

и потому

$$N(1 - \zeta^k) = N(1 - \zeta) N(\varepsilon_k).$$

Следовательно, $N\varepsilon_k = 1$, и, значит, ε_k является *единицей*. Этим доказано, что для любого $k = 1, \dots, l-1$ число $1 - \zeta^k$ ассоциировано с числом $1 - \zeta = \lambda$. Поэтому (34) вытекает из (36).

Пусть, наконец, $\alpha = a(\zeta)$ — произвольный элемент кольца D_l . Так как $\zeta = 1 - \lambda$, то $\alpha = b(\lambda)$, где $b(X) \equiv a(1 - X)$, и потому

$$\alpha \equiv b(0) \pmod{\lambda}.$$

Этим все утверждения предложения 5 доказаны. ■

Обратим внимание, что, как мы показали при доказательстве последнего утверждения предложения 5, любой элемент $\alpha \in D_l$ допускает представление вида $\alpha = b(\lambda)$, т. е. вида

$$(37) \quad \alpha = b_0 + b_1\lambda + \dots + b_{l-2}\lambda^{l-2}.$$

§ 6. Единицы кольца D_l

Мы изложим в этом параграфе простейшие сведения о единицах кольца D_l , использующиеся в доказательстве Куммера теоремы Ферма для регулярных простых чисел.

Во второй половине параграфа на число l будут наложены некоторые дополнительные условия. В §§ 13—15 будет показано, что на самом деле эти условия равносильны условию регулярности.

В первую очередь мы найдем все элементы кольца D_l , являющиеся корнями из единицы. Примером такого элемента служит число ζ , являющееся, по построению, корнем из единицы степени l . Другой пример доставляет нам число $-\zeta$, являющееся, очевидно, корнем из единицы степени $2l$. Всевозможные степени числа $-\zeta$ (имеющие, как легко показать, вид $\pm \zeta^a$, где $a = 0, 1, \dots, l-1$) также являются корнями из единицы степени $2l$ (и, очевидно, исчерпывают все такие корни). Оказывается, что это все корни из единицы, содержащиеся в кольце D_l .

Предложение 1. Любой корень из единицы, содержащийся в кольце D_l , является корнем степени $2l$ и, значит, может быть представлен в виде

$$(1) \quad \pm \zeta^a, \quad a = 0, 1, \dots, l-1.$$

Доказательство. Нам надо показать, что если в кольце D_l имеет место равенство $\alpha^N = 1$ с целым положительным показателем N , причем $\alpha^{N_1} \neq 1$ ни для одного положительного $N_1 < N$, то N делит $2l$, т. е. не делится ни на l^2 , ни на 4, ни на одно простое число $p \neq l$.

Пусть $N = l^2 n$. Рассмотрим число $\beta = \alpha^n$. Как мы знаем (см. предложение 4 § 5), существует такое целое рациональное число c_0 , что

$$\beta^l \equiv c_0 \pmod{l}.$$

С другой стороны, ясно, что $\beta^l \neq 1$, но $(\beta^l)^l = 1$, т. е. β^l является отличным от 1 корнем степени l из единицы. Но все такие корни содержатся, по построению, в D_l и имеют вид ζ^a , где $0 < a \leq l-1$. Этим доказано, что $\beta^l = \zeta^a$ при некотором a , $0 < a \leq l-1$.

Таким образом, мы видим, что в кольце D^l имеет место сравнение вида

$$\zeta^a \equiv c_0 \pmod{l},$$

где $0 < a \leq l-1$ и $c_0 \in \mathbb{Z}$, означающее, что число $\zeta^a - c_0$ делится на l в кольце D_l . Поскольку в силу предложения 3 § 5 это невозможно, то, следовательно, N не делится на l^2 .

Пусть $N = 4n$ или $N = pn$, где p — простое нечетное число, отличное от l . Снова рассмотрим число $\beta = \alpha^n$. Ясно, что $\beta = \pm i$ при $N = 4n$, т. е. $\beta^2 = -1$, и $\beta^p = 1$ при $N = pn$. В обоих случаях

$$\beta^p \equiv 1 \pmod{p},$$

где $p = 2$ при $N = 4n$.

С другой стороны, согласно формуле (11) § 1 (примененной к $l = p$ и $a(X) = b(X)$), если $\beta = b(\zeta)$, то $\beta^p \equiv b(\zeta^p) \pmod{p}$. Следовательно,

$$b(\zeta^p) \equiv 1 \pmod{p}.$$

Но поскольку $p \not\equiv 0 \pmod{l}$, существует такой показатель k , что $p \equiv g^k \pmod{l}$, где g , как и в § 5, фиксированный первообразный корень по модулю l . Это озна-

чает, что $\zeta^p = \zeta^{\sigma^k} = \sigma^k \zeta$, и потому $b(\zeta^p) = \sigma^k b(\zeta) = \sigma^k \beta$. Тем самым доказано, что

$$\sigma^k \beta \equiv 1 \pmod{p},$$

т. е., что $\sigma^k \beta - 1 = p\alpha$, где $\alpha \in D_l$. Но тогда $\beta - 1 = \sigma^{-k}(\sigma^k \beta - 1) = \sigma^{-k}(p\alpha) = p(\sigma^{-k}\alpha)$ и, следовательно,

$$\beta \equiv 1 \pmod{p}.$$

Это означает, что элемент β может быть представлен в виде $\beta = 1 + p^k \gamma$, где $k \geq 1$ и $\gamma \in D_l$ не делится на p . Отсюда, пользуясь формулой бинома Ньютона и учитывая, что $2k + 1 \geq k + 2$ при $k \geq 1$, мы немедленно получаем, что

$$\beta^p \equiv 1 + p^{k+1} \gamma \pmod{p^{k+2}}.$$

Если теперь $p > 2$ (т. е. мы имеем дело со случаем $N = pn$), то $\beta^p = 1$ и, следовательно,

$$p^{k+1} \gamma \equiv 0 \pmod{p^{k+2}},$$

т. е. $\gamma \equiv 0 \pmod{p}$, что противоречит выбору γ . Таким образом, предположение, что N делится на p , приводит к противоречию.

Если же $p = 2$ (т. е. мы имеем дело со случаем $N = 4n$), то $\beta^p = -1$ и, следовательно,

$$0 \equiv 2 + 2^{k+1} \gamma \pmod{2^{k+2}}, \quad \text{т. е.} \quad 2^k \gamma \equiv 1 \pmod{2^{k+1}},$$

что явно невозможно. Таким образом, N не может делиться и на 4. ■

З а м е ч а н и е. В формулировке предложения 1 слова «в кольце D_l » можно заменить словами «в поле K_l », ибо можно показать, что любой корень из единицы, содержащийся в поле K_l , автоматически будет принадлежать кольцу D_l (см. ниже § 12). В дальнейшем это замечание использоваться не будет.

Каждый корень из единицы $\alpha \in D_l$ обладает, очевидно, тем свойством, что $|\alpha| = 1$. Оказывается, что верно и обратное:

П р е д л о ж е н и е 2. Если для числа $\alpha \in D_l$ имеет место равенство

$$(2) \quad |\alpha| = 1,$$

то α является корнем из единицы.

Д о к а з а т е л ь с т в о. Пусть A_l — множество всех чисел $\alpha \in D_l$, удовлетворяющих условию (2).

Для произвольного числа $\alpha \in A_l$ рассмотрим многочлен

$$(3) \quad (X - \alpha^{(1)}) \dots (X - \alpha^{(l-1)}) = \\ = X^{l-1} + c_1 X^{l-2} + \dots + c_{l-1},$$

корнем которого является число $\alpha = \alpha^{(1)}$. Ясно, что абсолютная величина $|c_k|$ каждого коэффициента c_k , $k = 1, \dots, l-1$, этого многочлена не превосходит соответствующего коэффициента многочлена

$$(4) \quad (X + |\alpha^{(1)}|) \dots (X + |\alpha^{(l-1)}|).$$

С другой стороны, как было показано в § 5, из (2) вытекает, что $|\alpha^{(k)}| = 1$ для любого $k = 1, \dots, l-1$. Следовательно, многочлен (4) имеет вид $(X + 1)^{l-1}$. Этим доказано, что

$$(5) \quad |c_k| \leq \binom{l-1}{k}, \quad k = 1, \dots, l-1.$$

Но (см. § 5) мы знаем, что для любого числа $\alpha \in D_l$ многочлен (3) имеет целые коэффициенты. Поскольку целых чисел c_k , удовлетворяющих неравенствам (5) существует (при данном l) только конечное число, этим доказано, что множество многочленов вида (3) (для всевозможных $\alpha \in A_l$) конечно. Так как конечное число многочленов данной степени имеет только конечное число корней и так как любой элемент $\alpha \in A_l$ является корнем соответствующего многочлена (3), отсюда вытекает, что множество A_l конечно.

С другой стороны, ясно, что если $\alpha \in A_l$, то $\alpha^n \in A_l$ для каждого $n \in \mathbb{Z}$. Поэтому, ввиду конечности A_l , для любого $\alpha \in A_l$ существуют такие различные показатели m и n , что $\alpha^m = \alpha^n$. Но тогда $\alpha^{n-m} = 1$, т. е. α является корнем из единицы. ■

Несмотря на то, что все корни многочлена (2) из § 5 являются комплексными (невещественными) числами, в поле K_l (и в кольце D_l) имеется достаточно много вещественных чисел.

В частности, оказывается, что единицами вида ξ^a и вещественными единицами исчерпываются, по существу, все единицы кольца D_l .

Предложение 3. Любая единица кольца D_l имеет вид

$$\zeta^a \varepsilon_0,$$

где ε_0 — вещественная единица.

Доказательство. Пусть

$$\varepsilon = a_0 + a_1 \zeta + \dots + a_{l-2} \zeta^{l-2}$$

— произвольная единица кольца D_l . Так как $\bar{\zeta} = \zeta^{-1} = \zeta^{l-1}$, то комплексно сопряженное число

$$\bar{\varepsilon} = a_0 + a_1 \bar{\zeta} + \dots + a_{l-2} \bar{\zeta}^{l-2}$$

лежит в D_l и является, очевидно, единицей. Поэтому единицей будет и число

$$\mu = \frac{\bar{\varepsilon}}{\varepsilon} \in D_l.$$

Эта единица обладает, очевидно, тем свойством, что $|\mu| = 1$. Следовательно, согласно предложению 2, она является корнем из единицы. Поскольку, согласно предложению 1, любой корень из единицы имеет вид $\pm \zeta^c$, тем самым доказано, что существует такое целое число $c \geq 0$, что

$$\bar{\varepsilon} = \pm \zeta^c \varepsilon.$$

Согласно предложению 5 § 5 существует такое целое рациональное число b_0 , что

$$\varepsilon \equiv b_0 \pmod{\lambda}.$$

При этом, так как $\bar{\lambda} \equiv 0 \pmod{\lambda}$, то также

$$\bar{\varepsilon} \equiv b_0 \pmod{\lambda}.$$

Поэтому, если

$$\bar{\varepsilon} = -\zeta^c \varepsilon,$$

то

$$b_0 \equiv -b_0 \pmod{\lambda},$$

ибо $\zeta \equiv 1 \pmod{\lambda}$. Следовательно,

$$2b_0 \equiv 0 \pmod{\lambda},$$

т. е. $2b_0$ делится на λ . Но мы знаем (предложение 5 § 5), что если целое рациональное число делится в кольце D_l на λ , то оно делится и на l . Следовательно, $2b_0$, а значит, и b_0 делится на l . В частности, b_0 делится на λ и, значит, ε делится на λ , что невозможно (ибо $N\varepsilon = 1$ не делится на $N\lambda = l$).

Полученное противоречие показывает, что $\bar{\varepsilon} = \zeta^c \varepsilon$.
Мы положим

$$\varepsilon_0 = \zeta^{-mc} \varepsilon, \quad \text{где} \quad m = \frac{l-1}{2}.$$

Тогда

$$\varepsilon = \zeta^a \varepsilon_0, \quad \text{где} \quad a = mc,$$

причем (напомним, что $\bar{\zeta} = \zeta^{-1}$)

$$\bar{\varepsilon}_0 = \bar{\zeta}^{-mc} \bar{\varepsilon} = \zeta^{mc} \zeta^c \varepsilon = \zeta^{(m+1)c} \varepsilon = \zeta^{-mc} \varepsilon = \varepsilon_0,$$

так что единица ε_0 вещественна. ■

Для исследования первого случая теоремы Ферма методом Эйлера — Куммера, к которому мы перейдем в следующем параграфе, нам достаточно предложения 3. Однако для более трудного второго случая нам понадобятся также еще критерий того, что некоторая единица ε кольца D_l является l -й степенью η' другой единицы η .

Согласно предложению 4 § 5, для того чтобы единица ε была l -й степенью некоторой другой единицы, необходимо, чтобы $\varepsilon \equiv e \pmod{l}$ для некоторого целого $e \in \mathbb{Z}$.

Является ли это условие достаточным? Мы дадим ответ на этот вопрос лишь в некоторых частных случаях, вполне достаточных, однако, для наших целей.

Мы будем постоянно пользоваться отображением $\sigma: D_l \rightarrow D_l$, построенным в § 5. Напомним, что это отображение зависит от выбора некоторого первообразного корня g по модулю l и на ζ действует по формуле $\sigma\zeta = \zeta^g$. Нам будет удобно выбор этого корня несколько специализировать.

По малой теореме Ферма $g^{l-1} \equiv 1 \pmod{l}$, т. е. $g^{l-1} = 1 + al$, где $a \in \mathbb{Z}$. Оказывается, что *существует первообразный корень g по модулю l , для которого число a не делится на l , т. е. такой, что*

$$(6) \quad g^{l-1} \not\equiv 1 \pmod{l^2}.$$

Действительно, пусть g — произвольный первообразный корень по модулю l , и пусть $g^{l-1} = 1 + al$. Если a не делится на l , то g удовлетворяет условию (6). Пусть a делится на l . Рассмотрим число $g + l$,

также являющееся первообразным корнем по модулю l . По формуле бинোма Ньютона

$$\begin{aligned}(g+l)^{l-1} &\equiv g^{l-1} + (l-1)g^{l-2}l \equiv \\ &\equiv g^{l-1} - g^{l-2}l \equiv 1 + l(a - g^{l-2}) \pmod{l^2}.\end{aligned}$$

Поскольку $a - g^{l-2}$ не делится, очевидно, на l , корень $g+l$ удовлетворяет условию (6). ■

В дальнейшем мы всегда будем предполагать, что первообразный корень g удовлетворяет условию (6).

Заметим, что если (6) выполнено, то $g^m + 1 \not\equiv 0 \pmod{l^2}$, где, как всегда, $m = \frac{l-1}{2}$. Действительно, $g^{l-1} - 1 = (g^m + 1)(g^m - 1)$, и потому, если $g^{l-1} - 1$ не делится на l^2 , то $g^m + 1$ также не делится на l^2 . ■

Введем в рассмотрение многочлен

$$\omega(X) = 1 + X + X^2 + \dots + X^{l-2},$$

аналогичный многочлену деления круга

$$\varphi(X) = 1 + X + X^2 + \dots + X^{l-1}.$$

(Предупреждение: многочлен $\omega(X)$ не является неприводимым многочленом деления круга на $l-1$ частей.)

Имеет место формула

$$\begin{aligned}(7) \quad \omega(g^k) &= 1 + g^k + \dots + g^{(l-2)k} = \\ &= \begin{cases} -1 \pmod{l}, & \text{если } k \equiv 0 \pmod{l-1}, \\ 0 \pmod{l}, & \text{если } k \not\equiv 0 \pmod{l-1}. \end{cases}\end{aligned}$$

Действительно, если $k \equiv 0 \pmod{l-1}$, то $g^k \equiv 1 \pmod{l}$, и потому

$$\begin{aligned}\omega(g^k) &= 1 + g^k + (g^k)^2 + \dots + (g^k)^{l-2} \equiv \\ &\equiv l - 1 \equiv -1 \pmod{l}.\end{aligned}$$

Если же $k \not\equiv 0 \pmod{l-1}$, то $g^k - 1 \not\equiv 0 \pmod{l}$, и потому сравнение

$$\begin{aligned}(g^k - 1)(1 + (g^k)^2 + \dots + (g^k)^{l-2}) &\equiv \\ &\equiv g^{(l-1)k} - 1 \equiv 0 \pmod{l}\end{aligned}$$

можно сократить на $g^k - 1$. ■

Пусть теперь x_0, x_1, \dots, x_{l-2} и y_0, y_1, \dots, y_{l-2} — произвольные целые числа. Предположим, что либо

$$(8) \quad y_k \equiv \sum_{j=0}^{l-2} g^{jk} x_j \equiv x_0 + g^k x_1 + \dots + g^{(l-2)k} x_{l-2} \pmod{l}$$

для любого $k = 0, 1, \dots, l-2$, либо

$$(9) \quad x_j \equiv - \sum_{k=0}^{l-2} g^{-lk} y_k \equiv \\ \equiv -(y_0 + g^{-l} y_1 + \dots + g^{-(l-2)} y_{l-2}) \pmod{l}$$

для любого $j = 0, 1, \dots, l-2$, где g^{-1} обозначает число g^{l-2} (обладающее тем свойством, что $gg^{l-2} \equiv 1 \pmod{l}$).

Лемма 1. Если выполнено (8), то выполнено (9), и наоборот.

Доказательство. Согласно формуле (7)

$$\sum_{k=0}^{l-2} g^{-lk} y_k \equiv \sum_{k=0}^{l-2} \sum_{r=0}^{l-2} g^{(r-l)k} x_r \equiv \sum_{r=0}^{l-2} \omega(g^{r-l}) x_r \equiv -x_l \pmod{l}$$

и

$$\sum_{j=0}^{l-2} g^{jk} x_j \equiv - \sum_{j=0}^{l-2} \sum_{r=0}^{l-2} g^{(k-r)l} y_r \equiv - \sum_{r=0}^{l-2} \omega(g^{k-r}) y_r \equiv \\ \equiv y_k \pmod{l}. \quad \blacksquare$$

Аналогичные формулы имеют место и для квадрата g^2 первообразного корня g . Действительно, легко видеть, что

$$(7') \quad \sum_{j=0}^{m-1} g^{2kj} = 1 + g^{2k} + \dots + g^{2(m-1)k} \equiv \\ \equiv \begin{cases} m \pmod{l}, & \text{если } k \equiv 0 \pmod{m}, \\ 0 \pmod{l}, & \text{если } k \not\equiv 0 \pmod{m}, \end{cases}$$

где, как всегда, $m = \frac{l-1}{2}$. В самом деле, так как

$$\omega(X) = (1+X)(1+X^2 + \dots + X^{2(m-1)}),$$

то

$$\omega(g^k) = (1+g^k)(1+g^{2k} + \dots + g^{2(m-1)k}).$$

Следовательно, если $k \not\equiv 0 \pmod{m}$ и потому $g^k + 1 \not\equiv 0 \pmod{l}$ и $k \not\equiv 0 \pmod{l-1}$, то $1 + g^{2k} + \dots + g^{2(m-1)k} \equiv 0 \pmod{l}$. Если же $k \equiv 0 \pmod{m}$, то $g^{2k} \equiv 1 \pmod{l}$ и $1 + g^{2k} + \dots + g^{2(m-1)k} \equiv m \pmod{l}$. \blacksquare

Пусть теперь x_0, \dots, x_{m-1} и y_0, \dots, y_{m-1} — произвольные целые числа, и пусть либо

$$(8') \quad y_k \equiv \sum_{j=0}^{m-1} g^{2jk} x_j \pmod{l}$$

для любого $k = 0, \dots, m-1$, либо

$$(9') \quad x_j \equiv -2 \sum_{k=0}^{m-1} g^{-2jk} y_k \pmod{l}$$

для любого $j = 0, \dots, m-1$.

Лемма 2. Если выполнено (8'), то выполнено (9'), и наоборот.

Доказательство. Согласно формуле (7')

$$-2 \sum_{k=0}^{m-1} g^{-2jk} y_k \equiv -2 \sum_{k=0}^{m-1} \sum_{r=0}^{m-1} g^{2(r-j)k} x_r \equiv \\ \equiv -2mx_j \equiv x_j \pmod{l}$$

И

$$\begin{aligned} \sum_{j=0}^{m-1} g^{2jk} x_j &\equiv -2 \sum_{j=0}^{m-1} \sum_{r=0}^{m-1} g^{2(k-r)j} y_r \equiv \\ &\equiv -2my_k \equiv y_k \pmod{l}. \end{aligned}$$

Следствие. Если

$$\sum_{j=0}^{m-1} g^{2jk} x_j \equiv 0 \pmod{l}$$

для всех $k = 0, 1, \dots, m-1$, то $x_j \equiv 0 \pmod{l}$ для всех $j = 0, 1, \dots, m-1$. ■

Вернемся теперь к кольцу D_t .

Пусть

$$\xi_k = \omega(g^k \sigma) \xi = \sum_{i=0}^{l-2} g^{ik} \sigma^i \xi, \quad k = 0, 1, \dots, l-2,$$

т. е. пусть

$$(10) \quad \begin{aligned} \zeta_0 &= \zeta + \sigma\zeta + \dots + \sigma^{l-2}\zeta, \\ \zeta_1 &= \zeta + g\sigma\zeta + \dots + g^{l-2}\sigma^{l-2}\zeta, \\ &\vdots \\ \zeta_{l-2} &= \zeta + g^{l-2}\sigma\zeta + \dots + g^{(l-2)^2}\sigma^{l-2}\zeta. \end{aligned}$$

Легко видеть, что

$$(11) \quad \sigma \zeta_k \equiv g^{-k} \zeta_k \pmod{l}$$

для любого $k = 0, 1, \dots, l-2$. Действительно,

$$\begin{aligned} \sigma \sum_{j=0}^{l-2} g^{jk} \sigma^j \zeta &= \sum_{j=1}^{l-1} g^{(j-1)k} \sigma^j \zeta = g^{-k} \sum_{j=1}^{l-1} g^{jk} \sigma^j \zeta = \\ &= g^{-k} \left(\sum_{j=0}^{l-2} g^{jk} \sigma^j \zeta + g^{(l-1)k} \sigma^{l-1} \zeta - \sigma^0 \zeta \right) \equiv \\ &\equiv g^{-k} \zeta_k \pmod{l}, \end{aligned}$$

ибо $g^{(l-1)k} \equiv 1 \pmod{l}$ и $\sigma^{l-1} = \sigma^0$. ■

Предложение 4. Для любого $\alpha \in D_l$ существуют такие однозначно определенные по модулю l целые числа a_0, a_1, \dots, a_{l-2} , что

$$(12) \quad \alpha \equiv a_0 \zeta_0 + a_1 \zeta_1 + \dots + a_{l-2} \zeta_{l-2} \pmod{l}.$$

Доказательство. Пусть

$$\alpha = c_0 \zeta + c_1 \sigma \zeta + \dots + c_{l-2} \sigma^{l-2} \zeta$$

(см. формулу (20) § 5). Тогда, если имеет место (12), то

$$\sum_{j=0}^{l-2} c_j \sigma^j \zeta \equiv \sum_{k=0}^{l-2} a_k \zeta_k \equiv \sum_{k=0}^{l-2} \sum_{j=0}^{l-2} a_k g^{jk} \sigma^j \zeta \pmod{l},$$

и потому

$$(13) \quad c_j \equiv \sum_{k=0}^{l-2} a_k g^{jk} \pmod{l}.$$

Следовательно, согласно лемме 1,

$$(14) \quad a_k \equiv - \sum_{j=0}^{l-2} c_j g^{-jk} \pmod{l}.$$

Таким образом, числа a_0, a_1, \dots, a_{l-2} — если они существуют — однозначно определены по модулю l формулами (14).

Для доказательства их существования достаточно проверить, что числа (14) удовлетворяют соотношению (12). Но это ясно, поскольку, согласно лемме 1, из (14) следует (13), и потому

$$\alpha = \sum_{j=0}^{l-2} c_j \sigma^j \zeta \equiv \sum_{j=0}^{l-2} \sum_{k=0}^{l-2} a_k g^{jk} \sigma^j \zeta \equiv \sum_{k=0}^{l-2} a_k \zeta_k \pmod{l}. \quad \blacksquare$$

Другое доказательство (использующее простейшие факты линейной алгебры). Множество классов чисел кольца D_l по модулю l является $l-1$ -мерным линейным пространством над полем \mathbb{Z}/l с базисом, состоящим из классов чисел $\xi, \sigma\xi, \dots, \sigma^{l-2}\xi$. Утверждение леммы 1 состоит в том, что классы чисел $\xi_0, \xi_1, \dots, \xi_{l-2}$ также составляют базис. Поэтому для доказательства этой леммы достаточно показать, что определитель линейных выражений (10) отличен от нуля (в поле \mathbb{Z}/l). Но это действительно так, поскольку этот определитель представляет собой определитель Вандермонда различных (по модулю l) чисел $1, g, \dots, g^{l-2}$. ■

Следствие. Если хотя бы для одного $k = 0, 1, \dots, l-2$ имеет место сравнение

$$a\xi_k \equiv 0 \pmod{l}, \quad \text{где } a \in \mathbb{Z},$$

то $a \equiv 0 \pmod{l}$. ■

Как и в § 5, мы для каждого $k = 0, 1, \dots, l-2$ введем в рассмотрение число g_k , удовлетворяющее неравенствам $0 < g_k < l$ и такое, что

$$g^k \equiv g_k \pmod{l}.$$

Заметим, что, вообще говоря, $g_1 \neq g$, поскольку мы не предполагаем, что $0 < g < l$. Вместе с тем, конечно, $g_0 = 1$.

Числа g_0, g_1, \dots, g_{l-2} совпадают с точностью до порядка с числами $1, 2, \dots, l-1$ и

$$\sigma^k \xi = \xi^{g_k}.$$

Мы положим

$$\bar{\omega}(X) = 1 + g_1 X + \dots + g_{l-2} X^{l-2}.$$

Таким образом,

$$\bar{\omega}(X) \equiv \omega(gX) \pmod{l}$$

и, значит,

$$\bar{\omega}(X)(gX - 1) \equiv X^{l-1} - 1 \pmod{l},$$

ибо $\omega(X)(X - 1) = X^{l-1} - 1$ и $g^{l-1} \equiv 1 \pmod{l}$. Иными словами,

$$(15) \quad \bar{\omega}(X)(gX - 1) = X^{l-1} - 1 + l\psi(X),$$

где $\psi(X)$ — некоторый многочлен (как легко видеть, без свободного члена, т. е. такой, что $\psi(0) = 0$).

В явном виде многочлен $\psi(X)$ выражается формулой

$$\psi(X) = \sum_{k=1}^{l-1} \frac{g g_{l-k-1} - g_{l-k}}{l} X^{l-k}$$

(условно полагаем, что $g_{l-1} = 1$). Однако это выражение нам не понадобится.

Легко видеть, что

$$(16) \quad \psi(g^{l-2}) \not\equiv 0 \pmod{l}.$$

Действительно, по определению

$$l\psi(X) = \varpi(X)(gX - 1) - (X^{l-1} - 1)$$

и, следовательно,

$$l\psi(g^{l-2}) = \varpi(g^{l-2})(g^{l-1} - 1) - [(g^{l-2})^{l-1} - 1].$$

Так как

$$(g^{l-2})^{l-1} - 1 = (1 + al)^{l-2} - 1 \equiv (l-2)al \equiv -2al \pmod{l^2},$$

где $al = g^{l-1} - 1$, отсюда вытекает (после сокращения на l), что

$$\psi(g^{l-2}) \equiv \varpi(g^{l-2})a + 2a \pmod{l}.$$

Но, согласно формуле (7),

$$\varpi(g^{l-2}) \equiv \omega(g^{l-1}) \equiv -1 \pmod{l}.$$

Поэтому

$$\psi(g^{l-2}) \equiv a \pmod{l}.$$

Поскольку, согласно условию (6), число a не делится на l , это доказывает (16). ■

Заметим, что условие (6) далее мы нигде использовать не будем. Оно нам нужно только для доказательства соотношения (16).

Числа $\psi(g^k)$ при $k < l-2 = 2m-1$ вполне могут делиться на l . Впрочем, нас будут интересовать только нечетные показатели $k = 1, 3, \dots, 2m-3$. Мы назовем число l *куммеровым*, если числа $\psi(g)$, $\psi(g^3)$, \dots , $\psi(g^{2m-3})$ не делятся на l , или, что в силу (16) равносильно, если произведение

$$(17) \quad \psi(g)\psi(g^3)\dots\psi(g^{2m-3})\psi(g^{2m-1})$$

не делится на l .

Подставив в многочлены $\varphi(X)$ и $\bar{\omega}(X)$ вместо X оператор σ , мы получим отображения $\varphi(\sigma)$, $\bar{\omega}(\sigma): D_l \rightarrow D_l$. Поскольку $\sigma^{l-1} = 1$, из формулы (15) следует, что

$$(18) \quad \bar{\omega}(\sigma)(g\sigma - 1) = l\varphi(\sigma).$$

Пусть

$$\varphi'(X) = 1 + 2X + \dots + (l-1)X^{l-2}$$

— производная многочлена деления круга $\varphi(X)$. Так как числа $g_0 = 1, g_1, \dots, g_{l-2}$ с точностью до порядка совпадают с числами $1, 2, \dots, l-1$, то

$$\begin{aligned} X\varphi'(X) &= X + 2X^2 + \dots + (l-1)X^{l-1} = \\ &= X + g_1X^{g_1} + \dots + g_{l-2}X^{g_{l-2}}. \end{aligned}$$

Но по определению $\sigma^k \zeta = \zeta^{g_k}$ и, значит,

$$\begin{aligned} \zeta + g_1\zeta^{g_1} + \dots + g_{l-2}\zeta^{g_{l-2}} &= \\ &= (1 + g_1\sigma + \dots + g_{l-2}\sigma^{l-2})\zeta = \bar{\omega}(\sigma)\zeta. \end{aligned}$$

Этим доказано, что

$$\bar{\omega}(\sigma)\zeta = \zeta\varphi'(\zeta).$$

С другой стороны, дифференцируя тождество

$$(X-1)\varphi(X) = X^l - 1,$$

мы получим тождество

$$\varphi(X) + (X-1)\varphi'(X) = lX^{l-1},$$

откуда следует, что $(\zeta-1)\varphi'(\zeta) = l\zeta^{l-1}$, т. е. что

$$(19) \quad \zeta\varphi'(\zeta) = \frac{l}{\zeta-1}.$$

Таким образом,

$$(20) \quad \bar{\omega}(\sigma)\zeta = \frac{l}{\zeta-1}.$$

Применив σ^m , где, как всегда, $m = \frac{l-1}{2}$, и учитывая (см. формулу (18) § 5), что $\sigma^m \zeta = \bar{\zeta} = \zeta^{-1}$, мы получим отсюда соотношение

$$\sigma^m \bar{\omega}(\sigma)\zeta = \frac{l}{\zeta^{-1}-1} = \frac{l\zeta}{1-\zeta}.$$

Следовательно,

$$(21) \quad \frac{\xi}{1-\xi} = \frac{1}{l} \sigma^m \varpi(\sigma) \xi$$

и, значит, (см. формулу (18)),

$$(22) \quad (g\sigma - 1) \left(\frac{\xi}{1-\xi} \right) = \sigma^m \psi(\sigma) \xi.$$

Теперь мы уже можем вернуться к исследованию единиц кольца D_l .

Так как каждое число вида $\sigma^k \xi$ имеет вид ξ^a для некоторого a (а именно, для $a = g_k$), то число $1 - \sigma^k \xi$ ассоциировано с числом $1 - \xi = \lambda$. Поэтому для любых целых чисел n_1, \dots, n_m , для которых

$$n = n_1 + \dots + n_m \geq 0,$$

и любого $a = 0, 1, \dots, l-1$ число

$$(23) \quad \pm \xi^a (1 - \sigma_\xi^{n_1})^{n_1} \dots (1 - \sigma_\xi^{n_m})^{n_m}$$

лежит в D_l и ассоциировано с числом λ^n . В частности, если $n = 0$, то число (23) является единицей.

Единицы вида (23) мы будем называть *специальными единицами* кольца D_l . Ясно, что они образуют подгруппу группы всех единиц.

Предложение 5. Если число l куммерово, то любая специальная единица ε , для которой существует такое целое число c , что $\varepsilon \equiv c \pmod{l}$, является l -й степенью некоторой, тоже специальной, единицы η .

Доказательство. По определению $\varepsilon = e(\xi)$, где

$$e(X) = \pm X^a (1 - X^{g_1})^{n_1} \dots (1 - X^{g_m})^{n_m}$$

и

$$n_1 + \dots + n_m = 0.$$

Так как $\varepsilon \equiv c \pmod{l}$, то существуют такие многочлены $F_1(X)$ и $F_2(X)$, что

$$e(X) = c + lF_1(X) + \varphi(X)F_2(X).$$

Дифференцируя это тождество и деля на $e(X)$ (т. е. вычисляя логарифмическую производную), мы полу-

чим (после умножения на X) тождество

$$\begin{aligned} a - n_1 \frac{g_1 X^{g_1}}{1 - X^{g_1}} - \dots - n_m \frac{g_m X^{g_m}}{1 - X^{g_m}} &= \\ &= \frac{lX F'_1(X) + X \varphi'(X) F_2(X) + X \varphi(X) F'_2(X)}{e(X)}. \end{aligned}$$

Положим здесь $X = \xi$. Поскольку

$$\frac{\xi^{g_k}}{1 - \xi^{g_k}} = \sigma^k \left(\frac{\xi}{1 - \xi} \right), \quad k = 1, \dots, m,$$

мы, перейдя к сравнениям по модулю l и вводя многочлен

$$E(X) = n_1(gX) + n_2(gX)^2 + \dots + n_m(gX)^m,$$

получим соотношение

$$a - E(\sigma) \left(\frac{\xi}{1 - \xi} \right) \equiv \xi \varphi'(\xi) \cdot \frac{F_2(\xi)}{e} \pmod{l}.$$

Пусть

$$\frac{F_2(\xi)}{e} = b + \lambda \alpha, \quad \text{где } b \in \mathbb{Z}, \alpha \in D_l$$

(см. формулу (35) § 5). Тогда (см. формулы (19) и (20))

$$\begin{aligned} \xi \varphi'(\xi) \cdot \frac{F_2(\xi)}{e} &= \frac{l}{\xi - 1} (b + \lambda \alpha) = b \frac{l}{\xi - 1} - \alpha l = \\ &= b \bar{\omega}(\sigma) \xi - \alpha l \equiv b \bar{\omega}(\sigma) \xi \pmod{l}, \end{aligned}$$

так что

$$a - E(\sigma) \left(\frac{\xi}{1 - \xi} \right) \equiv b \bar{\omega}(\sigma) \xi \pmod{l}.$$

Применив к этому сравнению оператор $g\sigma - 1$ и учтя, что $(g\sigma - 1)a = (g - 1)a$, мы в силу формул (22) и (18) получим сравнение

$$(g - 1)a - E(\sigma) \sigma^m \psi(\sigma) \xi \equiv b l \psi(\sigma) \xi \equiv 0 \pmod{l},$$

т. е. сравнение

$$(24) \quad \sigma^m \psi(\sigma) E(\sigma) \xi \equiv (1 - g)a \pmod{l}.$$

Положив $(1-g)a = d$ и применив σ^{m+k} , мы можем это сравнение переписать в следующем виде:

$$\psi(\sigma)E(\sigma)\sigma^k\zeta \equiv d \bmod l,$$

где $k = 0, 1, \dots, l-2$.

Отсюда непосредственно вытекает, что для произвольного элемента

$$\alpha = a_0\zeta + a_1\sigma\zeta + \dots + a_{l-2}\sigma^{l-2}\zeta = a(\sigma)\zeta$$

кольца D_l имеет место сравнение

$$\psi(\sigma)E(\sigma)\alpha \equiv a(1)d \bmod l.$$

В частности,

$$\psi(\sigma)E(\sigma)\zeta_k \equiv \delta(g^k)d \bmod l,$$

где ζ_k — числа, заданные формулами (10), и значит (см. формулы (7)),

$$\psi(\sigma)E(\sigma)\zeta_k \equiv 0 \bmod l \quad \text{при } k \neq 0.$$

Но из формул (11) следует, что

$$q(\sigma)\zeta_k \equiv q(g^{-k})\zeta_k \bmod l$$

для любого многочлена $q(X)$. Применительно к многочлену $q(X) = \psi(X)E(X)$ мы, следовательно, получаем, что

$$\psi(g^{-k})E(g^{-k})\zeta_k \equiv 0 \bmod l,$$

и, значит (см. следствие из предложения 4), что

$$\psi(g^{-k})E(g^{-k}) \equiv 0 \bmod l$$

для любого $k = 1, \dots, l-2$.

Конечно, в этом сравнении g^{-k} можно заменить на g^{l-1-k} . Положив $j = l-1-k$, мы поэтому получим сравнение

$$\psi(g^j)E(g^j) \equiv 0 \bmod l,$$

имеющее место для любого $j = 1, \dots, l-2$.

Но так как число l по условию куммерово, то $\psi(g^j) \not\equiv 0 \bmod l$ при $j = 1, 3, \dots, l-2$. Поэтому

$$E(g^j) \equiv 0 \bmod l$$

при $j = 1, 3, \dots, l-2$, т. е.

$$\sum_{k=0}^{m-1} n_{k+1}g^{2jk} \equiv 0 \bmod l$$

при $j = 1, 2, \dots, m$ или, что, очевидно, равносильно, при $j = 0, 1, \dots, m-1$.

Применяя следствие из леммы 2, мы получаем отсюда, что для любого $k = 1, 2, \dots, m$ имеет место сравнение $n_k \equiv 0 \pmod{l}$, т. е. что все числа

$$q_1 = \frac{n_1}{l}, \dots, q_m = \frac{n_m}{l}$$

целые. Значит, $E(X) \equiv 0 \pmod{l}$, и потому

$$E(\sigma)\xi \equiv 0 \pmod{l},$$

откуда в силу формулы (24) следует, что $(1-g)a \equiv 0 \pmod{l}$. Поэтому $a \equiv 0 \pmod{l}$, что возможно только при $a = 0$.

Построив по числам q_1, \dots, q_m специальную единицу

$$\eta = \pm (1 - \sigma\xi)^{q_1} \dots (1 - \sigma^m\xi)^{q_m},$$

мы и получим теперь, что $\eta^l = \varepsilon$. ■

Чтобы перейти от специальных единиц к произвольным, мы потребуем выполнения следующего условия:

К. Факторгруппа группы единиц кольца D_l по подгруппе специальных единиц является конечной группой.

Это условие означает, что существует конечное множество единиц $\varepsilon_1, \dots, \varepsilon_n$, обладающих тем свойством, что любая единица ε кольца D_l единственным образом представляется в виде $\varepsilon_i\eta$, где $i = 1, \dots, n$, а η — специальная единица. Число n этих «особых» единиц, т. е. порядок факторгруппы группы единиц по подгруппе специальных единиц мы будем обозначать символом h_2 и будем называть (по причинам, которые выяснятся ниже в своем месте) *вторым множителем*.

Поскольку при возведении любого элемента группы в степень, равную порядку группы, получается единица группы, для любой единицы ε кольца D_l единица ε^{h_2} специальна.

Из теории групп известно (это так называемая теорема Коши), что в каждой конечной группе G для любого простого делителя l ее порядка существует элемент порядка l . Для случая абелевой группы G (только этот случай нам и нужен) эта теорема без труда доказывается индукцией по порядку n группы G .

Действительно, пусть x — произвольный (отличный от единицы) элемент группы G , и пусть m — его порядок. Если l делит m , то доказывать нечего (элементом порядка l будет элемент $x^{m/l}$). Пусть l не делит m . Рассмотрим факторгруппу G' группы G по циклической подгруппе G_x порядка m , порожденной элементом x . Порядок n' этой факторгруппы равен n/m и потому делится на l .

По предположению индукции в группе G' существует элемент y' порядка l . Пусть $y \in G$ — произвольный элемент из смежного класса y' . Тогда $y^l \in G_x$, и потому $(y^m)^l = (y^l)^m = 1$. Поэтому остается лишь доказать, что $y^m \neq 1$. Так как l не делит m , то существуют такие целые числа a и b , что $la + mb = 1$. Следовательно, $y = y^{la}y^{mb}$ и, значит, если $y^m = 1$, то $y = y^{la} \in G_x$, что невозможно. Поэтому $y^m \neq 1$. ■

Отсюда вытекает следующее важное предложение:

Предложение 6. Если число l куммерово и выполнено условие К, то $h_2 \not\equiv 0 \pmod{l}$.

Доказательство. Если $h_2 \equiv 0 \pmod{l}$, то, согласно теореме Коши, в факторгруппе группы единиц по подгруппе специальных единиц существует элемент порядка l , и, значит, в группе единиц существует неспециальная единица ϵ , для которой единица ϵ^l специальна. Являясь l -й степенью, единица ϵ^l сравнима по модулю l с некоторым числом $c \in \mathbb{Z}$. Поэтому в силу предложения 5 в кольце D_l существует такая специальная единица η , что $\epsilon^l = \eta^l$. Таким образом, $(\epsilon\eta^{-1})^l = 1$, т. е. $\epsilon\eta^{-1} = \zeta^a$ для некоторого a . Следовательно, вопреки предположению, единица $\epsilon = \zeta^a\eta$ специальна. Полученное противоречие доказывает, что $h_2 \not\equiv 0 \pmod{l}$. ■

Теперь мы уже можем доказать наш основной результат.

Предложение 7 (лемма Куммера). Если число l куммерово и выполнено условие К, то любая единица $\epsilon \in D_l$, сравнимая по модулю l с целым рациональным числом, является l -й степенью некоторой единицы.

Доказательство. Как было выше замечено, единица ϵ^{h_2} специальна. Кроме того, она, очевидно, сравнима по модулю l с некоторым целым рациональным числом (если $\epsilon \equiv c \pmod{l}$, то $\epsilon^{h_2} \equiv c^{h_2} \pmod{l}$). Поэтому, согласно предложению 5, в кольце D_l существует такая специальная единица η , что

$$\epsilon^{h_2} = \eta^l.$$

Согласно предложению 6 числа h_2 и l взаимно просты. Поэтому существуют такие целые числа u и v , что $h_2u + lv = 1$. Но тогда

$$\varepsilon = \varepsilon^{h_2u} \varepsilon^{lv} = \eta^{lu} \varepsilon^{lv} = (\eta^u \varepsilon^v)^l,$$

и предложение 7 доказано. ■

§ 7. Первый случай теоремы Ферма

Чтобы выпукло показать трудности, возникающие при попытках доказать теорему Ферма, мы разобьем доказательство Куммера первого случая теоремы Ферма для регулярных показателей на два этапа. В этом параграфе мы выведем теорему из некоего вспомогательного утверждения, а в следующих параграфах обсудим пути его доказательства.

Вспомогательное утверждение. Если

$$(1) \quad x^l + y^l = z^l, \quad l \geq 3,$$

где x, y, z — взаимно простые целые рациональные числа, не делящиеся на простое число l , то в кольце D_l имеет место равенство

$$(2) \quad x + \xi y = \varepsilon \alpha^l,$$

где $\alpha \in D_l$, а ε — единица кольца D_l .

Ввиду этого утверждения, чтобы в первом случае теоремы Ферма прийти к противоречию, достаточно показать, что равенство (2) в кольце D_l возможно (при выполнении равенства (1)) только тогда, когда хотя бы одно из чисел x, y и z делится на l . При этом мы можем считать, что $l \geq 5$, поскольку при $l = 3$ теорема Ферма нами уже доказана.

Лемма. Если для целых рациональных чисел x и y имеет место равенство (2), где $\alpha \in D_l$, а ε — единица кольца D_l , то при $l \geq 5$ либо x или y делятся на l , либо $x \equiv y \pmod{l}$.

Доказательство. Согласно предложению 4 § 5 существует такое целое рациональное число b_0 , что

$$\alpha^l \equiv b_0 \pmod{l},$$

а согласно предложению 4 § 6, единица ε имеет вид

$$\varepsilon = \zeta^a \varepsilon_0,$$

где ε_0 — вещественная единица. Следовательно, полагая

$$\eta = b_0 \varepsilon_0,$$

мы получим, что

$$x + \xi y \equiv \xi^a \eta \pmod{l},$$

т. е. что

$$(3) \quad \xi^{-a} (x + \xi y) \equiv \eta \pmod{l},$$

где η — вещественное число.

Заметим теперь, что если $\alpha \equiv \beta \pmod{l}$, т. е. $\alpha = \beta + l\gamma$, где $\gamma \in D_l$, то $\bar{\alpha} = \bar{\beta} + l\bar{\gamma}$, где $\bar{\gamma} \in D_l$, и потому $\bar{\alpha} \equiv \bar{\beta} \pmod{l}$. В частности,

$$\overline{\xi^{-a} (x + \xi y)} \equiv \bar{\eta} \pmod{l}.$$

Но $\bar{\eta} = \eta$, а $\bar{\xi} = \xi^{-1}$. Следовательно,

$$\xi^a (x + \xi^{-1} y) \equiv \eta \pmod{l},$$

и, значит,

$$\xi^a (x + \xi^{-1} y) \equiv \xi^{-a} (x + \xi y) \pmod{l},$$

т. е.

$$x\xi^a + y\xi^{a-1} - x\xi^{-a} - y\xi^{1-a} \equiv 0 \pmod{l}.$$

Обозначая символом $\langle k \rangle$ неотрицательный остаток от деления целого числа k на l (вычет числа k), мы можем это соотношение переписать в следующем виде:

$$(4) \quad x\xi^{\langle a \rangle} + y\xi^{\langle a-1 \rangle} - x\xi^{\langle -a \rangle} - y\xi^{\langle 1-a \rangle} \equiv 0 \pmod{l}.$$

Но, согласно предложению 3 § 5, число $a_0 + a_1\xi + \dots + a_{l-2}\xi^{l-2}$ кольца D_l тогда и только тогда делится на l , когда все его коэффициенты a_0, a_1, \dots, a_{l-2} делятся на l . Поэтому, если показатели в (4) все различны и отличны от $l-1$, то сравнение (4) возможно только тогда, когда числа x и y делятся на l . Таким образом, в этом случае все доказано.

Пусть среди показателей в (4) имеется число $l-1$. Это возможно тогда и только тогда, когда

$$\langle a \rangle = 0, 1, 2, l-1,$$

и соответственно

$$\begin{aligned}\langle a-1 \rangle &= l-1, & 0, & & 1, & & l-2, \\ \langle -a \rangle &= 0, & l-1, & l-2, & 1, & & \\ \langle 1-a \rangle &= 1, & 0, & l-1, & 2.\end{aligned}$$

Так как, по условию, $l \geq 5$, то в каждом из этих четырех случаев только один из показателей в (4) равен $l-1$. Член с этим показателем мы должны преобразовать по формуле

$$\xi^{l-1} = -1 - \xi - \dots - \xi^{l-2}.$$

После такого преобразования этот член заменится суммой одночленов $1, \xi, \dots, \xi^{l-2}$ с коэффициентами $\pm x$ или $\pm y$. Так как число $l-1$ этих одночленов не меньше четырех (ибо $l \geq 5$), то при приведении подобных членов хотя бы один из них не сократится с остальными тремя членами левой части сравнения (4). (Например, если $\langle -a \rangle = l-1$, то заведомо останется слагаемое $x\xi$.) Поскольку в результате приведения подобных членов в левой части сравнения (4) получается число кольца D_l , записанное в нормальной форме $a_0 + a_1\xi + \dots + a_{l-2}\xi^{l-2}$, коэффициент при этом оставшемся одночлене должен делиться на l .

Таким образом, и в этом случае либо x , либо y делится на l .

Пусть все показатели в (4) меньше $l-1$, но пусть среди них есть равные. Поскольку равенства $\langle a \rangle = \langle a-1 \rangle$ и $\langle -a \rangle = \langle 1-a \rangle$, очевидно, вообще невозможны (соседние числа не могут давать при делении на l одинаковых остатков), нам следует рассмотреть только четыре случая

$$\begin{aligned}\langle a \rangle &= \langle -a \rangle, & \langle a \rangle &= \langle 1-a \rangle, \\ \langle a-1 \rangle &= \langle 1-a \rangle, & \langle a-1 \rangle &= \langle -a \rangle,\end{aligned}$$

т. е. случаи

$$\begin{aligned}a &\equiv -a \pmod{l}, & a &\equiv 1-a \pmod{l}, \\ a-1 &\equiv 1-a \pmod{l}, & a-1 &\equiv -a \pmod{l}.\end{aligned}$$

В первом случае $2a \equiv 0 \pmod{l}$, т. е. $2a = Al$, где A — целое число (очевидно, четное). Поэтому

$$a-1 = (l-1) + \left(\frac{A}{2} - 1\right)l$$

и, следовательно, $\langle a - 1 \rangle = l - 1$, что, по условию, невозможно.

Аналогично, во втором случае $2a \equiv 2 \pmod{l}$, т. е. $2a = 2 + Al$, где A — целое (очевидно, четное) число. Поэтому

$$-a = (l - 1) - \left(\frac{A}{2} + 1\right)l$$

и, следовательно, мы снова получаем невозможное равенство $\langle -a \rangle = l - 1$.

В третьем же и четвертом случаях $2a \equiv 1 \pmod{l}$, т. е. $2a = 1 + Al$, где A — целое число (очевидно, нечетное).

Поэтому

$$a = \frac{l+1}{2} + \frac{A-1}{2}l$$

и, следовательно, $\langle a \rangle = \frac{l+1}{2}$, а значит,

$$\langle a - 1 \rangle = \langle -a \rangle = \frac{l-1}{2}$$

и

$$\langle 1 - a \rangle = \langle a \rangle = \frac{l+1}{2}.$$

Таким образом, в этих случаях сравнение (4) приобретает вид

$$(5) \quad (x - y)\zeta^{\frac{l+1}{2}} + (y - x)\zeta^{\frac{l-1}{2}} \equiv 0 \pmod{l}.$$

Поскольку левая часть сравнения (5) имеет нормальный вид (показатели $\frac{l+1}{2}$ и $\frac{l-1}{2}$ различны и меньше числа $l-1$), из него следует, что $x - y$ делится на l , т. е. что

$$x \equiv y \pmod{l}.$$

Тем самым лемма полностью доказана. ■

Из этой леммы и Вспомогательного утверждения вытекает, что если

$$(6) \quad x^l + y^l = z^l,$$

где числа x, y, z взаимно просты и не делятся на l , то $x \equiv y \pmod{l}$. Но вместе с равенством (6) имеет место и равенство

$$x^l + (-z)^l = (-y)^l.$$

Поэтому то же рассуждение показывает, что $x \equiv \equiv -z \pmod{l}$.

Следовательно,

$$x + y - z \equiv 3x \pmod{l}.$$

С другой стороны, из равенства (6) в силу малой теоремы Ферма вытекает, что

$$z \equiv x + y \pmod{l}.$$

Следовательно,

$$3x \equiv 0 \pmod{l},$$

что невозможно, поскольку $l > 3$, а x не делится на l .

Итак, предположив, что для не делящихся на l взаимно простых чисел x, y, z имеет место соотношение (6), мы, используя Вспомогательное утверждение, получили противоречие.

Тем самым доказано, что *первый случай теоремы Ферма имеет место для всех l , для которых верно Вспомогательное утверждение.*

Поскольку

$$x^l + y^l = (x + y)(x + \zeta y) \dots (x + \zeta^{l-1}y),$$

равенство

$$(7) \quad x^l + y^l = z^l$$

может быть переписано в следующем виде:

$$(8) \quad (x + y)(x + \zeta y) \dots (x + \zeta^{l-1}y) = z^l.$$

Если

А) все множители в левой части равенства (8) взаимно просты,

Б) в кольце D_l справедлива основная теорема арифметики,

то каждый из множителей в (8) с точностью до ассоциированности будет l -й степенью (ибо, согласно (8), их произведение является l -й степенью). В частности, для первого множителя в кольце D_l найдется такой элемент α и такая единица ε , что

$$x + \zeta y = \varepsilon \alpha^l.$$

Этим доказано Вспомогательное утверждение с точностью, конечно, до двух больших «если». Впрочем, первое «если» легко доказывается:

Предложение 1. Если целые рациональные числа x и y взаимно просты, а их сумма $x + y$ не делится на l , то все числа

$$(9) \quad x + y, x + \xi y, \dots, x + \xi^{l-1} y$$

попарно взаимно просты (в кольце D_l).

Доказательство. Пусть $0 \leq m, n \leq l-1$ и $m \neq n$. Достаточно, очевидно, показать, что в кольце D_l существуют такие элементы α, β , что

$$(10) \quad (x + \xi^m y) \alpha + (x + \xi^n y) \beta = 1.$$

Так как числа x, y по условию взаимно просты, то существуют такие целые числа a и b , что $xa + yb = 1$. Аналогично, так как взаимно просты числа l и $x + y$, то существуют такие целые числа u и v , что $lu + (x + y)v = 1$. Кроме того, поскольку $1 - \xi^{n-m} \sim 1 - \xi$ и $1 - \xi^m \sim 1 - \xi$, существуют такие единицы $\epsilon, \eta \in D_l$, что $\epsilon(1 - \xi^{n-m}) = 1 - \xi$ и $\eta(1 - \xi) = \epsilon(1 - \xi^m)$, а поскольку $l \sim (1 - \xi)^{l-1}$, существует такое число $\gamma \in D_l$, что $\gamma(1 - \xi) = l$.

Непосредственная подстановка в соотношение (10) теперь показывает, что это соотношение выполнено при

$$\begin{aligned} \alpha &= v - (vy\eta + u\gamma\epsilon)(\xi^{n-m}a - \xi^{-m}b), \\ \beta &= (vy\eta + u\gamma\epsilon)(a - \xi^{-m}b). \quad \blacksquare \end{aligned}$$

Предложение 1 немедленно обеспечивает выполнение условия А), так как в равенстве (1) числа x и y , по условию, взаимно просты, а число z , в силу малой теоремы Ферма сравнимое по модулю l с числом $x + y$, не делится по условию на l .

Что же касается условия Б), то, как мы знаем, оно выполнено только для некоторых l . Следовательно, мы пока вынуждены ограничиться только этими l .

Резюмируя, мы видим, что метод Эйлера пока позволил нам доказать теорему Ферма в следующей форме:

Теорема 1. Пусть $l \geq 3$ — такое простое число, что в кольце D_l справедлива основная теорема ариф-

метики. Тогда если для целых рациональных чисел x, y, z имеет место равенство

$$x^l + y^l = z^l,$$

то хотя бы одно из этих чисел делится на l .

Можно показать, что условиям этой теоремы удовлетворяют простые числа

$$(11) \quad l = 3, 5, 7, 11, 13, 17, 19.$$

В пределах первой сотни других простых чисел, удовлетворяющих условиям теоремы 1, нет.

Подчеркнем, однако, что проверка того, что для чисел (11) в кольце D_l справедлива основная теорема арифметики, является при $l > 5$ совсем не простой задачей. Таким образом, утверждать, что для чисел (11) нами доказан первый случай теоремы Ферма, мы, собственно говоря, права пока не имеем.

§ 8. Теория дивизоров

Как же дело обстоит с Вспомогательным утверждением, когда разложение на простые множители в кольце D_l не однозначно? Оказывается, что его все же можно доказать и в этом случае (по крайней мере, для некоторых l). Идея, принадлежащая Куммеру, состоит, как уже говорилось, в том, чтобы восстановить в D_l однозначность разложения на простые множители, добавив некоторые новые «идеальные» числа. Эта мысль Куммера преобразовала всю теорию алгебраических чисел и в руках Дедекинда, Кронекера и Золотарева привела к созданию совершенно новых концепций, оказавших глубокое влияние на все отделы современной математики.

Идеальные числа Куммера называются теперь «дивизорами». Абстрактно, ситуацию с ними можно описать следующим образом.

Предположим, что нам задано некоторое множество \mathcal{D} , в котором определено коммутативное и ассоциативное умножение, обладающее единицей (в абстрактной алгебре такие множества называются *коммутативными моноидами*). Элементы моноида \mathcal{D} мы будем обозначать малыми готическими буквами.

В частности, единицу моноида \mathcal{D} мы будем обозначать символом e .

Говорят, что элемент $a \in \mathcal{D}$ *делит* элемент $c \in \mathcal{D}$, если существует такой элемент $b \in \mathcal{D}$, что $c = ab$. Элемент $b \neq e$ называется *простым*, если он делится только на себя и на единицу e . Моноид \mathcal{D} называется *свободным* (коммутативным) моноидом (или моноидом с однозначным разложением на простые множители), если каждый элемент $a \in \mathcal{D}$ может быть представлен в виде произведения простых элементов

$$a = p_1 \dots p_r, \quad r \geq 0,$$

и такое разложение с точностью до порядка множителей единственно (при $r = 0$ произведение считается равным e). Таким образом, в свободном моноиде нет никаких обратимых элементов («единиц»), кроме «настоящей» единицы e .

Примером свободного моноида является множество \mathbb{N} натуральных чисел по отношению к умножению.

В свободном моноиде для любых элементов существует, очевидно, единственный *наибольший общий делитель* и единственное *наименьшее общее кратное*. Если наибольший общий делитель равен e , то элементы называются *взаимно простыми*.

Ясно, что в произвольном свободном моноиде сохраняются известные свойства делимости в свободном моноиде натуральных чисел. Например, если ab делится на c и a взаимно просто с c , то b делится на c . Если a и b взаимно просты и $ab = c^n$, то существуют такие элементы a_1 и b_1 , что $a = a_1^n$ и $b = b_1^n$, и т. д.

Для произвольного кольца D множество D^* всех его отличных от нуля элементов является, очевидно, моноидом. Предположим, что задано некоторое отображение этого моноида в свободный моноид \mathcal{D} . Обозначая образ элемента $\alpha \in D^*$ символом (α) , мы потребуем, чтобы для любых элементов $\alpha, \beta \in D^*$ было выполнено равенство

$$(\alpha\beta) = (\alpha)(\beta),$$

т. е. чтобы отображение $\alpha \mapsto (\alpha)$ было *гомоморфизмом моноидов*. Тогда, если α делится на β в D , то (α) будет делиться на (β) в \mathcal{D} . Мы потребуем, чтобы было верно и обратное;

Аксиома 1. Элемент $\alpha \in D^*$ тогда и только тогда делится на элемент $\beta \in D^*$, когда элемент $(\alpha) \in \mathcal{D}$ делится на элемент $(\beta) \in \mathcal{D}$.

В частности, отсюда следует, что $(\alpha) = (\beta)$ тогда и только тогда, когда элементы α и β ассоциированы. Единицы ϵ кольца D характеризуются поэтому равенством $(\epsilon) = \epsilon$.

Если элемент a делит элемент (α) , то мы будем говорить, что a делит α . Совокупность всех элементов $\alpha \in D^*$, делящихся на элемент $a \in \mathcal{D}$, плюс элемент $0 \in D$ (который мы, таким образом, по определению, считаем делящимся на любой элемент $a \in \mathcal{D}$), мы обозначим символом $[a]$. Естественно потребовать, чтобы сумма и разность элементов кольца D , делящихся на элемент $a \in \mathcal{D}$, также делилась на a .

Аксиома 2. Если $\alpha, \beta \in [a]$, то $\alpha \pm \beta \in [a]$.

Наконец, потребуем, чтобы в \mathcal{D} не было «лишних» элементов, т. е. чтобы любые два элемента из \mathcal{D} отличались по их свойствам делимости по отношению к элементам кольца D .

Аксиома 3. Если $[a] = [b]$, то $a = b$ и для любого α множество $[a]$ содержит отличные от нуля элементы.

Если для кольца D задан свободный коммутативный моноид \mathcal{D} и гомоморфизм $\alpha \mapsto (\alpha)$, удовлетворяющий аксиомам 1—3, то говорят, что в D задана теория дивизоров. Элементы моноида \mathcal{D} называются при этом дивизорами, а дивизоры вида (α) , где $\alpha \in D$, — главными дивизорами. Единица ϵ моноида \mathcal{D} называется единичным дивизором.

Заметим, что в этом определении ни существование, ни единственность теории дивизоров не предполагаются. Впрочем, можно без труда доказать, что в некотором естественном смысле теория дивизоров для любого кольца D может существовать только одна. Этот факт нам не понадобится, и мы его доказывать не будем (см. Б о р е в и ч З. И., Ш а ф а р е в и ч И. Р. Теория чисел. — М.: Наука, 1972, гл. III, § 2, п. 2).

Напротив, существование теории дивизоров накладывает на кольцо D очень сильные ограничения. В общем виде мы этим вопросом заниматься не будем, поскольку это увело бы нас далеко в сторону.

Легко видеть, что каждое кольцо D , в котором выполняется основная теорема арифметики, обладает теорией дивизоров, причем в этой теории все дивизоры будут главными.

Действительно, пусть \mathcal{D} — множество классов ассоциированных элементов множества D^* (см. § 4). Обозначая класс, содержащий элемент α , символом (α) и полагая $(\alpha)(\beta) = (\alpha\beta)$, мы, как непосредственно проверяется, корректно определим в множестве \mathcal{D} умножение, относительно которого оно будет свободным коммутативным моноидом. Отображение $\alpha \mapsto (\alpha)$ будет при этом гомоморфизмом, удовлетворяющим аксиомам 1—3. При этом дивизор (α) будет прост тогда и только тогда, когда прост элемент α . ■

Обратно, если для кольца D существует теория дивизоров, в которой все дивизоры главные, то в D выполняется основная теорема арифметики.

Действительно, достаточно заметить, что в таком кольце дивизор (π) прост тогда и только тогда, когда прост элемент π (если $\pi = \pi_1\pi_2$, то $(\pi) = (\pi_1)(\pi_2)$, а если $(\pi) = (\pi_1)(\pi_2)$, то π ассоциирован с произведением $\pi_1\pi_2$; обратим внимание, что здесь существенно использовано предположение, что все дивизоры главные), и потому разложение каждого дивизора (α) в произведение простых дивизоров даст разложение элемента α в произведение простых элементов, причем с точностью до ассоциированности это разложение будет единственным. ■

Таким образом, чем больше неглавных дивизоров, тем дальше свойства делимости элементов кольца D (обладающего теорией дивизоров) отличаются от стандартных свойств делимости натуральных чисел. Чтобы придать этому высказыванию точный смысл, назовем два дивизора a и b эквивалентными (обозначение $a \sim b$), если они отличаются только на главные дивизоры, т. е. существуют такие элементы $\alpha, \beta \in D^*$, что

$$(\alpha)a = (\beta)b.$$

Ясно, что это отношение действительно является отношением эквивалентности (оно рефлексивно, симметрично и транзитивно); и потому моноид \mathcal{D} распадается на классы $\{a\}$ эквивалентных между собой ди-

визоров. Очевидно, далее, то формула $\{a\}\{b\} = \{ab\}$ корректно определяет умножение классов дивизоров. Это умножение ассоциативно и коммутативно, так что относительно него множество \mathcal{H} всех классов дивизоров является моноидом. Более того легко видеть, что моноид \mathcal{H} является (абелевой) группой, т. е. любой его элемент обратим. Действительно, согласно аксиоме 3 для любого дивизора a существует элемент $\alpha \neq 0$, делящийся на a , т. е. такой, что $(\alpha) = a\mathfrak{b}$, где \mathfrak{b} — некоторый дивизор. Это означает, что $a\mathfrak{b} = e$, т. е. что $\{b\} = \{a\}^{-1}$ в \mathcal{H} . ■

Группа \mathcal{H} называется группой классов дивизоров кольца D . Она (точнее, число ее элементов) и измеряет отклонение арифметики в D от арифметики натуральных чисел.

Заметим, что любой главный дивизор эквивалентен, очевидно, единичному дивизору, т. е. его класс является единицей группы \mathcal{H} . Верно и обратное: если $a \sim e$, т. е. $(\alpha)a = (\beta)$, то, согласно аксиоме 1, существует такой элемент γ , что $\alpha\gamma = \beta$ и, значит, $(\alpha)(\gamma) = (\beta)$, т. е. $a = (\gamma)$. Таким образом, дивизор тогда и только тогда эквивалентен единичному дивизору, когда он является главным дивизором:

$$a \sim e \Leftrightarrow a = (\alpha).$$

В случае, когда группа \mathcal{H} конечна, число ее элементов, т. е. число классов дивизоров кольца D , мы будем обозначать символом h . Согласно доказанному выше в кольце D тогда и только тогда выполнена основная теорема арифметики, когда группа \mathcal{H} состоит только из одного элемента, т. е. h определено и равно 1.

Мы наложим на рассматриваемую теорию дивизоров следующую дополнительную аксиому:

Аксиома Р. В группе \mathcal{H} нет элементов порядка 1.

В аксиоме Р, как и всюду у нас, под 1 понимается данное фиксированное простое число.

Из аксиомы Р вытекает, что если $a^l \sim b^l$, то $a \sim b$. Действительно, эквивалентность $a^l \sim b^l$ означает, что для классов имеет место равенство $\{a\}^l = \{b\}^l$, т. е. (поскольку \mathcal{H} — группа) равенство $(\{a\}\{b\}^{-1})^l = \{e\}$. Но так как в группе \mathcal{H} нет элементов порядка 1, последнее равенство возможно только тогда, когда

$\{a\}\{b\}^{-1} = \{e\}$, т. е. когда $\{a\} = \{b\}$ и, значит, $a \sim b$. ■

Заметим, что если группа \mathcal{H} конечна, то аксиома **P** равносильна требованию, чтобы простое число l не делило числа классов h (порядка группы \mathcal{H}).

Вернемся теперь к теореме Ферма.

Будем называть простое число l *регулярным*, если кольцо D_l обладает теорией дивизоров, удовлетворяющей аксиоме **P**. Обратим внимание, что в аксиоме **P** фигурирует то же число l , что и в конструкции кольца D_l .

Предложение 1. *Для каждого регулярного простого числа l Вспомогательное утверждение из § 7 верно.*

Доказательство. Если $x^l + y^l = z^l$, то

$$(x + y)(x + \zeta y) \dots (x + \zeta^{l-1}y) = z^l.$$

Перейдем в этом равенстве к дивизорам. Из формулы (10) § 7 непосредственно вытекает, что все главные дивизоры $(x + \zeta^m y)$, $0 \leq m \leq l-1$, попарно взаимно просты. Поэтому из того, что произведение этих дивизоров является l -й степенью (оно равно дивизору $(z)^l$), следует, что каждый из них будет l -й степенью. Таким образом, в частности, существует такой дивизор $\alpha \in \mathcal{D}$, что

$$(x + \zeta y) = \alpha^l.$$

Это равенство означает, что $\alpha^l \sim e$, откуда, как мы знаем, следует, что $\alpha \sim e$, т. е. что $\alpha = (\alpha)$ для некоторого элемента $\alpha \in D_l$. Таким образом,

$$(x + \zeta y) = (\alpha^l),$$

и потому числа $x + \zeta y$ и α^l ассоциированы, т. е. существует такая единица $\varepsilon \in D_l$, что

$$x + \zeta y = \varepsilon \alpha^l. \quad \blacksquare$$

Тем самым, согласно § 7, для регулярных простых чисел доказан первый случай теоремы Ферма:

Т е о р е м а 1. *Если простое число $l \geq 3$ регулярно, то равенство*

$$x^l + y^l = z^l$$

для целых рациональных чисел x, y и z возможно только тогда, когда хотя бы одно из этих чисел делится на l .

Конечно, эту теорему следует дополнить исследованием, какие простые числа регулярны и как про данное простое число узнать, регулярно оно или нет. Без этого теорема 1 никакой реальной ценности, естественно, не имеет. Но мы пока отложим выяснение этого вопроса и займемся вторым случаем теоремы Ферма.

§ 9. Второй случай теоремы Ферма

В этом параграфе мы покажем, что если простое число l не только регулярно, но еще и куммерово, и если, кроме того, для него выполнено условие К из § 6, то для l справедлив и второй случай теоремы Ферма, т. е. равенство

$$(1) \quad x^l + y^l = z^l$$

невозможно и тогда, когда одно из (не равных нулю) чисел x, y, z делится на l .

Поскольку числа x, y, z предполагаются попарно взаимно простыми, только одно из них может делиться на l . Мы будем предполагать, что на l делится число z , что общности не ограничивает, поскольку если на l делится, например, y , то достаточно равенство (1) переписать в виде

$$x^l + (-z)^l = (-y)^l.$$

Пусть $z = l^k z_0$, где z_0 не делится на l , а $k \geq 1$. Поскольку в кольце D_l имеет место равенство

$$l = \varepsilon_0 \lambda^{l-1}, \quad \lambda = 1 - \zeta,$$

где ε_0 — некоторая единица (см. формулу (34) § 5), мы можем переписать равенство (1) в следующем виде (обозначив z_0 снова через z и положив $m = k(l-1)$):

$$(2) \quad x^l + y^l = \varepsilon \lambda^{lm} z^l,$$

где ε — единица. Здесь числа x, y, z взаимно просты с l , а значит (рассматриваемые как элементы кольца D_l) и с λ .

Мы докажем, что равенство типа (2) невозможно даже тогда, когда под x, y, z мы будем понимать произвольные числа кольца D_l , взаимно простые с λ

(и потому не равные нулю). Другими словами, мы докажем, что второй случай теоремы Ферма (для рассматриваемых l) справедлив и в кольце D_l .

Заметим, что первый случай теоремы Ферма (и значит, полная теорема Ферма) также справедлив в кольце D_l . Для доказательства достаточно несколько усложнить рассуждения предыдущих двух параграфов.

В отличие от первого случая, мы не можем доказать второй случай только для целых рациональных чисел: необходимо доказывать более сильное утверждение, относящееся к числам из D_l . (Такого рода ситуация типична для индуктивных доказательств; часто индукция проходит только тогда, когда мы в достаточной мере усилим доказываемое утверждение.)

В доказательстве мы будем существенно пользоваться тем, что *главный дивизор* $I = (\lambda)$, где $\lambda = 1 - \zeta$, является *простым дивизором*. Мы докажем этот факт позже (в § 13), а пока, чтобы не прерывать изложения, примем его без доказательства.

Число α кольца D_l мы назовем *полупервичным* (у нас нет здесь возможности объяснить происхождение этого термина), если, во-первых, оно не делится на I (т. е. на λ), и, во-вторых, существует такое целое рациональное число b_0 (автоматически отличное от нуля), что разность $\alpha - b_0$ делится на I^2 (т. е. $\alpha \equiv b_0 \pmod{\lambda^2}$).

Другими словами, число α полупервично, если в его разложении (37) из § 5 число b_0 не делится на l , а $b_1 = 0$.

Легко видеть, что для любого числа $\alpha \in D_l$, не делящегося на I , существует такое целое рациональное число a , что произведение $\zeta^a \alpha$ полупервично.

Действительно, согласно формуле (37) § 5,

$$\alpha \equiv b_0 + b_1 \lambda \pmod{\lambda^2},$$

где, по условию, $b_0 \not\equiv 0 \pmod{l}$. Пусть a_0 — такое целое рациональное число, что $a_0 b_0 \equiv 1 \pmod{l}$, и пусть $a = a_0 b_1$.

Так как

$$\zeta^a = (1 - \lambda)^a \equiv 1 - a\lambda \pmod{\lambda^2},$$

то

$$\zeta^a \alpha \equiv (1 - a\lambda)(b_0 + b_1 \lambda) \equiv b_0 + (b_1 - ab_0)\lambda \pmod{\lambda^2}.$$

Но, по построению, $b_1 - ab_0 = b_1(1 - a_0b_0)$ делится на l , а, значит, и на λ .

Следовательно, $\zeta^a \alpha \equiv b_0 \pmod{\lambda^2}$. ■

Поскольку $\zeta' = 1$, равенство (2) не меняется при умножении чисел x , y и z на любые степени числа ζ . Поэтому, без ограничения общности, мы можем считать, что *все числа x , y и z в равенстве (2) полупервичны*. Заметим, что при этой редукции показатель m не меняется.

После этих предварительных замечаний мы можем непосредственно перейти к доказательству невозможности равенства типа (2).

Предполагая, что равенства типа (2) существуют, выберем среди них то, у которого показатель m наименьший (а числа x , y , z полупервичны и, напомним, взаимно просты с l). Чтобы не вводить новых обозначений, будем считать, что этим равенством является (2).

Заметим, что теперь m уже не имеет, вообще говоря, вида $k(l-1)$. Однако, тем не менее, справедлива следующая лемма:

Л е м м а 1. *Показатель m больше единицы:*

$$m > 1.$$

Д о к а з а т е л ь с т в о. Перепишем равенство (2), разложив левую часть на множители:

$$(3) \quad (x + y)(x + \zeta y) \dots (x + \zeta^{l-1}y) = \varepsilon \lambda^{lm} z^l.$$

Так как дивизор $I = (\lambda)$ прост, то хотя бы один из множителей слева должен делиться на I . Но так как все эти множители сравнимы друг с другом по модулю λ (ибо $(x + \zeta^a y) - (x + \zeta^b y) = \zeta^a(1 - \zeta^{b-a})y$ делится на $\lambda = 1 - \zeta$), то на I делится каждый из них. В частности, на I делится $x + y$.

Поскольку числа x и y полупервичны, существует такое целое рациональное число a , что

$$x + y \equiv a \pmod{\lambda^2}$$

(число $x + y$ не полупервично, потому что оно делится на λ). Это сравнение показывает, что целое рациональное число a делится на λ . Но тогда оно делится на l , т. е. на λ^{l-1} . Значит, оно заведомо делится на λ^2 , а потому на λ^2 делится и число $x + y$.

Таким образом, в равенстве (3) все множители слева делятся на λ , а первый из них делится даже на λ^2 . Следовательно, левая часть этого равенства делится на λ^{l+1} . Поэтому на λ^{l+1} делится и правая часть. Так как z взаимно просто с λ , это возможно только тогда, когда $m > 1$. ■

Произведенное исследование делимости на λ множителей левой части равенства (3) можно уточнить:

Л е м м а 2. Числа

$$(4) \quad x + \xi y, \dots, x + \xi^{l-1} y,$$

делясь на λ , не делятся на λ^2 . Число

$$x + y$$

делится на $\lambda^{l(m-1)+1}$, но не делится на $\lambda^{l(m-1)+2}$.

До к а з а т е л ь с т в о. Достаточно, очевидно, доказать, что ни одно из чисел (4) не делится на λ^2 . Пусть, например, число $x + \xi^k y$ делится на λ^2 . Тогда на λ^2 будет делиться число

$$(1 - \xi^k) y = (x + y) - (x + \xi^k y),$$

а значит, и число $1 - \xi^k$, что невозможно, ибо, как мы знаем, число $1 - \xi^k$ ассоциировано с $\lambda = 1 - \xi$. ■

Дальнейшие рассуждения повторяют (с соответствующими усложнениями) доказательство Вспомогательного утверждения из § 8.

Пусть m — наибольший общий делитель главных дивизоров (x) и (y) . Так как x и y не делятся на $l = (\lambda)$, то и m не делится на l . Поэтому, согласно лемме 2, дивизоры вида $(x + \xi^k y)$, $k \neq 0$, делятся на $l m$, а дивизор $(x + y)$ — даже на $l^{l(m-1)+1} m$. Пусть

$$(5) \quad \begin{aligned} (x + y) &= l^{l(m-1)+1} m c_0, \\ (x + \xi^k y) &= l m c_k, \quad k = 1, \dots, l-1. \end{aligned}$$

Согласно лемме 2 ни один из дивизоров c_0, c_1, \dots, c_{l-1} не делится на l .

Л е м м а 3. Дивизоры c_0, c_1, \dots, c_{l-1} попарно взаимно просты.

До к а з а т е л ь с т в о. Пусть, например, дивизоры c_i и c_k , $0 \leq i < k \leq l-1$, имеют общий делитель p .

Тогда числа $x + \zeta^i y$ и $x + \zeta^k y$ делятся на $\text{Im} \eta$, и потому числа

$$\begin{aligned}(x + \zeta^k y) \zeta^i - (x + \zeta^i y) \zeta^k &= \zeta^i (1 - \zeta^{k-i}) x, \\ - (x + \zeta^k y) + (x + \zeta^i y) &= \zeta^i (1 - \zeta^{k-i}) y\end{aligned}$$

также делятся на $\text{Im} \eta$. Поскольку множитель $\zeta^i (1 - \zeta^{k-i})$ ассоциирован с $\lambda = 1 - \zeta$, отсюда следует, что числа x и y делятся на η , что противоречит определению наибольшего общего делителя. ■

Эта лемма является аналогом предложения 1 § 7.

Перейдя в (3) к дивизорам и подставив их выражения (5), мы получим (после сокращения на l^m) равенство

$$m' c_0 c_1 \dots c_l = z^l,$$

где $z = (z)$. Поскольку дивизоры c_0, c_1, \dots, c_l попарно взаимно просты, это равенство возможно только тогда, когда эти дивизоры являются l -ми степенями, т. е. имеют вид

$$(6) \quad c_i = a_i^l, \quad i = 0, 1, \dots, l-1,$$

где a_i — некоторые дивизоры (очевидно, не делящиеся на l).

Лемма 4. Если число l регулярно, то дивизоры a_0, a_1, \dots, a_{l-1} эквивалентны.

Доказательство. Подставив в (5) выражения (6), мы получим, что

$$\begin{aligned}(x + y) &= l^{l(m-1)+1} m a_0^l, \\ (x + \zeta^k y) &= l m a_k^l, \quad k = 1, \dots, l-1.\end{aligned}$$

Перемножив эти равенства «крест накрест» и сократив на ml , мы получим соотношения

$$(7) \quad (x + y) a_k^l = (x + \zeta^k y) (l^{m-1} a_0)^l, \quad k = 1, \dots, l-1,$$

означающие, что $a_k^l \sim (l^{m-1} a_0)^l$. Так как число l регулярно, то отсюда следует, что $a_k \sim l^{m-1} a_0$. Но дивизор $l = (\lambda)$ главный и потому $l^{m-1} a_0 \sim a_0$. Таким образом, $a_k \sim a_0$ для любого $k = 1, \dots, l-1$. ■

Согласно лемме 4, существуют такие числа $\alpha_k, \beta_k \in D_l$, что

$$(8) \quad (\alpha_k) a_0 = (\beta_k) a_k, \quad k = 1, \dots, l-1.$$

Так как дивизоры α_i , $i = 0, 1, \dots, l-1$, не делятся на $I = (\lambda)$, то без ограничения общности можно считать, что числа α_k и β_k не делятся на λ .

Умножив равенства (7) на $(\alpha_k \beta_k)^l$ и воспользовавшись соотношением (8), мы получим следующее соотношение между главными дивизорами:

$$(x+y)(\alpha_k)^l = (x+\zeta^k y)(\lambda^{m-1} \beta_k)^l, \quad k = 1, \dots, l-1.$$

Но равенство главных дивизоров равносильно равенству соответствующих чисел с точностью до множителя, являющегося единицей. Следовательно,

$$(9) \quad (x+\zeta^k y) \lambda^{l(m-1)} \beta_k^l = (x+y) \varepsilon_k \alpha_k^l,$$

где ε_k — некоторая единица кольца D_l . Это равенство (являющееся аналогом Вспомогательного утверждения из § 7) нам понадобится только при $k = 1, 2$.

Л е м м а 5. В кольце D_l существуют такие числа x_1 , β , z_1 , не делящиеся на λ (а значит, отличные от нуля), и такие единицы ε_0 и ε , что

$$(10) \quad x_1^l + \varepsilon_0 \beta^l = \varepsilon \lambda^{l(m-1)} z_1^l.$$

До к а з а т е л ь с т в о. Покажем, что равенство (10) имеет место при

$$x_1 = \alpha_1 \beta_2, \quad \beta = \alpha_2 \beta_1, \quad z_1 = \beta_1 \beta_2, \\ \varepsilon_0 = \frac{\varepsilon_2}{\varepsilon_1 (1 + \zeta)}, \quad \varepsilon = \frac{\zeta}{\varepsilon_1 (1 + \zeta)}$$

(ясно, что число $1 + \zeta$ является единицей).

Так как

$$(x + \zeta y)(1 + \zeta) - (x + \zeta^2 y) = (x + y) \zeta,$$

то, умножив это равенство на $\lambda^{l(m-1)}$ и воспользовавшись соотношением (9) при $k = 1, 2$, мы получим, что

$$(x+y) \left(\frac{\alpha_1}{\beta_1} \right)^l \varepsilon_1 (1 + \zeta) - (x+y) \left(\frac{\alpha_2}{\beta_2} \right)^l \varepsilon_2 = \\ = (x+y) \zeta \lambda^{l(m-1)}.$$

Сократив это равенство на $x+y$ и умножив на $(\beta_1 \beta_2)^l \varepsilon_1^{-1} (1 + \zeta)^{-1}$, мы и получим (10). ■

Теперь мы уже без особого труда можем прийти к противоречию.

Согласно предложению 4 § 5 существуют такие целые рациональные числа a и b , что

$$x_1^l \equiv a \pmod{l} \quad \text{и} \quad \beta^l \equiv b \pmod{l}.$$

При этом числа a и b не делятся, очевидно, на l .

С другой стороны, так как $l(m-1) \geq l > l-1$ (см. лемму 1), то правая часть соотношения (10) делится на $l \sim \lambda^{l-1}$. Следовательно, на l делится и левая часть $x_1^l + \varepsilon_0 \beta^l \equiv a + \varepsilon_0 b \pmod{l}$. Поэтому

$$a + \varepsilon_0 b \equiv 0 \pmod{l}.$$

Но, поскольку b не делится на l , существует такое целое число b' , что $bb' \equiv 1 \pmod{l}$. Следовательно,

$$\varepsilon_0 \equiv b' b \varepsilon_0 \equiv -b' a \pmod{l}.$$

Этим доказано, что единица ε_0 удовлетворяет условиям предложения 7 § 6. Следовательно, если число l куммерово и выполнено условие К из § 6, то в кольце D_l существует такая единица η , что она является l -й степенью некоторой другой единицы η :

$$\varepsilon_0 = \eta^l.$$

Таким образом, в кольце D_l существуют такие (отличные от нуля) числа $x_1, y_1 = \eta \beta$ и z_1 , не делящиеся на λ , и такая единица ε , что

$$x_1^l + y_1^l = \varepsilon \lambda^{l(m-1)} z_1^l.$$

Мы видим, что, отправляясь от равенства (2) с показателем m , мы пришли к такому же равенству с меньшим показателем $m-1$. Поскольку это невозможно (показатель m был выбран наименьшим возможным), тем самым доказано, что для рассматриваемых l равенство (2) невозможно.

Резюмируя, мы видим, что теорема Ферма нами доказана в следующей формулировке:

Теорема 1. Если простое число $l \geq 3$ регулярно, куммерово и для него выполнено условие К из § 6, то ни для каких отличных от нуля рациональных чисел x, y, z равенство

$$x^l + y^l = z^l$$

невозможно.

Теперь нам остается только исследовать, какие простые числа удовлетворяют условиям этой теоремы.

Оказывается, что в наше определение регулярного простого числа входят требования, которые выполнены для любого простого l и которые, следовательно, можно исключить. Именно, оказывается, что *каждое кольцо D_l допускает теорию дивизоров с конечной группой \mathcal{H} классов дивизоров.*

Это утверждение является частным случаем общей теоремы, относящейся к кольцам целых элементов произвольного поля алгебраических чисел (см. конец § 11). Впервые эта общая теорема была доказана Дедекиндом (тогда как утверждение о кольце D_l — Куммером) и впоследствии неоднократно передоказывалась многими авторами. Мы докажем эту теорему, следуя идеям Дедекинда.

§ 10. Теория идеалов

Пусть D — произвольное кольцо. Непустое подмножество A кольца D называется его *идеалом* (термин предложен Дедекиндом из-за связи с идеальными числами Куммера), если

- 1) $\alpha \pm \beta \in A$ для любых элементов $\alpha, \beta \in A$;
- 2) $\alpha\beta \in A$ для любых элементов $\alpha \in A, \beta \in D$.

Примером идеала является так называемый *нулевой идеал*, состоящий только из нуля 0 кольца D . В дальнейшем *все идеалы предполагаются ненулевыми.*

Примером ненулевого идеала является само кольцо D .

Этот идеал называется *единичным*. Мы будем обозначать его символом (1).

Последний пример может быть обобщен. Пусть $\alpha \in D$ — произвольный отличный от нуля элемент кольца D . Ясно, что все элементы кольца D , делящиеся на α , составляют идеал. Этот идеал обозначается символом (α) и называется *главным идеалом*, порожденным элементом α . При $\alpha = 1$ (а также при α , являющемся произвольной единицей) мы, очевидно, получаем единичный идеал.

Ясно, что *пересечение любого семейства идеалов также является идеалом*. Поэтому для любого множества $X \subset D$ существует наименьший идеал, содержащий это множество (им является пересечение всех идеалов, содержащих X). Этот идеал обозначается

символом (X) и называется идеалом, порожденным множеством X .

Легко видеть, что идеал (X) состоит из всех элементов вида $\alpha_1\xi_1 + \dots + \alpha_n\xi_n$, где $\alpha_1, \dots, \alpha_n \in D$ и $\xi_1, \dots, \xi_n \in X$ (докажите!).

Если X состоит из конечного числа элементов ξ_1, \dots, ξ_n , то идеал (X) обозначается символом (ξ_1, \dots, ξ_n) . В частности, при $n = 1$ и $\xi_1 = \xi$ мы получаем главный идеал (ξ) .

Кольцо D называется *кольцом главных идеалов*, если в нем любой идеал главный. Поскольку утверждение, что $(\alpha, \beta) = (\delta)$, в точности равносильно тому, что δ является наибольшим общим делителем элементов α, β и имеет вид $\alpha x_0 + \beta y_0$, мы видим, что в случае, когда любой идеал порождается двумя элементами (или хотя бы конечным числом элементов), это понятие кольца главных идеалов совпадает с понятием, введенным в § 4.

В случае, когда кольцо D допускает теорию дивизоров, понятие главного идеала может быть обобщено иным способом. Именно, согласно аксиоме 2 из § 8, для любого дивизора α множество $[\alpha]$ всех элементов кольца D (включая нуль), делящихся на α , обладает свойством 1) идеалов. Свойство 2) для него также, очевидно, выполнено. Следовательно, $[\alpha]$ является идеалом (согласно аксиоме 3 — ненулевым).

Таким образом, соответствие $\alpha \mapsto [\alpha]$ переводит дивизоры в идеалы и обладает, очевидно, тем свойством, что для любого главного дивизора (α) соответствующий идеал $[(\alpha)]$ — это в точности введенный выше главный идеал (α) . Это оправдывает обозначение одним и тем же символом главного дивизора и соответствующего главного идеала; при достаточной внимательности это привести к недоразумениям не может.

Согласно аксиоме 3 из § 8, отображение $\alpha \mapsto [\alpha]$ моноида дивизоров в множество идеалов инъективно, т. е. различные дивизоры оно переводит в различные идеалы. Это, казалось бы, позволяет отождествить дивизоры с идеалами и, в частности, строить теорию дивизоров, исходя из идеалов. В этом и состоит идея Дедекинда. С его точки зрения, дивизоры и идеалы — это одно и то же.

Однако оказалось, что существуют кольца, допускающие теорию дивизоров, но в которых есть идеалы, не имеющие вида $[a]$ (примером является кольцо многочленов от двух переменных и в нем идеал всех многочленов без свободного члена). Таким образом, в этих кольцах «слишком много» идеалов. С другой стороны, имеются кольца, моноид главных идеалов которых не погружается в свободный моноид. В таких кольцах теория дивизоров вообще невозможна.

Поэтому в настоящее время принято строго различать идеалы и дивизоры.

Программа Дедекинда удалась только потому, что в кольцах целых алгебраических чисел идеалы образуют свободный моноид и в этих кольцах нет «лишних» идеалов.

Проводя в жизнь идею Дедекинда, следует, конечно, начать с определения умножения идеалов.

Пусть A и B — два идеала произвольного (пока) кольца D . Рассмотрим множество X всех элементов вида $\alpha\beta$, где $\alpha \in A$, $\beta \in B$. Это множество, вообще говоря, идеалом не является. Мы примем за *произведение* AB идеалов A и B идеал, порожденный множеством X . Согласно сказанному выше, идеал AB состоит из всевозможных элементов вида $\alpha_1\beta_1 + \dots + \alpha_n\beta_n$, где $\alpha_1, \dots, \alpha_n \in A$, $\beta_1, \dots, \beta_n \in B$.

Ясно, что это умножение ассоциативно, коммутативно и обладает единицей (ею служит идеал $(1) = D$). Таким образом, относительно этого умножения множество $\text{Id}(D)$ всех (ненулевых) идеалов кольца D является моноидом.

Очевидно, что главный идеал, порожденный произведением элементов кольца D , является произведением соответствующих главных идеалов:

$$(1) \quad (\alpha\beta) = (\alpha)(\beta).$$

Это означает, что отображение $\alpha \mapsto (\alpha)$ моноида D^* в моноид $\text{Id}(D)$ представляет собой гомоморфизм.

Из формулы (1) следует, что если элемент α делит элемент γ , то идеал (α) делит идеал (γ) . Обратное также верно: если (α) делит (γ) , то α делит γ . Действительно, любой идеал вида $(\alpha)B$ состоит из элементов вида $\alpha\beta$, где $\beta \in B$. Поэтому, если $(\alpha)B = (\gamma)$, то $\alpha\beta_0 = \gamma$, где $\beta_0 \in B$, т. е. γ делится на α . ■

Таким образом, для отображения $\alpha \mapsto (\alpha)$ выполнены аксиомы 1 теории дивизоров.

Полезно также иметь в виду, что если $(\gamma)A = (\gamma)B$, то $A = B$ (возможность сокращения на главный идеал). Действительно, равенство $(\gamma)A = (\gamma)B$ означает, что любой элемент вида $\gamma\alpha$, $\alpha \in A$, имеет вид $\gamma\beta$, $\beta \in B$, и обратно. Сокращая на γ , мы получаем, что любой элемент $\alpha \in A$ лежит в B и обратно. ■

По построению $AB \subset A$. Таким образом, если идеал C делится на идеал A , то $C \subset A$. (Обратите внимание, что делящий идеал «больше» делимого идеала.)

Обратное, во всяком случае, верно, когда идеал A главный, т. е. если $C \subset (\alpha)$, то существует такой идеал B , что $C = (\alpha)B$. Действительно, включение $C \subset (\alpha)$ означает, что любой элемент $\gamma \in C$ имеет вид $\alpha\beta$, где $\beta \in D$. Пусть B — множество всех таких элементов $\beta \in D$, что $\alpha\beta \in C$. Непосредственно проверяется, что B — идеал и что $(\alpha)B = C$. ■

Чтобы пойти дальше, необходимо наложить на D определенные условия. Мы не будем пытаться искать минимально необходимые условия, а наложим на D условия, позволяющие наиболее быстро прийти к цели, и вместе с тем не исключающие колец D_l , которые, собственно говоря, нам только и нужны.

В первую очередь мы потребуем, чтобы в D существовало n таких элементов

$$\omega_1, \omega_2, \dots, \omega_n$$

(где n — некоторое натуральное число), что любой элемент $\alpha \in D$ однозначно представляется в виде

$$(2) \quad \alpha = a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n,$$

где a_1, a_2, \dots, a_n — целые рациональные числа. На языке теории групп это свойство означает, что аддитивная группа кольца D является решеткой (свободной абелевой группой) ранга n с базисом $\omega_1, \omega_2, \dots, \omega_n$. Кольцо D_l обладает этим свойством при $n = l - 1$, и $\omega_1 = 1, \omega_2 = \xi, \dots, \omega_n = \xi^{l-2}$.

В теории групп доказывается, что любая подгруппа A решетки D ранга n является решеткой ранга $r \leq n$.

Изложим для полноты доказательство этого утверждения.

Пусть A_k , $k = 1, \dots, n + 1$, — подгруппа группы A , состоящая из элементов (2), для которых $a_1 = \dots = a_{k-1} = 0$. (Таким

образом, $A_1 = A$ и $A_{n+1} = 0$.) Ясно, что для любого $k = 1, \dots, n$ множество всех коэффициентов a_k элементов из A_k составляет идеал (возможно, нулевой) в кольце целых чисел \mathbb{Z} . Но в этом кольце все идеалы главные (ибо имеет место алгоритм деления с остатком), и поэтому существует коэффициент $a_k^{(0)}$, порождающий этот идеал (случай $a_k^{(0)} = 0$ здесь не исключается). Пусть ξ_k — произвольный элемент группы A_k с этим коэффициентом (если $a_k^{(0)} = 0$, то мы положим $\xi_k = 0$).

Покажем, что элементы ξ_1, \dots, ξ_n порождают группу A , т. е. что любой элемент $\alpha \in A$ имеет вид

$$(3) \quad \alpha = b_1 \xi_1 + \dots + b_n \xi_n,$$

где b_1, \dots, b_n — целые рациональные числа.

Поскольку $A_{n+1} = 0$, то для элементов из A_{n+1} формула (3) имеет место. Рассуждая по индукции, предположим, что для некоторого $k \leq n$ уже доказано, что любой элемент из A_{k+1} имеет вид (3) (с $b_1 = \dots = b_k = 0$), и покажем, что тогда любой элемент $\alpha \in A_k$ также имеет вид (3) (с $b_1 = \dots = b_{k-1} = 0$). Ясно, что этим все будет доказано.

Пусть

$$\alpha = a_k \omega_k + \dots + a_n \omega_n.$$

По построению коэффициент a_k делится на $a_k^{(0)}$ (если $a_k^{(0)} = 0$, то $a_k = 0$ для всех элементов $\alpha \in A_k$), т. е. существует такое целое число b_k , что $a_k = a_k^{(0)} b_k$. Тогда $\alpha - b_k \xi_k \in A_{k+1}$ и поэтому $\alpha - b_k \xi_k = b_{k+1} \xi_{k+1} + \dots + b_n \xi_n$. Следовательно, $\alpha = b_k \xi_k + b_{k+1} \xi_{k+1} + \dots + b_n \xi_n$.

Вобщем говоря, среди элементов ξ_1, \dots, ξ_n могут быть равные нулю. Перенумеровав (если нужно) эти элементы, мы можем считать, что $\xi_1 \neq 0, \dots, \xi_r \neq 0$ и $\xi_{r+1} = 0, \dots, \xi_n = 0$. Соответствующим образом перенумеровав элементы базиса $\omega_1, \dots, \omega_n$, мы при этом можем считать, что для любого $k = 1, \dots, n$ по-прежнему $\xi_k \in A_k$, т. е. что в выражении элемента ξ_k через базис $\omega_1, \dots, \omega_n$ коэффициенты при $\omega_1, \dots, \omega_{k-1}$ равны нулю. Но теперь, кроме того, мы можем утверждать, что при $k = 1, \dots, r$ коэффициент $a_k^{(0)}$ элемента ξ_k отличен от нуля, ибо, по построению, $a_k^{(0)} = 0$ только при $\xi_k = 0$.

Отсюда следует, что элементы ξ_1, \dots, ξ_r независимы, т. е. равенство $a_1 \xi_1 + \dots + a_r \xi_r = 0$, где a_1, \dots, a_r — целые рациональные числа, имеет место только при $a_1 = 0, \dots, a_r = 0$. Действительно, в противном случае будет существовать отличное от нуля число a_i с наименьшим i , и тогда в разложении элемента $a_1 \xi_1 + \dots + a_r \xi_r = 0$ по базису $\omega_1, \dots, \omega_n$ коэффициентом при ω_i будет отличное от нуля число $a_i a_i^{(0)}$, что невозможно.

Этим доказано, что любой элемент $\alpha \in A$ однозначно выражается через ξ_1, \dots, ξ_r , т. е. что A является решеткой с базисом ξ_1, \dots, ξ_r (и, следовательно, ранга r).

Далее, известно, что ранг n решетки не зависит от выбора базиса и равен максимальному числу независимых элементов решетки.

Заметим, что, в отличие от классического случая линейных пространств, *не любые* n независимых элементов решетки составляют ее базис. Для этого необходимо и достаточно, чтобы определитель, составленный из коэффициентов разложений этих элементов по элементам базиса, был равен ± 1 .

Действительно, при $r = n$ мы имеем в A базис ξ_1, \dots, ξ_n вида

$$\begin{aligned} \xi_1 &= a_1^{(0)}\omega_1 + a_1^{(1)}\omega_2 + \dots + a_1^{(n-1)}\omega_n \\ \xi_2 &= a_2^{(0)}\omega_2 + \dots + a_2^{(n-2)}\omega_n \\ &\vdots \\ \xi_n &= a_n^{(0)}\omega_n, \end{aligned}$$

$$a_1\omega_1 + a_2\omega_2 + \dots + a_n\omega_n,$$
$$0 \leq a_1 < |a_1^{(0)}|, \quad 0 \leq a_2 < |a_2^{(0)}|, \quad \dots, \quad 0 \leq a_n < |a_n^{(0)}|,$$

Отсюда следует, что существует только конечное число подгрупп группы D , содержащих подгруппу A .

Действительно, при естественном гомоморфизме $D \rightarrow D/A$ такие подгруппы взаимно однозначно соответствуют всевозможным подгруппам группы D/A , а этих подгрупп конечное число.

Все эти утверждения применимы к произвольному идеалу A кольца D , поскольку, по определению, идеал является, в частности, подгруппой аддитивной группы кольца. Таким образом, во-первых, мы видим, что *любой идеал A является решеткой*.

Во-вторых, так как для любого элемента $\alpha \in A$ элементы $\alpha\omega_1, \dots, \alpha\omega_n$ идеала A , очевидно, независимы, то *ранг любого идеала кольца D* (рассматри-

Действительно, пусть ξ_1, \dots, ξ_n — базис идеала A . Тогда любой элемент идеала AB может быть, как легко видеть, представлен в виде $\xi_1\beta_1 + \dots + \xi_n\beta_n$, где $\beta_1, \dots, \beta_n \in B$. Поскольку $AB = B$, отсюда следует, что для ξ_1, \dots, ξ_n имеют место равенства вида

$$\begin{aligned} \xi_1 &= \xi_1\beta_{11} + \dots + \xi_n\beta_{1n}, \\ &\dots \dots \dots \beta_{ij} \in B, \\ \xi_n &= \xi_1\beta_{n1} + \dots + \xi_n\beta_{nn}, \end{aligned}$$

т. е. равенства (4) с $\rho = 1$. Поэтому число $\rho = 1$ является корнем уравнения вида (6), т. е., другими словами, имеет место равенство $1 = -\beta_1 - \dots - \beta_n$, где β_1, \dots, β_n выражаются через элементы β_{ij} идеала B посредством действий сложения, вычитания и умножения и, следовательно, принадлежат этому идеалу. Но тогда и $1 \in B$, т. е. $B = (1)$. ■

Сама же лемма 1 непосредственно вытекает из простейших фактов линейной алгебры. Действительно, равенства (5) означают, что $(\xi_1, \dots, \xi_n) \neq (0, \dots, 0)$ является решением системы линейных однородных уравнений

$$\begin{aligned} (\beta_{11} - \rho) \xi_1 + \dots + \beta_{1n} \xi_n &= 0, \\ \dots \dots \dots \beta_{n1} \xi_1 + \dots + (\beta_{nn} - \rho) \xi_n &= 0. \end{aligned}$$

Но из линейной алгебры известно, что если система n линейных однородных уравнений от n неизвестных имеет решение $\neq (0, \dots, 0)$, то ее определитель равен нулю.

Следовательно,

$$\begin{vmatrix} \beta_{11} - \rho & \dots & \beta_{1n} \\ \dots & \dots & \dots \\ \beta_{n1} & \dots & \beta_{nn} - \rho \end{vmatrix} = 0.$$

Раскрыв определитель, мы и получим для ρ уравнение вида (6). ■

Чтобы пойти дальше, мы еще больше сузим класс рассматриваемых колец. Именно, мы потребуем, чтобы для кольца D существовало n его инъективных отображений $\alpha \mapsto \alpha^{(i)}$, $i = 1, \dots, n$, в поле комплексных чисел \mathbb{C} , сохраняющих сложение и умножение (т. е. являющихся *гомоморфизмами*) и таких, что для любого $\alpha \in D$ элементарные симметрические многочлены от $\alpha^{(1)}, \dots, \alpha^{(n)}$ являются целыми рациональными числами (иными словами, требуется, чтобы многочлен $(x - \alpha^{(1)}) \dots (x - \alpha^{(n)})$ имел целые коэффициенты).

Для кольца D_i такие отображения были построены в § 5.

Для произвольного D мы введем норму $N\alpha$ элемента $\alpha \in D$ формулой

$$N\alpha = \alpha^{(1)} \dots \alpha^{(n)}.$$

Эта норма является целым рациональным числом, но, вообще говоря, уже не обязательно неотрицательным (хотя по-прежнему $N\alpha = 0$ тогда и только тогда, когда $\alpha = 0$). Как и в случае кольца D_l , для любых элементов $\alpha, \beta \in D$ имеет место равенство

$$N(\alpha\beta) = N\alpha \cdot N\beta$$

(ибо по условию $(\alpha\beta)^{(i)} = \alpha^{(i)}\beta^{(i)}$ для любого $i = 1, \dots, n$). Кроме того,

$$N\alpha = \alpha^n$$

для любого рационального α .

Удобно (хотя совсем не обязательно) «вложить» кольцо D в поле \mathbb{C} посредством отображения $\alpha \mapsto \alpha^{(1)}$, т. е. считать, что $D \subset \mathbb{C}$ и $\alpha^{(1)} = \alpha$ для любого $\alpha \in D$. (Заметим, что в случае кольца D_l дело обстоит именно так.)

Считая кольцо D вложенным в поле \mathbb{C} , мы можем определить поле отношений K кольца D просто как наименьшее подполе поля \mathbb{C} , содержащее кольцо D , или, иначе, как множество всех чисел из \mathbb{C} вида $\frac{\beta}{\alpha}$, где $\alpha, \beta \in D$ и $\alpha \neq 0$, избегая, тем самым, простой, но несколько кропотливой абстрактной процедуры построения этого поля для кольца D , не вложенного в \mathbb{C} .

В случае кольца D_l для любого $i = 1, \dots, n$, где $n = l - 1$, было выполнено включение $\alpha^{(i)} \in D$. Теперь это, вообще говоря, не так. Однако легко видеть, что $\alpha^{(2)} \dots \alpha^{(n)} \in D$ для любого $\alpha \in D$, т. е. что $N\alpha$ делится на α в D . Действительно, по условию число $\alpha = \alpha^{(1)}$ удовлетворяет уравнению вида

$$\alpha^n + c_1\alpha^{n-1} + \dots + c_{n-1}\alpha + c_n = 0.$$

с целыми коэффициентами, причем $N\alpha = (-1)^n c_n$. Поэтому

$$\begin{aligned} \frac{N\alpha}{\alpha} &= \frac{(-1)^n c_n}{\alpha} = (-1)^{n+1} \frac{\alpha^n + c_1\alpha^{n-1} + \dots + c_{n-1}\alpha}{\alpha} = \\ &= (-1)^{n+1} (\alpha^{n-1} + c_1\alpha^{n-2} + \dots + c_{n-1}) \in D. \quad \blacksquare \end{aligned}$$

Известным уже нам рассуждением (см. § 5) отсюда выводится, что любой элемент ξ поля K может быть (очевидно, единственным образом) записан в виде

$$(7) \quad \xi = x_1\omega_1 + \dots + x_n\omega_n,$$

где $\omega_1, \dots, \omega_n$ — базис кольца D , а x_1, \dots, x_n — рациональные числа (и, конечно, каждое число ξ такого вида лежит в K).

Лемма 2. Существует такое натуральное число $T = T(D)$, зависящее только от кольца D , что для каждого элемента $\xi \in K$ найдется такой элемент $\alpha \in D$ и такое натуральное число $s < T$, что

$$N(s\xi - \alpha) < 1.$$

Доказательство. Выбрав в D базис $\omega_1, \dots, \omega_n$, мы примем за T произвольное натуральное число, удовлетворяющее неравенствам

$$T > Q^n > \prod_{i=1}^n (|\omega_1^{(i)}| + \dots + |\omega_n^{(i)}|),$$

где Q — некоторое натуральное число.

Ясно, что для любого элемента (7) поля K и любого натурального i можно подобрать такой элемент $\alpha_i \in D$, что для элемента

$$(8) \quad i\xi - \alpha_i = y_1\omega_1 + \dots + y_n\omega_n$$

будут выполнены неравенства

$$0 \leq |y_1| < 1, \dots, 0 \leq |y_n| < 1.$$

Разобьем полуинтервал $[0, 1)$ на Q полуинтервалов вида

$$(9) \quad \left[\frac{j}{Q}, \frac{j+1}{Q} \right), \quad j = 0, \dots, Q-1.$$

Каждая координата y_1, \dots, y_n числа (8) лежит в одном из этих интервалов. Поэтому существует всего Q^n возможностей распределения этих координат по полуинтервалам (9). Следовательно, если мы рассмотрим числа (8) для всех i от 0 до Q^n (т. е. всего $Q^n + 1$ чисел), то по крайней мере два числа будут давать одну и ту же комбинацию распределения координат по полуинтервалам (9). Разность этих чисел имеет вид

$s\xi - \alpha$, где $s \in \mathbb{N}$, а $\alpha \in D_I$, а ее координаты удовлетворяют неравенствам

$$|y_1| < \frac{1}{Q}, \dots, |y_n| < \frac{1}{Q}.$$

Поэтому

$$|(s\xi - \alpha)^{(i)}| < \frac{1}{Q} (|\omega_1^{(i)}| + \dots + |\omega_n^{(i)}|), \quad i=1, \dots, n,$$

и, значит,

$$|N(s\xi - \alpha)| < \frac{1}{Q^n} \prod_{i=1}^n (|\omega_1^{(i)}| + \dots + |\omega_n^{(i)}|) < 1.$$

Для завершения доказательства остается заметить, что натуральное число s , являясь разностью двух натуральных чисел, не превосходящих Q^n , также не превосходит Q^n и, следовательно, меньше T . ■

По аналогии с дивизорами назовем два идеала A и B эквивалентными, если существуют такие главные идеалы (α) и (β) , что

$$(\alpha)A = (\beta)B.$$

Ясно, что множество всех идеалов распадается на классы эквивалентных идеалов.

Предложение 1. Для любого кольца D , удовлетворяющего перечисленным выше условиям, число классов идеалов конечно.

Доказательство. Пусть A — произвольный идеал.

Среди отличных от нуля чисел идеала A существует число α_0 , для которого натуральное число $|N\alpha_0|$ имеет наименьшее возможное значение, так что

$$|N\alpha_0| \leq |N\alpha|$$

для любого отличного от нуля элемента $\alpha \in A$.

Пусть $\alpha \in A$. Применяя лемму 2 к элементу

$$\xi = \frac{\alpha}{\alpha_0} \in K,$$

мы найдем натуральное число $s < T$ и элемент $\gamma \in D$, удовлетворяющие соотношению

$$\left| N\left(s\frac{\alpha}{\alpha_0} - \gamma\right) \right| < 1,$$

т. е. соотношению

$$|N(s\alpha - \gamma\alpha_0)| < |N\alpha_0|.$$

Поскольку $s\alpha - \gamma\alpha_0 \in A$, это неравенство возможно только при $s\alpha = \gamma\alpha_0$. Этим доказано, что α_0 делит элемент $s\alpha$, а значит, и элемент $S\alpha$, где $S = T!$.

Таким образом, для любого элемента $\alpha \in A$ существует такой элемент $\beta \in D$, что

$$(10) \quad \alpha_0\beta = S\alpha.$$

Пусть B — множество всех таких β (при всевозможных $\alpha \in A$). Ясно, что если $\beta_1, \beta_2 \in B$, то $\beta_1 \pm \beta_2 \in B$ (если $\alpha_0\beta_1 = S\alpha_1$ и $\alpha_0\beta_2 = S\alpha_2$, где $\alpha_1, \alpha_2 \in A$, то $\alpha_0(\beta_1 \pm \beta_2) = S(\alpha_1 \pm \alpha_2)$, где $\alpha_1 \pm \alpha_2 \in A$). Кроме того, если $\alpha_0\beta = S\alpha$, то $\alpha_0(\beta\gamma) = S(\alpha\gamma)$ для любого $\gamma \in D$, и, следовательно, $\beta\gamma \in B$ (ибо $\alpha\gamma \in A$). Этим доказано, что B представляет собой идеал.

Равенство (10) означает теперь, что

$$(\alpha_0)B = (S)A,$$

т. е. что идеал B эквивалентен идеалу A .

Кроме того, так как $\alpha_0 \in A$, то $(S)(\alpha_0) \subset (\alpha_0)B$, т. е. $(S) \subset B$.

Но мы уже знаем, что число идеалов, содержащих данный фиксированный идеал (в нашем случае — идеал (S)), конечно. Таким образом, каждый идеал A эквивалентен идеалу B , принадлежащему некоторому конечному множеству идеалов.

Следовательно, число классов идеалов конечно. ■

Пусть снова A — произвольный (ненулевой) идеал кольца D . Попробуем доказать, что некоторая его степень A^q , $q \geq 0$, является главным идеалом.

Так как число неэквивалентных идеалов конечно, должны существовать такие два числа $p > 0$ и $q > 0$, что $A^p \sim A^{p+q}$. По определению, это означает, что существуют такие элементы $\alpha, \beta \in D^*$, что

$$(11) \quad (\alpha)A^p = (\beta)A^{p+q}.$$

Пусть ξ_1, \dots, ξ_n — базис идеала A^p . Тогда любой элемент идеала $A^{p+q} \subset A^p$ может быть представлен в виде $a_1\xi_1 + \dots + a_n\xi_n$, где a_1, \dots, a_n — целые рациональные числа, а значит, любой элемент идеала

(β) A^{p+q} — в виде $\beta(a_1\xi_1 + \dots + a_n\xi_n)$. В частности, такое представление будут иметь элементы $\alpha\xi_1, \dots, \alpha\xi_n \in (\alpha)A^p = (\beta)A^{p+q}$. Таким образом, полагая

$$\rho = \frac{\alpha}{\beta} \in K,$$

мы видим, что справедливы равенства вида

$$\begin{aligned} \rho \xi_1 &= a_{11}\xi_1 + \dots + a_{1n}\xi_n, \\ . &. \\ \rho \xi_n &= a_{n1}\xi_1 + \dots + a_{nn}\xi_n, \end{aligned}$$

где a_{ij} , $i, j = 1, \dots, n$, — целые рациональные числа. Применив к этим равенствам лемму 1, мы получим, что число ρ является корнем некоторого алгебраического уравнения n -й степени

$$(12) \quad X^n + a_1 X^{n-1} + \dots + a_n = 0$$

с целыми коэффициентами a_1, \dots, a_n и равным единице старшим коэффициентом.

Назовем кольцо D *целозамкнутым*, если любой элемент ρ его поля отношений K , удовлетворяющий уравнению вида (12), принадлежит D .

Таким образом, если D целозамкнуто, то $\rho = \frac{\alpha}{\beta} \in D$, т. е. β делит α .

Поэтому равенство (11) мы можем сократить на β и записать в следующем виде:

$$(\rho) A^p = A^{p+q}.$$

Пусть теперь $\gamma_1, \dots, \gamma_n$ — базис идеала A^q . Так как $\gamma_i \xi_j \in A^{p+q} = (\rho) A^p$, где $i, j = 1, \dots, n$, то при любом $i = 1, \dots, n$ для числа

$$\rho_i = \frac{\gamma_i}{\rho}$$

имеют место равенства вида

$$\begin{aligned}\rho_i^{\xi} \bar{s}_1 &= a_{i1}^{(i)} \bar{s}_1 + \dots + a_{in}^{(i)} \bar{s}_n, \\&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \rho_i^{\xi} \bar{s}_n &= a_{ni}^{(i)} \bar{s}_1 + \dots + a_{nn}^{(i)} \bar{s}_n,\end{aligned}$$

откуда, как и выше, следует, что ρ_i является корнем некоторого уравнения вида (12) и, значит (в силу целозамкнутости кольца D), лежит в D . Это означает, что γ_i делится на ρ .

Следовательно, на ρ делятся все числа идеала A^q . Сокращая их на ρ , мы, очевидно, получим некоторый новый идеал B (с базисом ρ_1, \dots, ρ_n). По построению $(\rho)B = A^q$ и, значит,

$$(\rho)A^p = A^{p+q} = (\rho)A^p B.$$

Но мы знаем, что в моноиде идеалов возможно сокращение равенств на главный идеал. Следовательно,

$$A^p = A^p B,$$

откуда, как мы знаем, следует, что $B = (1)$. Поэтому

$$A^q = (\rho).$$

Тем самым нами доказано следующее предложение:

Предложение 2. Если кольцо D , удовлетворяющее перечисленным выше условиям, кроме того, еще целостамкнуто, то некоторая степень любого идеала является главным идеалом. ■

Следствие. Для любого идеала A существует такой идеал A' , что произведение AA' является главным идеалом.

Действительно, достаточно положить $A' = A^{q-1}$. ■

Отсюда непосредственно вытекает ряд важных выводов.

Например, теперь легко показать, что закон сокращения справедлив для любых идеалов, т. е. если $CA = CB$, то $A = B$. Действительно, пусть C' — такой идеал, что $C'C = (\gamma)$. Тогда $(\gamma)A = C'(CA) = C'(CB) = (\gamma)B$, и, следовательно, $A = B$. ■

Далее, если $C \subset A$, то A делит C , т. е. существует такой идеал B , что $C = AB$. Действительно, если $C \subset A$, то $CA' \subset AA'$ для любого идеала A' . Если, в частности, идеал AA' главный, то, как мы выше уже доказали, существует такой идеал B , что $CA' = AA'B$. Сокращая на A' , мы и получим, что $C = AB$. ■

В частности, отсюда следует, что любой простой идеал P максимален, т. е. если $A \supset P$, то $A = (1)$.

Наконец, легко видеть, что элемент $\alpha \in D$ тогда и только тогда делится на идеал A (т. е. на A делится идеал (α)), когда $\alpha \in A$. Действительно, если (α) делится на A , то $(\alpha) \subset A$ и потому $\alpha \in A$. Обратно, если $\alpha \in A$, то $(\alpha) \subset A$ и, следовательно, по доказанному, (α) делится на A . ■

Последнее утверждение в точности означает, что для моноида идеалов (с отображением $\alpha \mapsto (\alpha)$) выполнена аксиома 3 теории дивизоров (см. § 8). Аксиома 2 также, очевидно, выполнена (если α и β делятся на A , то $\alpha \in A$, $\beta \in A$ и потому $\alpha \pm \beta \in A$, т. е. $\alpha \pm \beta$ делится на A). Выполнение аксиомы 1 мы выше уже отмечали.

Таким образом, для того чтобы показать, что моноид идеалов $\text{Id}(D)$ вместе с отображением $\alpha \mapsto (\alpha)$ составляет теорию дивизоров для кольца D , осталось лишь показать, что этот моноид свободен, т. е. что разложение любого идеала в произведение простых идеалов единственно (с точностью до порядка множителей).

Но это теперь также совсем просто.

Сначала докажем, что для любых двух идеалов A и B существует их наибольший общий делитель, т. е. идеал, который делит A и B и который делится на любой идеал, делящий идеалы A и B . Легко видеть, что таким идеалом будет идеал $(A \cup B)$, порожденный теоретико-множественным объединением идеалов A и B . Действительно, ясно, что $A \subset (A \cup B)$ и $B \subset (A \cup B)$, т. е. $(A \cup B)$ делит A и B . Если же C делит A и B , т. е. $C \supset A$ и $C \supset B$, то $C \supset A \cup B$ и потому $C \supset (A \cup B)$, т. е. C делит $(A \cup B)$.

Мы будем идеал $(A \cup B)$ обозначать символом (A, B) .

Эта конструкция показывает, в частности, что любой идеал $A = (\alpha_1, \dots, \alpha_k)$ является наибольшим общим делителем главных идеалов $(\alpha_1), \dots, (\alpha_k)$.

Легко видеть, далее, что для любых трех идеалов A, B и C справедливо равенство

$$(A, B)C = (AC, BC)$$

(дистрибутивность наибольшего общего делителя по отношению к умножению).

Действительно, если $A = (\alpha_1, \dots, \alpha_p)$, $B = (\beta_1, \dots, \beta_q)$, то $(A, B) = (\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q)$, и потому $(A, B)C = (\alpha_1\gamma, \dots, \alpha_p\gamma, \beta_1\gamma, \dots, \beta_q\gamma)$, где γ пробегает идеал C (или какое-нибудь множество, порождающее этот идеал). Аналогично, $AC = (\alpha_1\gamma, \dots, \alpha_p\gamma)$, $BC = (\beta_1\gamma, \dots, \beta_q\gamma)$, и потому

$$(A, B)C = (AC, BC). \quad \blacksquare$$

Теперь мы уже можем непосредственно доказать однозначность разложения идеалов в произведение простых идеалов. Для этого, очевидно, достаточно доказать, что *если простой идеал P делит произведение AB , то он делит идеал B* (ср. со свойством $(*)$ в § 4). Но если P не делит A , то $(A, P) \neq P$ и потому $(A, P) = (1)$ (ибо P — простой, а значит, максимальный идеал). Следовательно,

$$B = (1)B = (A, P)B = (AB, PB),$$

и так как P делит AB и PB , то P делит B . ■

Таким образом, нами доказано, что в кольце D идеалы (ненулевые) обладают всеми свойствами, которые мы требуем от дивизоров. Это означает, что справедлива следующая теорема:

Теорема 1. Если

а) аддитивная группа кольца D является решеткой конечного ранга n ;

б) существуют n мономорфизмов $\alpha \mapsto \alpha^{(i)}, i=1, \dots, n$, кольца D в поле \mathbb{C} , обладающих тем свойством, что для любого $\alpha \in D$ все элементарные симметрические многочлены от $\alpha^{(1)}, \dots, \alpha^{(n)}$ являются целыми рациональными числами;

в) кольцо D целозамкнуто,
то это кольцо допускает теорию дивизоров.

В этой теории дивизорами являются ненулевые идеалы кольца D , а соответствие $\alpha \mapsto (\alpha)$ относит каждому элементу $\alpha \in D^$ порожденный им главный идеал.*

При этом группа классов дивизоров (идеалов) конечна.

Последнее утверждение является простой переформулировкой предложения 1 и следствия из предложения 2.

Так как кольцо D_1 тривиальным образом обладает свойствами а) и б), то, если мы докажем, что оно обладает и свойством в), от требований, которые мы в § 8 наложили на регулярные простые числа, останется только аксиома P . При этом, пользуясь конечностью группы \mathcal{H} , мы эту аксиому сможем сформулировать в ослабленной форме, требуя лишь, чтобы число l не делило порядка h группы \mathcal{H} . Все это, конечно, будет большим сдвигом в направлении эффективной характеристики регулярных простых чисел.

Мы докажем целозамкнутость кольца D_1 в следующем параграфе, а пока лишь заметим, что условие в) целозамкнутости отличается от условий а) и б) (вообще говоря, не необходимых для существования в кольце D теории дивизоров) тем, что оно абсолютно необходимо. Другими словами, *в нецелозамкнутом кольце D теории дивизоров существовать не может.*

Действительно, если элемент $\xi = \frac{\beta}{\alpha}$ поля отношений K кольца D , обладающего теорией дивизоров, не лежит в D , то существует простой дивизор \mathfrak{p} , делящий α в большей степени, чем β , т. е. такой, что если β делится на \mathfrak{p}^k и не делится на \mathfrak{p}^{k+1} , то α делится на \mathfrak{p}^{k+1} . Поэтому, если $\xi^n + a_1\xi^{n-1} + \dots + a_n = 0$, где a_1, \dots, a_n — целые числа, т. е. если

$$\beta^n = -(a_1\beta^{n-1}\alpha + \dots + a_s\beta^{n-s}\alpha^s + \dots + a_n\alpha^n),$$

то β^n делится на \mathfrak{p}^{kn+1} (ибо $kn+1 \leq (n-s)k + s(k+1)$ для любого $s = 1, \dots, n$ и потому на \mathfrak{p}^{kn+1} делится каждый слагаемый вида $\beta^{n-s}\alpha^s$). Следовательно, β делится на \mathfrak{p}^i , где $i > k + \frac{1}{n}$, т. е., вопреки предположению, делится по крайней мере на \mathfrak{p}^{k+1} . ■

Таким образом, единственного условия теоремы 1, которое для кольца D_1 трудно проверить, избежать нельзя.

§ 11. Целые алгебраические числа

Мы уже неоднократно встречали уравнения вида

$$(1) \quad X^n + a_1X^{n-1} + \dots + a_n = 0,$$

где a_1, \dots, a_n — целые рациональные числа. Корни таких уравнений называются *целыми алгебраическими числами.*

Просто же *алгебраическими числами* (подразумевается, необязательно целыми) называются корни уравнений более общего вида

$$(2) \quad a_0X^n + a_1X^{n-1} + \dots + a_n = 0,$$

где также a_0, a_1, \dots, a_n — целые рациональные числа.

Ясно, что класс алгебраических чисел не изменится, если в уравнении (2) считать коэффициенты a_0, a_1, \dots, a_n произвольными рациональными числами. Это означает, что алгебраические числа, как мы их определили, являются ни чем иным, как числами, алгебраическими *над полем* \mathbb{Q} (см., например, Постников М. М. Теория Галуа. — М.: Физматгиз, 1963, стр. 11).

Заметим, что аналогичное расширение класса уравнений (1) приводит к уравнениям (2).

Разлагая левую часть уравнения (2) на множители и отбирая множитель, корнем которого является число α , мы получим, что *любое алгебраическое число является корнем некоторого неприводимого многочлена с рациональными коэффициентами*. Без ограничения общности можно считать, что старший коэффициент этого многочлена равен 1.

Пусть α является целым числом, т. е. корнем уравнения (1). По лемме Гаусса (см. § 4) левая часть уравнения (1) разлагается в произведение неприводимых (над полем \mathbb{Q}) многочленов с целыми коэффициентами. Так как старшие коэффициенты этих многочленов равны ± 1 (их произведение равно 1), то, следовательно, *неприводимый многочлен $h(X)$, корнем которого является целое алгебраическое число α и старший коэффициент которого равен 1, имеет целые коэффициенты*.

В частности, отсюда следует, что *целое алгебраическое число тогда и только тогда рационально, когда оно лежит в \mathbb{Z}* . Действительно, многочлен $h(X)$ для такого числа имеет степень 1. ■

Умножив уравнение (2) на a_0^{n-1} , мы можем переписать его в виде

$$(a_0 X)^n + a_1 (a_0 X)^{n-1} + \dots + a_n a_0^{n-1} = 0.$$

Таким образом, для $Y = a_0 X$ мы имеем уравнение вида (1). Этим доказано, что *любое алгебраическое число ξ может быть представлено в виде*

$$\xi = \frac{\alpha}{a},$$

где α — целое алгебраическое, а a — целое рациональное число.

Можно показать, что сумма, разность, произведение и частное двух алгебраических чисел являются алгебраическими числами, т. е., иными словами, что *все алгебраические числа образуют поле*. Концептуальное («в современном духе») доказательство этого факта можно найти, например, в упомянутой выше «Теории Галуа» на стр. 24. Здесь мы приведем более непосредственное доказательство, требующее зато некоторых вычислений.

Пусть α и β — алгебраические числа. По определению, число α является корнем некоторого уравнения вида (2). Пусть

$$(3) \quad \alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$$

— все корни этого уравнения. Аналогично, пусть

$$(4) \quad \beta_1 = \beta, \beta_2, \dots, \beta_m$$

— все корни уравнения

$$b_0 X^m + b_1 X^{m-1} + \dots + b_m = 0,$$

которому удовлетворяет число β (степень m этого уравнения, вообще говоря, отлична от степени n уравнения, которому удовлетворяет число α).

Рассмотрим многочлен

$$F(X) = \prod_{i=1}^n \prod_{j=1}^m (X - \alpha_i \beta_j).$$

степени mn . Его коэффициенты являются многочленами с целыми коэффициентами от корней (3) и (4), очевидно, симметрическими, т. е. не меняющимися при любой перестановке этих корней. Поэтому они являются многочленами от соответствующих элементарных симметрических многочленов и, следовательно, согласно формулам Вьета, — многочленами (с целыми коэффициентами) от

$$\frac{a_1}{a_0}, \dots, \frac{a_m}{a_0}, \frac{b_1}{b_0}, \dots, \frac{b_m}{b_0}.$$

Это доказывает, что все коэффициенты многочлена F являются рациональными числами. Значит, все его корни $\alpha_i \beta_j$ и, в частности, корень $\alpha\beta = \alpha_1 \beta_1$ являются алгебраическими числами.

Этим наше утверждение доказано в отношении произведения $\alpha\beta$. Для суммы, разности и частного доказательство аналогично. ■

Это доказательство устанавливает также и другой факт, для нас очень важный. Именно, при $a_0 = b_0 = 1$ мы видим, что все коэффициенты многочлена G (старший коэффициент которого по построению равен единице) будут целыми числами. Ясно, что это заключение сохранится и по отношению к сумме и разности (но не по отношению к частному!). Этим доказано, что сумма, разность и произведение двух целых алгебраических чисел являются целыми алгебраическими числами, т. е. что *все целые алгебраические числа составляют кольцо*.

Однако арифметика этого кольца малоинтересна. Например, в нем совсем нет неразложимых (простых) элементов. Действительно, любое целое алгебраическое число α может быть разложено, например, по формуле

$$\alpha = \sqrt{\alpha} \sqrt{\alpha}$$

(легко видеть, что $\sqrt{\alpha}$ также является целым алгебраическим числом). Поэтому класс всех целых алгебраических чисел следует как-то ограничить.

Подполе K поля комплексных чисел называется полем *конечной степени*, если как линейное пространство над полем \mathbb{Q} оно имеет конечную размерность (которая называется *степенью* поля K).

Заметим, что в общей алгебре поля конечной степени называются «конечными расширениями» поля \mathbb{Q} .

Легко видеть, что *каждый элемент поля конечной степени является алгебраическим числом*. Действительно, если степень поля равна n , то для любого его элемента ξ элементы $1, \xi, \dots, \xi^n$ линейно зависимы (ибо их $n + 1$ штук), и, значит, имеет место равенство

$$c_0 \xi^n + c_1 \xi^{n-1} + \dots + c_n = 0$$

с рациональными коэффициентами. ■

На этом основании поля конечной степени называются также *полями алгебраических чисел*, хотя этот термин несколько двусмыслен, поскольку он не предусматривает обязательно конечность степени.

Подробному исследованию взаимоотношений между конечными и алгебраическими расширениями посвящена гл. I указанной выше «Теории Галуа».

Пусть K — произвольное поле алгебраических чисел (конечной степени). Ясно, что его подмножество D , состоящее из всех целых чисел поля K , является кольцом. Это кольцо называется *кольцом целых чисел* поля K . Арифметика таких колец и составляет содержание теории целых алгебраических чисел.

Так как (см. выше) любой элемент $\xi \in K$ имеет вид $\xi = \frac{\alpha}{a}$, где α — целое алгебраическое число (и, значит, — элемент кольца D), а a — целое рациональное число (и, значит, — тоже элемент D), то K является *полем отношений кольца D* .

По определению (см. стр. 120) кольцо D целозамкнуто, если оно содержит все целые алгебраические числа, содержащиеся в его поле отношений K . Если D является кольцом целых чисел некоторого поля K алгебраических чисел (которое, следовательно, является его полем отношений), то дело обстоит именно так. Следовательно, *кольцо D целых чисел произвольного поля алгебраических чисел K целозамкнуто*.

Вернемся теперь к l -круговому полю K_l и его подкольцу D_l . Поле K_l является, конечно, полем конечной степени (равной $l-1$), и потому к нему применимо все сказанное выше. В частности, его кольцо целых чисел D целозамкнуто. Поэтому для доказательства целозамкнутости кольца D_l достаточно доказать, что $D = D_l$.

Доказательство включения $D_l \subset D$. Достаточно заметить, что любой элемент $\alpha \in D_l$ является корнем многочлена

$$(5) \quad f(X) = (X - \alpha^{(1)}) \dots (X - \alpha^{(l-1)})$$

с целыми рациональными коэффициентами, старший коэффициент которого равен 1. ■

Многочлен (5) определен, конечно, для любого элемента $\alpha \in K_l$. Его свободный член совпадает с нормой $N\alpha$ числа α . Другой интересный коэффициент — это коэффициент при X^{l-2} . Взятый с обратным знаком, он называется *следом* элемента α и обозначается символом $\text{Tr } \alpha$. Согласно первой формуле Вьета,

$$\text{Tr } \alpha = \alpha^{(1)} + \dots + \alpha^{(l-1)}.$$

Отсюда следует, что след обладает свойством линейности, т. е.

$$\text{Tr}(\alpha + \beta) = \text{Tr} \alpha + \text{Tr} \beta, \quad \text{Tr}(a\alpha) = a \text{Tr} \alpha$$

для любых чисел $\alpha, \beta \in K_l$ и любого рационального числа $a \in \mathbb{Q}$.

Изучим более внимательно многочлен (5). В следующих ниже леммах

$$(6) \quad \alpha = a_0 + a_1 \xi + \dots + a_{l-1} \xi^{l-2} = a(\xi)$$

— произвольное число поля K_l .

Л е м м а 1. Если многочлен $g(X)$ с рациональными коэффициентами обладает тем свойством, что $g(\alpha^{(i)}) = 0$ хотя бы для одного $i = 1, \dots, l-1$, то

$$g(\alpha^{(i)}) = 0 \quad \text{для всех } i = 1, \dots, l-1.$$

Д о к а з а т е л ь с т в о. Рассмотрим многочлен

$$F(X) = g(a(X)).$$

По условию

$$F(\xi^{(i)}) = g(a(\xi^{(i)})) = g(\alpha^{(i)}) = 0$$

хотя бы для одного $i = 1, \dots, l-1$. Это означает, что многочлен $F(X)$ имеет общий корень с неприводимым многочленом

$$\varphi(X) = X^{l-1} + X^{l-2} + \dots + 1.$$

Следовательно, $F(X)$ делится на этот многочлен и потому $F(\xi^{(i)}) = 0$, т. е. $g(\alpha^{(i)}) = 0$, для любого $i = 1, \dots, l-1$. ■

Д р у г о е д о к а з а т е л ь с т в о. Пусть $1 \leq i_0, i \leq l-1$, и пусть τ — автоморфизм поля K_l , являющийся композицией автоморфизма, обратного к автоморфизму $\alpha \mapsto \alpha^{(i_0)}$, и автоморфизма $\alpha \mapsto \alpha^{(i)}$. Тогда $\tau(\alpha^{(i_0)}) = \alpha^{(i)}$, и потому $g(\alpha^{(i)}) = \tau g(\alpha^{(i_0)})$ для любого многочлена $g(X)$. Следовательно, если $g(\alpha^{(i_0)}) = 0$, то $g(\alpha^{(i)}) = 0$. ■

Л е м м а 2. Существует такое целое число q , что

$$f(X) = h(X)^q,$$

где $f(X)$ — многочлен (5), а $h(X)$ — неприводимый многочлен над полем \mathbb{Q} со старшим коэффициентом 1, корнем которого является алгебраическое число α .

Д о к а з а т е л ь с т в о. Так как $f(\alpha) = 0$, то $f(X)$ делится на $h(X)$. Пусть $f(X)$ делится на $h(X)^q$, но не

делится на $h(X)^{q+1}$, и пусть

$$f(X) = g(X)h(X)^q.$$

Если $g(X) \neq \text{const}$, то хотя бы один из корней $\alpha^{(i)}$, $i = 1, \dots, l-1$, многочлена $f(X)$ обращает $g(X)$ в нуль. Но тогда по лемме 1

$$g(\alpha^{(i)}) = 0 \quad \text{для любого } i = 1, \dots, l-1$$

и, в частности, $g(\alpha) = g(\alpha^{(1)}) = 0$. Таким образом, многочлен $g(X)$ имеет общий корень с неприводимым многочленом $h(X)$ и, значит, делится на $h(X)$. Поэтому многочлен $f(X)$ делится на $h(X)^{q+1}$. Полученное противоречие доказывает, что $g(X) = \text{const}$, т. е. что $f(X) = h(X)^q$ (ибо старшие коэффициенты многочленов $f(X)$ и $h(X)$ равны 1). ■

Лемма 3. Если α является целым алгебраическим числом, то все коэффициенты многочлена $f(X)$ представляют собой целые рациональные числа.

Доказательство. Как мы знаем, неприводимый (над \mathbb{Q}) многочлен $h(X)$, корнем которого является α и старший коэффициент которого равен 1, имеет целые коэффициенты. Поэтому многочлен $f(X) = h(X)^q$ также имеет целые коэффициенты. ■

Следствие. След $\text{Tr } \alpha$ любого целого алгебраического числа $\alpha \in K_l$ является целым рациональным числом.

Полезно заметить, что изложенные соображения имеют весь общий характер.

Пусть θ — произвольное целое алгебраическое число. Пусть оно является корнем неприводимого уравнения степени n . Тогда можно показать (ср. § 5), что совокупность K всех чисел вида

$$(7) \quad a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1},$$

где a_0, a_1, \dots, a_{n-1} — произвольные рациональные числа, является полем (очевидно, степени n). Оно обозначается символом $\mathbb{Q}(\theta)$. Все предыдущие рассуждения, относящиеся к полю K_l , остаются в силе и для любого поля $\mathbb{Q}(\theta)$ (если, конечно, заменить $l-1$ на n и ξ на θ). В частности, след любого целого алгебраического числа из $\mathbb{Q}(\theta)$ будет целым рациональным числом.

Аналогом кольца D_l будет кольцо $\mathbb{Z}[\theta]$ всех чисел вида (7) с целыми a_0, a_1, \dots, a_{n-1} . Очевидно, что все эти числа являются целыми алгебраическими числами, т. е. что имеет место включение $\mathbb{Z}[\theta] \subset D$, где D — кольцо целых чисел поля $K = \mathbb{Q}(\theta)$.

Эти замечания особо интересны потому, что любое поле конечной степени имеет вид $\mathbb{Q}(\theta)$ (см., например, «Теория Галуа», гл. I, п. 7).

Теперь мы уже можем доказать обратное включение.

Доказательство включения $D_l \supset D$. Надо доказать, что если элемент (6) поля K_l является целым алгебраическим числом, то все его коэффициенты a_0, a_1, \dots, a_{l-2} будут целыми рациональными числами.

С этой целью вычислим сначала след $\text{Tr } \alpha$ числа α (который, согласно следствию из леммы 2, является целым рациональным числом).

Если $\alpha = \xi^k$, где $k = 1, \dots, l-1$, то числа $\alpha^{(1)}, \dots, \alpha^{(l-1)}$ будут с точностью до порядка совпадать с числами $\xi^{(1)}, \dots, \xi^{(l-1)}$ (см. § 5) и, значит, будет иметь место равенство

$$\text{Tr } \xi^k = -1, \quad k = 1, \dots, l-1$$

(ибо по формуле Вьета сумма корней $\xi^{(1)} + \dots + \xi^{(l-1)}$ многочлена $X^{l-1} + X^{l-2} + \dots + 1$ равна -1). Если же $k = 0$, то $\text{Tr } \xi^k = l-1$.

Отсюда, в силу линейности следа, вытекает, что след числа (6) выражается формулой

$$\text{Tr } \alpha = (l-1)a_0 - a_1 - \dots - a_{l-2}.$$

Аналогичным способом вычисляется, что для любого $k = 0, \dots, l-2$

$$\text{Tr } (\xi^{-k}\alpha - \xi\alpha) = la_k.$$

Поскольку $\xi^{-k}\alpha - \xi\alpha$ является вместе с α целым алгебраическим числом (принадлежит кольцу D), этим доказано, что все числа la_k , $k = 0, \dots, l-2$, являются целыми рациональными числами.

Следовательно, $l\alpha \in D_l$ и потому

$$(8) \quad l\alpha = b_0 + b_1\lambda + \dots + b_{l-2}\lambda^{l-2}, \quad \lambda = 1 - \xi,$$

где b_0, b_1, \dots, b_{l-2} — целые числа (см. формулу (15) § 5).

Для завершения доказательства достаточно теперь показать, что все коэффициенты b_0, b_1, \dots, b_{l-2} делятся на l . Условно полагая $b_{-1} = 0$, проведем индукцию по k от $k = -1$ до $k = l-2$.

Пусть для некоторого k , $0 \leq k < l-2$, уже доказано, что все коэффициенты b_s с $s \leq k$ делятся на l .

Тогда в (8) все члены, кроме члена $b_k \lambda^k$, будут делиться на λ^{k+1} (ибо $l \sim \lambda^{l-1}$, см. формулу (14) § 5). Следовательно, и член $b_k \lambda^k$ будет делиться на λ^{k+1} , т. е. целое рациональное число b_k будет делиться на λ . Значит, число b_k делится и на l . ■

Заметим, что это доказательство существенно использует специфику поля K_l . Не удивительно поэтому, что аналог равенства $D_l = D$ в произвольном поле алгебраических чисел $\mathbb{Q}(\theta)$, вообще говоря, неверен, т. е. существуют поля $\mathbb{Q}(\theta)$, в которых имеются целые числа

$$a_0 + a_1 \theta + \dots + a_{n-1} \theta^{n-1}$$

с нецелыми коэффициентами a_0, a_1, \dots, a_{n-1} .

Рассмотрим, например, поле $\mathbb{Q}(\sqrt{-3})$. Из данного в § 4 описания поля K_3 следует, что поле $\mathbb{Q}(\sqrt{-3})$ совпадают с полем K_3 , и потому его целые числа имеют вид

$$\frac{a + b \sqrt{-3}}{2},$$

где a и b — целые рациональные числа одинаковой четности.

Однако можно без особого труда доказать (попытайтесь!), что для любого поля K конечной степени n аддитивная группа его кольца D целых элементов является решеткой ранга n , т. е. существуют такие целые числа $\omega_1, \dots, \omega_n$, что любое целое число $\alpha \in D$ единственным образом представляется в виде

$$a_1 \omega_1 + \dots + a_n \omega_n,$$

где a_1, \dots, a_n — целые числа. (Принято говорить, что $\omega_1, \dots, \omega_n$ составляют *фундаментальный базис* поля K .)

Например, при $K = \mathbb{Q}(\sqrt{-3})$ фундаментальный базис состоит из чисел $1, \frac{1 + \sqrt{-3}}{2}$.

Факт наличия фундаментального базиса означает, что кольцо D обладает свойством а) из теоремы 1 § 10. Как мы уже отмечали, оно автоматически обладает свойством в). Кроме того, нетрудно видеть (это мы фактически выше уже доказали), что оно обладает и свойством б). Поэтому *кольцо целых чисел произвольного поля алгебраических чисел обладает теорией ди-*

визоров, причем соответствующая группа классов дивизоров конечна.

Это утверждение является фундаментом всей теории алгебраических чисел.

Доказательство равенства $D = D_l$ завершает доказательство того, что простое число l тогда и только тогда регулярно, когда оно не делит числа h классов дивизоров кольца D_l .

§ 12. Куммеровы простые числа

Наша дальнейшая цель будет состоять в доказательстве того, что регулярные числа совпадают с куммеровыми. Эта теорема очень трудна и ее доказательство разбивается на две части: алгебро-арифметическую и аналитическую. В этом параграфе мы займемся более простой — первой частью. Окончательно же мы завершим доказательство теоремы только в § 15.

Мы рассмотрим также вопрос об объеме понятия регулярного (скрывающегося пока под псевдонимом куммерова) простого числа и найдем простой критерий, позволяющий для любого простого числа l автоматически вычислениями проверить регулярно оно или нет. Кроме того, мы докажем, что условие К из § 6 выполнено на самом деле для всех простых чисел l , и потому в теореме 3 § 9 о нем можно не упоминать.

Пусть θ — произвольный первообразный корень из единицы степени $l - 1 = 2m$, например

$$\theta = \cos \frac{\pi}{m} + i \sin \frac{\pi}{m}.$$

Особое значение для нас будут иметь степени

$$(1) \quad \theta, \theta^3, \dots, \theta^{2m-1}$$

числа θ с нечетными показателями. Ясно, что $\theta^m = -1$, и потому $\theta^{(2k+1)m} = -1$ для любого k . Это означает, что числа (1) являются корнями многочлена $X^m + 1$, а так как их m и все они различны, то никаких других корней этот многочлен не имеет. Этим доказано, что

$$(2) \quad (X - \theta)(X - \theta^3) \dots (X - \theta^{2m-1}) = X^m + 1.$$

Отсюда следует, что любой симметрический многочлен от $\theta, \theta^3, \dots, \theta^{2m-1}$ с целыми коэффициентами

является целым рациональным числом (лежит в \mathbb{Z}). В частности, это верно для числа

$$W(a) = a(\theta) a(\theta^3) \dots a(\theta^{2m-1}),$$

где $a = a(X)$ — произвольный многочлен с целыми коэффициентами.

Пусть теперь, как всегда, g — фиксированный первообразный корень по модулю l , удовлетворяющий условию (6) § 6 (и, следовательно, такой, что $g^m + 1 \not\equiv 0 \pmod{l}$).

Предложение 1. Для любого многочлена $a(X)$ с коэффициентами из \mathbb{Z} имеет место сравнение

$$W(a) \equiv a(g) a(g^3) \dots a(g^{2m-1}) \pmod{l}.$$

Доказательство. Пусть

$$a(X_1) a(X_2) \dots a(X_m) = F(\sigma_1, \dots, \sigma_m),$$

где $\sigma_1, \dots, \sigma_m$ — элементарные симметрические многочлены от X_1, X_2, \dots, X_m , а F — некоторый многочлен. Согласно (2) (и формулам Вьета) значения $\sigma_1^{(\theta)}, \dots, \sigma_m^{(\theta)}$ многочленов $\sigma_1, \dots, \sigma_m$ при $X_1 = \theta, X_2 = \theta^3, \dots, X_m = \theta^{2m-1}$ все равны нулю, кроме последнего $\sigma_m^{(\theta)}$, которое равно $(-1)^m$. Поэтому

$$W(a) = F(0, \dots, 0, (-1)^m).$$

С другой стороны,

$$a(g) a(g^3) \dots a(g^{2m-1}) = F(\sigma_1^{(g)}, \dots, \sigma_m^{(g)}),$$

где $\sigma_1^{(g)}, \dots, \sigma_m^{(g)}$ — значения симметрических многочленов $\sigma_1, \dots, \sigma_m$ при $X_1 = g, X_2 = g^3, \dots, X_m = g^{2m-1}$. Но числа g, g^3, \dots, g^{2m-1} и, с точностью до сравнимости, только эти числа являются корнями сравнения $X^m + 1 \equiv 0 \pmod{l}$. Поэтому (по тем же формулам Вьета)

$$\sigma_1^{(g)} \equiv 0, \dots, \sigma_{m-1}^{(g)} \equiv 0, \quad \sigma_m^{(g)} \equiv (-1)^m \pmod{l}.$$

Следовательно,

$$F(\sigma_1^{(g)}, \dots, \sigma_m^{(g)}) \equiv F(0, \dots, 0, (-1)^m) \pmod{l}.$$

Это доказывает предложение 1. ■

Мы применим это предложение к многочлену $\psi(X)$, определенному (см. формулу (15) § 6) формулой

$$(3) \quad \varpi(X)(gX - 1) = X^{l-1} - 1 + l\psi(X),$$

где

$$\varpi(X) = 1 + g_1X + \dots + g_{l-2}X^{l-2}.$$

С л е д с т в и е. Число l тогда и только тогда куммерово (см. § 6), когда оно не делит числа

$$W(\psi) = \psi(\theta)\psi(\theta^3) \dots \psi(\theta^{2m-1}).$$

Д о к а з а т е л ь с т в о. По определению число l куммерово, если оно не делит число $\psi(g)\psi(g^3) \dots \psi(g^{2m-1})$. Но согласно предложению 1 последнее число сравнимо по модулю l с числом $W(\psi)$. ■

Удобно, впрочем, перейти от многочлена ψ к более простому многочлену ϖ .

Поскольку $\theta^{k(l-1)} = 1$, из формулы (3) следует, что

$$\varpi(\theta^k)(g\theta^k - 1) = l\psi(\theta^k)$$

для любого $k = 1, 3, \dots, 2m-1$. Поэтому

$$l^m W(\psi) = W(\varpi) \cdot \Pi,$$

где

$$\Pi = (g\theta - 1)(g\theta^3 - 1) \dots (g\theta^{2m-1} - 1).$$

Но, положив в (2) $X = g^{-1}$, мы после умножения на g^m получим, что

$$\Pi = 1 + g^m.$$

Этим доказано, что

$$(4) \quad l^m W(\psi) = W(\varpi)(1 + g^m).$$

По условию (см. выше) делящееся на l число $1 + g^m$ не делится на l^2 . Поэтому из (4) следует, во-первых, что целое число $W(\varpi)$ делится на l^{m-1} и, во-вторых, что число l тогда и только тогда куммерово, когда это число не делится на l^m .

Так как для любого $j = 0, 1, \dots, m-1$ имеет место сравнение

$$g_{m+j} + g_j \equiv g^{m+j} + g^j \equiv g^j(g^m + 1) \equiv 0 \pmod{l}$$

и так как $0 < g_{m+j} < l$ и $0 < g_j < l$, то $g_{m+j} + g_j = l$.

В частности, это доказывает, что для любого $j = 0, 1, \dots, m-1$ разность $g_j - g_{m+j}$ нечетна.

С другой стороны, для любого $k = 1, 3, \dots, 2m-1$

$$\begin{aligned}\bar{\omega}(\theta^k) &= \sum_{j=0}^{2m+1} g_j \theta^{kj} = \sum_{j=0}^{m-1} (g_j \theta^{kj} + g_{m+j} \theta^{k(m+j)}) = \\ &= \sum_{j=0}^{m-1} (g_j - g_{m+j}) \theta^{kj},\end{aligned}$$

ибо $\theta^m = -1$. Поэтому

$$\bar{\omega}(\theta^k) = \sum_{j=0}^{m-1} \theta^{kj} + 2a_k(\theta),$$

где $a_k(X)$ — некоторый многочлен с целыми коэффициентами.

Поскольку $(1 + \theta^k + \dots + \theta^{k(m-1)})(1 - \theta^k) = 1 - \theta^{km} = 2$, отсюда следует, что

$$(1 - \theta^k) \bar{\omega}(\theta^k) = 2b_k(0),$$

где $b_k(X) = 1 + (1 - X^k)a_k(X)$ — также многочлен с целыми коэффициентами. Перемножив эти соотношения и учтя, что, согласно (2),

$$(1 - \theta)(1 - \theta^3) \dots (1 - \theta^{2m-1}) = 1^m + 1 = 2,$$

мы после сокращения на 2 получим, что

$$(5) \quad W(\bar{\omega}) = 2^{m-1} B(\theta),$$

где $B(X)$ — некоторый многочлен с целыми коэффициентами.

Поскольку многочлен $B(X)$ имеет целые коэффициенты, число $B(\theta)$ является целым алгебраическим числом (ибо число θ — целое). С другой стороны, согласно формуле (5) оно рационально. Следовательно, $B(\theta)$ представляет собой целое рациональное число (лежит в \mathbb{Z}). Этим доказано, что число $W(\bar{\omega})$ делится на 2^{m-1} .

Так как $l > 2$, то число $W(\bar{\omega})$, делясь на 2^{m-1} и l^{m-1} , делится и на $(2l)^{m-1}$. Это означает, что число

$$(6) \quad h_1 = \frac{|W(\bar{\omega})|}{(2l)^{m-1}}$$

является целым рациональным числом. Оно называется *первым множителем*.

Согласно сказанному выше число l тогда и только тогда куммерово, когда первый множитель h_1 не делится на l . ■

Рассмотрим теперь произведение $h_1 h_2$, где h_2 — второй множитель, введенный в § 6. Согласно предложению 6 § 6, если число l куммерово (и потому не делит h_1), то h_2 не делится на l . Следовательно, $h_1 h_2$ не делится на l . Обратно, пусть $h_1 h_2$ не делится на l . Тогда h_1 не делится на l , и потому число l куммерово. Этим доказано следующее предложение:

Предложение 2. Число l тогда и только тогда куммерово, когда оно не делит произведение $h_1 h_2$.

Эта характеристика куммеровых чисел вполне аналогична характеристике регулярных чисел из § 11, только роль числа h играет произведение $h_1 h_2$. Поэтому для доказательства совпадения куммеровых и регулярных простых чисел достаточно доказать, что $h = h_1 h_2$. Доказательство этого равенства (известного как формула Куммера для числа классов) составит предмет трех следующих параграфов. Пока же мы обратимся к исследованию объема понятия куммерова числа и установим так называемый критерий Куммера регулярности (на самом деле куммеровости) простого числа l . Это доказательство никак не связано со всем предыдущим и опирается исключительно на первоначальное (см. § 6) определение куммерова числа l как числа, не делящего ни одно из чисел

$$(7) \quad \psi(g), \psi(g^3), \dots, \psi(g^{2m-3}).$$

(Напомним — см. формулу (16) § 6, — что при нашем выборе первообразного корня g число $\psi(g^{2m-1}) = \psi(g^{l-1})$ на l не делится.)

Поскольку $g^l \equiv \bar{g} \pmod{l}$, вместо чисел (7) мы можем рассматривать сравнимые с ними по модулю l числа

$$(8) \quad \psi(g^l), \psi(g^{3l}), \dots, \psi(g^{(2m-3)l}).$$

С другой стороны, так как $g^{l-1} = 1 + al$, то $g^{(l-1)l} \equiv (1 + al)^l \equiv 1 \pmod{l^2}$, откуда следует, что, положив в тождестве (3) $X = g^{kl}$, мы получим сравнение

$$\mathfrak{B}(g^{kl})(g^{kl+1} - 1) \equiv l\psi(g^{kl}) \pmod{l^2}.$$

Поскольку $g^{kl+1} \equiv g^{k+1} \not\equiv 1 \pmod{l}$ при $k = 1, 3, \dots, 2m-3$, тем самым доказано, что число l тогда и

только тогда не делит ни одного из чисел (8) (и, значит, ни одного из чисел (7)), когда ни одно из чисел (9)

$$\varpi(g^l), \varpi(g^{3l}), \dots, \varpi(g^{(2m-3)l})$$

не делится на l^2 . ■

Так как $g \equiv g^l \pmod{l}$, то $g_s \equiv g^{ls} \pmod{l}$ для любого $s = 0, 1, \dots, l-2$, т. е.

$$g_s = g^{sl} + la_s,$$

где a_s — некоторые целые числа. Поэтому для любого $k = 1, 3, \dots, 2m-3$

$$\begin{aligned} g_s^{k+1} &= (g^{sl} + la_s)^{k+1} \equiv g^{s(k+1)l} + (k+1)la_s g^{skl} \equiv \\ &\equiv g^{s(k+1)l} + (k+1)(g_s - g^{sl})g^{skl} \equiv \\ &\equiv (k+1)g_s g^{skl} - k g^{s(k+1)l} \pmod{l^2}. \end{aligned}$$

Просуммировав по s от 0 до $l-2$, мы получим отсюда сравнение

$$\sum_{s=0}^{l-2} g_s^{k+1} \equiv (k+1) \sum_{s=0}^{l-2} g_s g^{skl} - k \sum_{s=0}^{l-2} g^{s(k+1)l} \pmod{l^2},$$

т. е. сравнение

$$\sum_{s=0}^{l-2} g_s^{k+1} \equiv (k+1) \varpi(g^{kl}) - k \sum_{s=0}^{l-2} g^{s(k+1)l} \pmod{l^2}.$$

Но (см. выше)

$$\begin{aligned} (1 - g^{(k+1)l}) \sum_{s=0}^{l-2} g^{s(k+1)l} &= 1 - g^{(l-1)(k+1)l} = \\ &= 1 - (g^{(l-1)l})^{k+1} \equiv 0 \pmod{l^2}, \end{aligned}$$

а так как $1 - g^{(k+1)l} \equiv 1 - g^{k+1} \not\equiv 0 \pmod{l}$, то

$$\sum_{s=0}^{l-2} g^{s(k+1)l} \equiv 0 \pmod{l^2}.$$

Поэтому

$$\sum_{s=0}^{l-2} g_s^{k+1} \equiv (k+1) \varpi(g^{kl}) \pmod{l^2}.$$

С другой стороны, так как числа g_0, g_1, \dots, g_{l-2} с точностью до порядка совпадают с числами $1, 2, \dots, l-1$, то, введя обозначение

$$(10) \quad S_n(a) = 1^n + 2^n + \dots + (a-1)^n,$$

получим, что

$$\sum_{s=0}^{l-2} g_s^{k+1} = S_{k+1}(l).$$

Тем самым, доказано, что

$$(k+1) \mathfrak{D}(g^{kl}) \equiv S_{k+1}(l) \pmod{l^2}$$

для любого $k = 1, 3, \dots, 2m-1$.

Так как $k+1 \not\equiv 0 \pmod{l}$, отсюда следует, что число l куммерово тогда и только тогда, когда ни одно из чисел

$$(11) \quad S_2(l), S_4(l), \dots, S_{2m-2}(l)$$

не делится на l^2 . ■

Этот критерий можно переформулировать в более удобном виде с помощью так называемых чисел Бернулли.

Лемма 1. Для любого многочлена $f(X)$ существует единственный многочлен $g(X)$ той же степени, удовлетворяющий соотношению

$$f(X) = \int_X^{X+1} g(t) dt.$$

Коэффициенты этого многочлена рациональны, если рациональны коэффициенты многочлена $f(X)$.

Доказательство. Пусть

$$y_n = \int_X^{X+1} t^n dt = \frac{(X+1)^{n+1} - X^{n+1}}{n+1}, \quad n = 0, 1, \dots$$

Ясно, что y_n представляет собой многочлен степени n от X со старшим коэффициентом, равным единице. Поэтому для любого многочлена $f(X) = a_0 X^n + \dots$ от X степени n разность $f(X) - a_0 y_n$ будет многочленом степени $n-1$. Посредством очевидной индукции отсюда выводится, что многочлен $f(X)$ единственным образом представляется в виде линейной комбинации

$$f(X) = a_0 y_n + a_1 y_{n-1} + \dots + a_n y_0$$

многочленов y_n, y_{n-1}, \dots, y_0 . Поэтому

$$f(X) = \int_X^{X+1} g(t) dt,$$

где

$$g(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n. \quad \blacksquare$$

С л е д с т в и е. Для любого $n \geq 0$ существует единственный многочлен $B_n(X)$, удовлетворяющий соотношению

$$(12) \quad \int_X^{X+1} B_n(t) dt = X^n.$$

Коэффициенты этого многочлена являются рациональными числами. \blacksquare

Свободный член $B_n = B_n(0)$ многочлена $B_n(X)$ называется n -м числом Бернулли.

Продифференцировав соотношение (12), мы получим равенство

$$(13) \quad B_n(X+1) - B_n(X) = nX^{n-1},$$

которое можно переписать в виде

$$\int_X^{X+1} \left(\frac{d}{dt} B_n(t) - nB_{n-1}(t) \right) dt = 0,$$

означающем, что многочлен

$$(14) \quad \frac{d}{dX} B_n(X) - nB_{n-1}(X)$$

является многочленом $g(X)$, отвечающим в силу леммы 1 многочлену $f(X)$, тождественно равному нулю. В силу единственности отсюда следует, что многочлен (14) также тождественно равен нулю. Таким образом,

$$\frac{d}{dX} B_n(X) = nB_{n-1}(X)$$

и, значит,

$$B_n(X) = n \int_0^X B_{n-1}(t) dt + B_n.$$

Это соотношение позволяет последовательно выразить все многочлены $B_n(X)$ через числа Бернулли.

Действительно, непосредственно очевидно, что $B_0 = 1$.
Поэтому

$$B_1(X) = 1 \int_0^X 1 \cdot dt + B_1 = X + B_1,$$

$$B_2(X) = 2 \int_0^X (t + B_1) dt + B_2 = X^2 + 2B_1X + B_2,$$

$$B_3(X) = 3 \int_0^X (t^2 + 2B_1t + B_2) dt + B_3 = \\ = X^3 + 3B_1X^2 + 3B_2X + B_3$$

и, вообще,

(15)

$$B_n(X) = X^n + nB_1X^{n-1} + \dots + \binom{n}{k} B_k X^{n-k} + \dots + B_n.$$

Действительно, если (15) имеет место для $B_{n-1}(X)$, то

$$B_n(X) = n \int_0^X (t^{n-1} + (n-1)B_1t^{n-2} + \dots \\ \dots + \binom{n-1}{k} B_k t^{n-k-1} + \dots + B_{n-1}) dt + B_n = \\ = X^n + nB_1X^{n-1} + \dots + \binom{n}{k} B_k X^{n-k} + \dots + B_{n-1}X + B_n,$$

ибо

$$\int_0^X t^{n-k-1} dt = \frac{1}{n-k-1} X^{n-k}$$

и

$$\frac{n}{n-k-1} \binom{n-1}{k} = \binom{n}{k}. \quad \blacksquare$$

С другой стороны, положив в (13) $X = 0$, мы получим, что при $n > 1$ имеет место равенство

$$(16) \quad B_n(1) = B_n(0),$$

т. е. равенство

$$1 + nB_1 + \dots + \binom{n}{k} B_k + \dots + nB_{n-1} + B_n = B_n.$$

Следовательно (мы заменяем $n - 1$ на n),

$$(17) \quad B_n = -\frac{1}{n+1} \left(1 + (n+1)B_1 + \dots \right. \\ \left. \dots + \binom{n+1}{k} B_k + \dots + \binom{n+1}{n-1} B_{n-1} \right).$$

Эта рекуррентная формула позволяет последовательно вычислить числа B_n , а значит, и многочлены $B_n(X)$.

Легко видеть, что *все числа Бернулли с нечетными индексами, большими единицы, равны нулю*:

$$B_{2k+1} = 0 \quad \text{при } k > 0.$$

Действительно, делая замену $\tau = 1 - t$, мы немедленно получаем, что

$$\int_X^{X+1} B_n(1-t) dt = - \int_{1-X}^{-X} B_n(\tau) d\tau = \int_{-X}^{1-X} B_n(\tau) d\tau = \\ = (-X)^n = (-1)^n X^n = (-1)^n \int_X^{X+1} B_n(t) dt,$$

откуда вытекает, что

$$B_n(1-X) = (-1)^n B_n(X).$$

Поэтому

$$B_n(1) = (-1)^n B_n(0),$$

и, значит (см. формулу (16)), если $n > 1$ нечетно, то $B_n = B_n(0) = 0$. ■

Что же касается числа B_1 , то, как непосредственно вытекает из формулы (17) при $n = 1$,

$$B_1 = -\frac{1}{2}.$$

Задача. Докажите, что знаки чисел Бернулли с четными индексами чередуются, т. е.

$$B_{2n} B_{2n+2} < 0 \quad \text{при } n \geq 1$$

Чтобы связать многочлены $B_n(X)$ с суммами степеней $S_n(a)$, мы, положив в (13) последовательно $X = 0, 1, \dots, a-1$, сложим получившиеся формулы. Тогда, очевидно, получится формула

$$B_n(a) - B_n(0) = n S_{n-1}(a),$$

т. е. формула

$$B_n(a) = nS_{n-1}(a) + B_n.$$

Тем самым мы получаем выражение

$$S_{n-1}(a) = \frac{B_n(a) - B_n}{n}$$

суммы $S_{n-1}(a)$ в виде многочлена от a степени n со свободным членом, равным нулю.

Заметим, что хотя коэффициенты многочленов $B_n(X) - B_n$ являются, вообще говоря, дробными числами, но при любом целом $X = a$ их значения представляют собой целые числа (и даже делящиеся на n).

Интересующие нас числа (11) мы можем теперь (имея в виду, что $2m - 1 = l - 2$) переписать в следующем виде:

$$\frac{B_3(l) - B_3}{3}, \quad \frac{B_5(l) - B_5}{5}, \quad \dots, \quad \frac{B_{l-2}(l) - B_{l-2}}{l-2}.$$

Впрочем, знаменатели 3, 5, ..., $l - 2$ этих чисел можно откинуть, поскольку они не делятся на l . Таким образом, нам достаточно рассмотреть числа

$$(18) \quad B_3(l) - B_3, B_5(l) - B_5, \dots, B_{l-2}(l) - B_{l-2}.$$

Число l куммерово тогда и только тогда, когда ни одно из этих чисел не делится на l^2 .

Рассмотрим теперь все простые делители знаменателей чисел Бернулли B_1, B_2, \dots, B_{n-1} . Согласно формуле (17) при добавлении к числам B_1, B_2, \dots, B_{n-1} числа B_n к этим делителям могут добавиться лишь простые делители числа $n + 1$, ни один из которых при $n + 1 < l$ не равен l . По индукции этим доказано, что *знаменатели чисел Бернулли*

$$(19) \quad B_1, B_2, B_4, \dots, B_{l-3}$$

не делятся на l . ■

Поэтому, умножив числа (18) на произведение знаменателей чисел (19), мы не изменим характера делимости этих чисел на l .

Но так как эти и только эти числа Бернулли участвуют в коэффициентах многочленов $B_k(X) - B_k$, $k \leq l - 2$, то после этого умножения числа (18) будут значениями при $X = l$ некоторых многочленов с целыми

коэффициентами (и без свободных членов). Поэтому тогда и только тогда ни одно из них не будет делиться на l^2 , когда в каждом из этих многочленов коэффициент при X не будет делиться на l . Поскольку, согласно формуле (15), этот коэффициент равен числу kB_{k-1} , где $k = 3, 5, \dots, l-2$, умноженному на знаменатели всех чисел (19), т. е. с точностью до множителей, не делящихся на l , равен числителю числа B_{k-1} , этим доказано следующее окончательное предложение:

Предложение 3 (критерий Куммера).
Простое число l тогда и только тогда куммерово, когда числители $m-1$ чисел Бернулли

$$(20) \quad B_2, B_4, \dots, B_{l-3} = B_{2(m-1)}$$

не делятся на l . ■

Первые шесть чисел Бернулли с четными индексами сравнительно невелики и без труда вычисляются по формуле (16):

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \\ B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}.$$

Отсюда сразу же следует, что *простые числа 5, 7, 11 и 13 являются куммеровыми.*

Для больших индексов числа Бернулли имеют вид

$$B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \quad B_{18} = \frac{43867}{798}, \\ B_{20} = -\frac{174611}{330}, \quad B_{22} = \frac{854513}{138}, \quad B_{24} = -\frac{236364091}{2730}, \\ (21) \quad B_{26} = \frac{8553103}{6}, \quad B_{28} = -\frac{23749461029}{870}, \\ B_{30} = \frac{8615841276005}{14322}, \quad B_{32} = -\frac{7709321041217}{510}, \\ B_{34} = \frac{2577867858367}{6}$$

и вычисление их уже довольно тяжело.

Поверив в правильность таблицы (21), мы можем уже без особого труда проверить, что *все простые числа < 37 куммеровы, а число 37 не куммерово* (ибо числитель 7 709 321 041 217 числа B_{32} делится на 37).

Впрочем, эту проверку можно довольно просто осуществить, и не пользуясь таблицей (21). Действительно, для любого данного l мы можем ввести в рассмотрение целые числа b_n , удовлетворяющие сравнениям

$$b_n Q_n \equiv P_n \pmod{l},$$

где P_n и Q_n — числитель и знаменатель числа Бернулли B_n . Ясно, что число l тогда и только тогда не делит числителей чисел (20), когда оно не делит чисел

$$b_2, b_4, \dots, b_{l-3}$$

Для последних чисел рекуррентные соотношения (17) заменяются соответствующими сравнениями

$$(22) \quad -(n+1)b_n \equiv 1 + (n+1)b_1 + \dots + \dots + \binom{n+1}{k} b_k + \dots + \binom{n+1}{n-1} b_{n-1} \pmod{l},$$

из которых их можно легко последовательно вычислять. При этом в сравнениях (22) можно априори считать, что $b_3 = b_5 = \dots = 0$. Кроме того, легко видеть, что $b_1 \equiv m \pmod{l}$, и потому $1 + (n+1)b_1 \equiv m - (k-1) \pmod{l}$ для любого четного $n = 2k$. Тем самым мы получаем следующее окончательное правило:

П р а в и л о. Чтобы узнать, является ли данное простое число l куммеровым, надо последовательно определить из сравнений

$$-3b_2 \equiv m \pmod{l},$$

$$-5b_4 \equiv m - 1 + 10b_2 \pmod{l},$$

.....

$$-(2k+1)b_{2k} \equiv m - (k-1) + \binom{2k+1}{2} b_2 + \dots + \binom{2k+1}{4} b_4 + \dots + \binom{2k+1}{2k-2} b_{2k-2} \pmod{l},$$

.....

$$-(l-2)b_{l-3} \equiv 2 + \binom{l-2}{2} b_2 + \binom{l-2}{4} b_4 + \dots + \dots + \binom{l-2}{l-5} b_{l-5} \pmod{l}$$

целые числа b_2, b_4, \dots, b_{l-3} из ряда $0, 1, \dots, l-1$.

Число l тогда и только тогда будет куммеровым, когда ни одно из этих чисел не равно нулю.

Например, при $l = 5$ имеется лишь одно сравнение

$$-3b_2 \equiv 2 \pmod{5},$$

которое имеет решение $b_2 \equiv 1$. Следовательно, число 5 куммерово.

При $l = 7$ имеется два сравнения

$$-3b_2 \equiv 3 \pmod{7},$$

$$-5b_4 \equiv 2 + 10b_2 \pmod{7},$$

которые имеют решение $b_2 \equiv 6$ и $b_3 \equiv 3$. Таким образом, число 7 также куммерово.

При $l = 11$ следует рассмотреть четыре сравнения

$$-3b_2 \equiv 5 \pmod{11},$$

$$-5b_4 \equiv 4 + 10b_2 \pmod{11},$$

$$-7b_6 \equiv 3 + 21b_2 + 35b_4 \pmod{11},$$

$$-9b_8 \equiv 2 + 36b_2 + 126b_4 + 84b_6 \pmod{11}.$$

Решая последовательно эти сравнения, мы получаем

$$-3b_2 \equiv 5 \Rightarrow b_2 \equiv 2,$$

$$-5b_4 \equiv 4 + 10b_2 \equiv 24 \equiv 2 \Rightarrow b_4 \equiv 4,$$

$$-7b_6 \equiv 3 + 21b_2 + 35b_4 \equiv 3 - b_2 + 2b_4 \equiv 9 \Rightarrow b_6 \equiv 5,$$

$$-9b_8 \equiv 2 + 36b_2 + 126b_4 + 84b_6 \equiv$$

$$\equiv 2 + 3b_2 + 5b_4 - 4b_6 \equiv 8 \Rightarrow b_8 \equiv 4.$$

Следовательно, число 11 куммерово.

Для больших l целесообразно предварительно вычислить (по модулю l) биномиальные коэффициенты, выписывая треугольник Паскаля и откидывая на каждом шагу слагаемые, кратные l . Например, при $l = 37$ мы получим треугольник, изображенный на следующей странице, в котором жирным шрифтом выделены нужные нам коэффициенты (по типографским соображениям от этого треугольника отсечены углы).

Кроме того, полезно заранее для любого $a = -(2k + 1)$ найти число a' , обладающее тем свой-

1 3 3 1
 1 4 6 4 1
 1 5 10 10 5 1
 1 6 15 20 15 6 1
 1 7 21 35 35 21 7 1
 1 8 28 19 33 19 28 8 1
 1 9 36 10 15 15 10 36 9 1
 1 10 8 9 25 30 25 9 8 10 1
 1 11 18 17 34 18 18 34 17 18 11 1
 1 12 29 35 14 15 36 15 14 35 29 12 1
 1 13 4 27 12 29 14 14 29 12 27 4 13 1
 1 14 17 31 2 4 6 28 6 4 2 31 17 14 1
 1 15 31 11 33 6 10 34 34 10 6 33 11 31 15 1
 1 16 9 5 7 2 16 7 31 7 16 2 7 5 9 16 1
 1 17 25 14 12 9 18 23 1 1 23 18 9 12 14 25 17 1
 1 18 5 2 26 21 27 4 24 2 24 4 27 21 26 2 5 18 1
 1 19 23 7 28 10 11 31 28 26 28 31 11 10 28 7 23 19 1
 1 20 5 30 35 1 21 5 22 17 15 17 22 5 21 1 35 30 5 20 1
 1 21 25 35 28 36 22 26 27 2 32 32 2 27 26 22 36 28 35 25 21 1
 1 22 9 23 26 27 21 11 16 29 34 27 34 29 16 11 21 27 26 23 9 22 1
 1 23 31 32 12 16 11 32 27 8 26 27 27 26 8 27 32 11 16 12 32 31 23 1
 1 24 17 26 7 28 27 6 22 35 34 13 11 13 34 35 22 6 27 28 7 26 17 24 1
 1 25 4 6 33 35 18 33 28 20 32 10 24 24 10 32 20 28 33 18 35 33 6 4 25 1
 1 26 29 10 2 31 16 14 24 11 15 5 34 11 34 5 15 11 24 14 16 31 2 10 29 26 1
 1 27 18 2 12 33 10 30 1 35 26 20 2 8 8 2 20 26 35 1 30 10 33 12 2 18 27 1
 1 28 8 20 14 8 6 3 31 36 24 9 22 10 16 10 22 9 24 36 31 3 6 8 14 20 8 28 1
 1 29 36 28 34 22 14 9 34 30 23 33 31 32 28 26 32 31 33 23 30 34 9 14 22 34 28 36 29 1
 30 28 27 25 19 36 23 6 27 16 19 27 26 21 15 21 26 27 19 16 27 6 23 36 19 25 27 28 30
 31 21 18 15 7 18 22 29 33 6 35 9 16 10 36 36 10 16 9 35 6 33 29 22 18 7 15 18 21 31
 15 2 33 22 25 3 14 25 2 4 7 25 26 9 35 9 26 25 7 4 2 25 14 3 25 22 33 2 15
 10 17 35 18 10 28 17 2 27 6 11 32 14 35 7 7 35 14 32 11 6 27 2 17 28 10 18 35 17 10

ством, что $aa' \equiv 1 \pmod{l}$. Так, например, при $l = 37$ имеем

a	-3	-5	-7	-9	-11	-13	-15	-17	-19
a'	12	-15	-16	4	10	-20	-5	13	-2

a	-21	-23	-25	-27	-29	-31	-33	-35
a'	7	8	-3	-11	14	-6	-9	19

После этого вычисления идут автоматически. Скажем, при $l = 37$ получаем:

$$\begin{aligned}
 b_2 &\equiv 12 \cdot 18 \equiv -6, \\
 b_4 &\equiv -15(17 - 6 \cdot 10) \equiv 16, \\
 b_6 &\equiv -16(16 - 6 \cdot 21 + 16 \cdot 35) \equiv 15, \\
 b_8 &\equiv 4(15 - 6 \cdot 36 + 16 \cdot 15 + 15 \cdot 10) \equiv 16, \\
 b_{10} &\equiv 10(14 - 6 \cdot 18 + 16 \cdot 34 + 15 \cdot 18 + 16 \cdot 17) \equiv 4, \\
 b_{12} &\equiv \dots \equiv 17, & b_{14} &\equiv \dots \equiv -5, \\
 b_{16} &\equiv \dots \equiv -15, & b_{18} &\equiv \dots \equiv -6, \\
 b_{20} &\equiv \dots \equiv 15, & b_{22} &\equiv \dots \equiv 15, \\
 b_{24} &\equiv \dots \equiv 17, & b_{26} &\equiv \dots \equiv 12, \\
 b_{28} &\equiv \dots \equiv -8, & b_{30} &\equiv \dots \equiv 2
 \end{aligned}$$

и, наконец,

$$\begin{aligned}
 b_{32} &\equiv -9(3 - 6 \cdot 10 + 16 \cdot 35 + 15 \cdot 10 + 16 \cdot 17 + \\
 &\quad + 4 \cdot 27 + 17 \cdot 11 - 5 \cdot 14 - 15 \cdot 7 - 6 \cdot 35 + 15 \cdot 32 + \\
 &\quad + 15 \cdot 6 + 17 \cdot 2 + 12 \cdot 28 - 8 \cdot 18 + 2 \cdot 17) \equiv 0 \pmod{37}.
 \end{aligned}$$

Следовательно, число 37 не куммерово (вычислять b_{34} нам уже не надо).

Недостаток этого способа состоит в том, что для каждого l все вычисления необходимо проделывать заново.

В основной теореме 3 § 9 мы предполагали, помимо всего прочего, что простое число l обладает тем свойством, что кольцо D_l удовлетворяет условию К из § 6. Рассмотрим теперь вопрос, нужно ли на самом деле это условие для справедливости теоремы.

Для этого нам необходимо предварительно более внимательно изучить вещественные элементы кольца D_l .

Примером таких элементов служат числа

$$\eta_0 = \xi + \xi^{-1} = \xi + \bar{\xi},$$

$$\eta_1 = \sigma \eta_0 = \sigma \xi + \sigma \bar{\xi},$$

$$\dots \dots \dots$$

$$\eta_{m-1} = \sigma^{m-1} \eta_0 = \sigma^{m-1} \xi + \sigma^{m-1} \bar{\xi}.$$

Предложение 4. Любое вещественное число $\beta \in D_l$ единственным образом представляется в виде

$$\beta = b_0 \eta_0 + b_1 \eta_1 + \dots + b_{m-1} \eta_{m-1},$$

где b_0, b_1, \dots, b_{m-1} — целые рациональные числа, т. е. в виде

$$\beta = b(\sigma) \eta_0,$$

где $b(X)$ — многочлен с целыми рациональными коэффициентами степени, не большей $m-1$.

Доказательство. Пусть

$$\beta = a(\sigma) \xi,$$

где $a(X)$ — многочлен с целыми рациональными коэффициентами степени, не большей $l-2 = 2m-1$. Положим

$$a(X) = b(X) + c(X) X^m,$$

где $b(X)$ и $c(X)$ — многочлены степени, не большей $m-1$. Тогда

$$\beta = b(\sigma) \xi + c(\sigma) \sigma^m \xi = (b(\sigma) + c(\sigma) \sigma^m) \xi$$

и

$$\bar{\beta} = \sigma^m \beta = c(\sigma) \xi + b(\sigma) \sigma^m \xi = (c(\sigma) + b(\sigma) \sigma^m) \xi.$$

Следовательно, из равенства $\beta = \bar{\beta}$ вытекает равенство

$$b(X) + c(X) X^m = c(X) + b(X) X^m,$$

откуда следует, что

$$b(X) = c(X).$$

Таким образом,

$$\beta = b(\sigma)(1 + \sigma^m)\zeta = b(\sigma)(\zeta + \bar{\zeta}) = b(\sigma)\eta_0. \quad \blacksquare$$

Удобно считать, что элементы $\eta_j = \sigma^j \eta_0$ определены для любых j . Конечно, $\eta_j = \eta_k$, если (и только если) $j \equiv k \pmod{m}$.

Предложение 5. Коэффициенты b_0, b_1, \dots, b_{m-2} произвольного вещественного элемента

$$(23) \quad \beta = b_0 \eta_0 + b_1 \eta_1 + \dots + b_{m-1} \eta_{m-1}$$

кольца D_l выражаются формулами

$$(24) \quad l b_k = (\eta_k - 2)\beta + \\ + (\eta_{k+1} - 2)\sigma\beta + \dots + (\eta_{k+m-1} - 2)\sigma^{m-1}\beta.$$

Докажем предварительно, что

$$(25) \quad \eta_0 \eta_j + \eta_1 \eta_{j+1} + \dots + \eta_{m-1} \eta_{m-1+j} = \\ = \begin{cases} l-2, & \text{если } j \equiv 0 \pmod{m}, \\ -2, & \text{если } j \not\equiv 0 \pmod{m}. \end{cases}$$

Так как $\eta_0 = \zeta + \zeta^{-1}$, то $\eta_0^2 = \zeta^2 + \zeta^{-2} + 2 = \eta_a + 2$, где a — такое число, что $g^a = 2 \pmod{l}$. Поэтому

$$\eta_1^2 = \sigma \eta_0^2 = \eta_{a+1} + 2, \quad \eta_2^2 = \eta_{a+2} + 2, \dots \\ \dots, \quad \eta_{m-1}^2 = \eta_{a+m-1} + 2$$

и, значит,

$$\eta_0^2 + \dots + \eta_{m-1}^2 = (\eta_a + \eta_{a+1} + \dots + \eta_{a+m-1}) + 2m.$$

Но ясно, что в сумму $\eta_a + \eta_{a+1} + \dots + \eta_{a+m-1}$ каждое число η_j , $j = 0, \dots, m-1$, входит, точно один раз, так что эта сумма равна

$$\eta_0 + \eta_1 + \dots + \eta_{m-1} = \zeta + \sigma\zeta + \dots + \sigma^{l-1}\zeta = -1.$$

Таким образом,

$$\eta_0^2 + \dots + \eta_{m-1}^2 = -1 + 2m = l - 2.$$

Аналогично, если $j \not\equiv 0 \pmod{m}$ и потому $\eta_j = \zeta^{g_j} + \zeta^{-g_j}$, где $g_j \neq 1$, $l-1$, то

$$\eta_0 \eta_j = (\zeta + \zeta^{-1})(\zeta^{g_j} + \zeta^{-g_j}) = \\ = \zeta^{g_j+1} + \zeta^{-g_j-1} + \zeta^{g_j-1} + \zeta^{-g_j+1} = \eta_a + \eta_b,$$

где a и b — такие показатели, что

$$\begin{aligned} g^a &\equiv g_i + 1 \pmod{l}, \\ g^b &\equiv g_i - 1 \pmod{l}. \end{aligned}$$

$$g^a \equiv g_f + 1 \pmod{l},$$

$$g^b \equiv g_l - 1 \pmod{l}.$$

Поэтому $\eta_k \eta_{k+j} = \sigma^k(\eta_0 \eta_j) = \eta_{a+k} + \eta_{b+k}$ для любого $k = 0, 1, \dots, m-1$, и, значит,

$$\eta_0\eta_j + \dots + \eta_{m-1}\eta_{m-1+j} = (\eta_a + \eta_{a+1} + \dots + \eta_{a+m-1}) + (\eta_b + \eta_{b+1} + \dots + \eta_{b+m-1}) = -1 - 1 = -2. \quad \square$$

Доказательство предложения 5. Применив к равенству (23) последовательно отображения σ , $\sigma^2, \dots, \sigma^{m-1}$, мы получим для коэффициентов b_0, b_1, \dots, b_{m-1} уравнения

$$\beta = b_0\eta_0 + b_1\eta_1 + \dots + b_{m-1}\eta_{m-1},$$

$$\sigma\beta = b_0\eta_1 + b_1\eta_2 + \dots + b_{m-1}\eta_m, \quad (26)$$

$$\sigma^{m-1}\beta = b_0\eta_{m-1} + b_1\eta_m + \dots + b_{m-1}\eta_{2m-2}.$$

Чтобы решить эти уравнения, мы умножим их соответственно на $\eta_k, \eta_{k+1}, \dots, \eta_{k+m-1}$, где $k = 0, 1, \dots, m-1$, и сложим. Тогда в силу формул (25) мы для любого $k = 0, 1, \dots, m-1$ получим равенство

$$\eta_k \beta + \eta_{k+1} \sigma \beta + \dots + \eta_{k+m-1} \sigma^{m-1} \beta = \\ = lb_k - 2(b_0 + b_1 + \dots + b_{m-1}).$$

С другой стороны, сложив уравнения (26), мы немедленно получим, что

$$\begin{aligned} \beta + \sigma\beta + \dots + \sigma^{m-1}\beta &= \\ &= (b_0 + b_1 + \dots + b_{m-1})(\eta_0 + \eta_1 + \dots + \eta_{m-1}) = \\ &= -(b_0 + b_1 + \dots + b_{m-1}). \end{aligned}$$

Поэтому

$$\begin{aligned} lb_k &= \eta_k \beta + \eta_{k+1} \sigma \beta + \dots + \eta_{k+m-1} \sigma^{m-1} \beta - \\ &\quad - 2(\beta + \sigma \beta + \dots + \sigma^{m-1} \beta) = \\ &= (\eta_k - 2) \beta + (\eta_{k+1} - 2) \sigma \beta + \dots + (\eta_{k+m-1} - 2) \sigma^{m-1} \beta \\ &\text{для любого } k = 0, 1, \dots, m-1. \blacksquare \end{aligned}$$

Для исследования условия К из § 6 нам понадобится, кроме того, еще одна общая конструкция:

Для любого отличного от нуля элемента α кольца D_l (или поля K_l), мы положим

$$L\alpha = (\ln|\alpha|, \ln|\sigma\alpha|, \dots, \ln|\sigma^{m-1}\alpha|) \in \mathbb{R}^m.$$

Таким образом, L будет представлять собой некоторое отображение множества $D_l^* = D_l \setminus 0$ в пространство \mathbb{R}^m вещественных векторов-строк (x_1, \dots, x_m) . Ясно, что умножение элементов из D_l^* это отображение переводит в сложение векторов из \mathbb{R}^m , т. е.

$$(27) \quad L(\alpha\beta) = L\alpha + L\beta$$

для любых элементов $\alpha, \beta \in D_l^*$.

Предложение 6. Векторы

$$(28) \quad L_1 = L(1 - \sigma\xi), \dots, L_m = L(1 - \sigma^m\xi)$$

составляют базис пространства \mathbb{R}^m , так что, в частности, любой вектор $L\alpha$, $\alpha \in D_l^*$, единственным образом через них линейно выражается:

$$(29) \quad L\alpha = x_1(\alpha)L_1 + \dots + x_m(\alpha)L_m,$$

где $x_1(\alpha), \dots, x_m(\alpha)$ — некоторые вещественные числа.

Доказательство. Поскольку $\sigma^i(1 - \sigma^k\xi) = 1 - \sigma^{i+k}\xi$, векторы L_1, \dots, L_m являются строками определителя

$$(30) \quad \begin{vmatrix} \ln|1 - \sigma\xi|, & \ln|1 - \sigma^2\xi|, & \dots, & \ln|1 - \sigma^m\xi| \\ \ln|1 - \sigma^2\xi|, & \ln|1 - \sigma^3\xi|, & \dots, & \ln|1 - \sigma^{m+1}\xi| \\ \dots & \dots & \dots & \dots \\ \ln|1 - \sigma^m\xi|, & \ln|1 - \sigma^{m+1}\xi|, & \dots, & \ln|1 - \sigma^{2m-1}\xi| \end{vmatrix},$$

и доказываемое утверждение равносильно тому, что этот определитель отличен от нуля.

Но, так как $\sigma^m\xi = \bar{\xi} = \xi^{-1}$ и $|\sigma^k\xi| = 1$, то

$$\begin{aligned} \ln|1 - \sigma^{m+k}\xi| &= \ln|1 - \sigma^k\xi^{-1}| = \\ &= \ln \frac{|1 - \sigma^k\xi|}{|\sigma^k\xi|} = \ln|1 - \sigma^k\xi|, \end{aligned}$$

откуда следует, что определитель (30) является так называемым *антициркулянт*ом, т. е. определителем вида

$$(31) \quad \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \\ \dots & \dots & \dots & \dots & \dots \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \end{vmatrix}.$$

$$(32) \quad a_n + a_1 \rho^k + \dots + a_{n-2} \rho^{(n-2)k} + a_{n-1} \rho^{(n-1)k},$$

$$k = 0, 1, \dots, n-1,$$

Доказательство. Переставим в определителе (31) первую строку с последней, вторую строку с предпоследней и т. д. (всего понадобится $m = \left[\frac{n}{2} \right]$ перестановок, отчего определитель умножится на $(-1)^m$). В результате получится так называемый *циркулянт* с матрицей

$$(33) \quad \begin{vmatrix} b_1 & b_2 & \dots & b_{n-1} & b_n \\ b_n & b_1 & \dots & b_{n-2} & b_{n-1} \\ \cdot & \cdot & \dots & \cdot & \cdot \\ b_2 & b_3 & \dots & b_n & b_1 \end{vmatrix},$$

$$(34) \quad b_1 + b_2 \rho^k + \dots + b_n \rho^{(n-1)k}, \quad k = 0, 1, \dots, n-1.$$
$$(35) \quad \left\| \begin{array}{c} 1 \\ \rho^k \\ \vdots \\ \rho^{(n-1)k} \end{array} \right\|, \quad k = 0, 1, \dots, n-1, \quad \left(\frac{2\pi}{n} \right)$$
$$(36) \quad \left\| \begin{array}{c} b_1 + b_2 \rho^k + \dots + b_n \rho^{(n-1)k} \\ b_n + b_1 \rho^k + \dots + b_{n-1} \rho^{(n-1)k} \\ \vdots \\ b_2 + b_3 \rho^k + \dots + b_1 \rho^{(n-1)k} \end{array} \right\|.$$
$$\begin{aligned} b_1 + b_2 \rho^k + \dots + b_n \rho^{(n-1)k} &= 1 \cdot (b_1 + b_2 \rho^k + \dots + b_n \rho^{(n-1)k}), \\ b_n + b_1 \rho^k + \dots + b_{n-1} \rho^{(n-1)k} &= \rho^k (b_1 + b_2 \rho^k + \dots + b_n \rho^{(n-1)k}), \\ \vdots &\vdots \\ b_2 + b_3 \rho^k + \dots + b_1 \rho^{(n-1)k} &= \rho^{(n-1)k} (b_1 + b_2 \rho^k + \dots \\ &\quad \dots + b_n \rho^{(n-1)k}). \end{aligned}$$

Следовательно, столбец (36) является произведением столбца (35) на число (34).

Это означает, что произведение матрицы (33) на матрицу P со столбцами (35) равно произведению матрицы P на диагональную матрицу Δ с диагональными элементами (34). (На языке линейной алгебры матрица P трансформирует матрицу (33) в диагональную матрицу Δ , т. е. столбцы матрицы P являются собственными векторами матрицы (33), принадлежащими собственным значениям (34)). Переходя к определителям и сокращая на определитель матрицы P (который, являясь определителем Вандермонда различных чисел $1, \rho, \rho^2, \dots, \rho^{n-1}$, отличен от нуля), мы получим, что определитель матрицы (33) равен определителю матрицы Δ , т. е. равен произведению чисел (34). ■

Для определителя (30) числа (32) имеют вид

$$\ln|1 - \sigma^m \xi| + \rho^k \ln|1 - \sigma \xi| + \dots \\ \dots + \rho^{(m-1)k} \ln|1 - \sigma^{m-1} \xi|,$$

где ρ — первообразный корень из единицы степени $m = \frac{l-1}{2}$. Так как $\rho = \theta^2$, где θ — первообразный корень из единицы степени $2m = l-1$ и $\ln|1 - \sigma^m \xi| = \ln|1 - \xi^{-1}| = \ln|1 - \xi|$, то мы получаем, следовательно, что определитель (30) равен произведению m чисел

$$(37) \quad c_k = \ln|1 - \xi| + \theta^{2k} \ln|1 - \sigma \xi| + \dots \\ \dots + \theta^{2(m-1)k} \ln|1 - \sigma^{m-1} \xi| = \\ = \sum_{j=0}^{m-1} \theta^{2jk} \ln|1 - \sigma^j \xi|, \quad k = 0, 1, \dots, m-1.$$

Поэтому доказательство предложения 4 сводится к доказательству того, что числа c_0, c_1, \dots, c_{m-1} отличны от нуля.

Число c_0 легко вычисляется. Так как $|1 - \sigma^{m+k} \xi| = |1 - \sigma^k \xi|$, то

$$c_0 = \ln|1 - \xi| + \ln|1 - \sigma \xi| + \dots + \ln|1 - \sigma^{m-1} \xi| = \\ = \ln|(1 - \xi)(1 - \sigma \xi) \dots (1 - \sigma^{m-1} \xi)| = \\ = \frac{1}{2} \ln|(1 - \xi)(1 - \sigma \xi) \dots \\ \dots (1 - \sigma^{m-1} \xi)(1 - \sigma^m \xi)(1 - \sigma^{m+1} \xi) \dots (1 - \sigma^{2m-1} \xi)| = \\ = \frac{1}{2} \ln|N(1 - \xi)|.$$

Поскольку $N(1 - \zeta) = l$, этим доказано, что

$$(38) \quad c_0 = \frac{1}{2} \ln l.$$

Таким образом, действительно $c_0 \neq 0$.

Тем самым все сводится к доказательству следующей леммы:

Л е м м а 2. Числа c_1, \dots, c_{m-1} отличны от нуля.

Мы докажем эту лемму позже (в § 15). ■

Заметим, что поскольку определитель (30) является антициркулянтном, все его столбцы состоят из одних и тех же чисел. Поэтому сумма элементов каждого столбца равна сумме элементов первого столбца. Но эта сумма равна по определению c_0 . Ввиду формулы (38) это доказывает, что

$$(39) \quad L_1 + L_2 + \dots + L_m = \frac{1}{2} \ln l \cdot E,$$

где E — вектор $(1, 1, \dots, 1)$.

Формула (39) по существу является лишь переводом формулы (38) на язык векторов. Однако формулу (38) можно записать на языке векторов и другим способом, допускающим важное обобщение. Действительно, поскольку определитель (30) симметричен, сумма элементов каждой его строки также равна c_0 . Поэтому, обозначая для любого вектора $X = (x_1, \dots, x_m) \in \mathbb{R}^m$ через ΣX сумму его компонент:

$$\Sigma X = x_1 + \dots + x_m,$$

мы можем формулу (38) записать в следующем виде:

$$(40) \quad \Sigma L_i = \frac{1}{2} \ln l, \quad i = 1, 2, \dots, m.$$

Обобщением этой формулы является тождество

$$(41) \quad \Sigma L\alpha = \frac{1}{2} \ln N\alpha,$$

имеющее место для любого элемента $\alpha \in D_l^*$. Доказательство этого тождества повторяет доказательство формулы (38): так как $\sigma^{m+k}\alpha = \overline{\sigma^k\alpha}$, то

$$N\alpha = |\alpha \cdot \sigma\alpha \cdot \dots \cdot \sigma^{m-1}\alpha|^2,$$

и потому

$$\begin{aligned}\frac{1}{2} \ln N\alpha &= \ln |\alpha \cdot \sigma\alpha \cdot \dots \cdot \sigma^{m-1}\alpha| = \\ &= \ln |\alpha| + \ln |\sigma\alpha| + \dots + \ln |\sigma^{m-1}\alpha| = \Sigma L\alpha. \blacksquare\end{aligned}$$

Для любого элемента $\alpha \in D_l^*$ коэффициенты $x_1(\alpha), \dots, x_m(\alpha)$ разложения (29) составляют некоторый вектор

$$X(\alpha) = (x_1(\alpha), \dots, x_m(\alpha)) \in \mathbb{R}^m.$$

Тем самым возникает отображение $X: D_l^* \rightarrow \mathbb{R}^m$, подобно отображению L переводящее умножение в D_l^* в сложение в \mathbb{R}^m , т. е. такое, что

$$X(\alpha\beta) = X(\alpha) + X(\beta)$$

для любых элементов $\alpha, \beta \in D_l^*$. (Отображения L и X отличаются друг от друга на линейное преобразование пространства \mathbb{R}^m с определителем (30).)

Легко видеть, что для каждого элемента $\alpha \in D_l^*$ справедлива формула

$$(42) \quad \Sigma X(\alpha) = \log_l N\alpha.$$

Действительно, ясно, что Σ является линейным функционалом, т. е. $\Sigma(X_1 + X_2) = \Sigma X_1 + \Sigma X_2$ и $\Sigma(cX) = c\Sigma X$ для любых векторов $X_1, X_2, X \in \mathbb{R}^m$ и любого числа $c \in \mathbb{R}$. Поэтому (см. формулы (40) и (41))

$$\begin{aligned}\frac{1}{2} \ln N\alpha &= \Sigma L\alpha = x_1(\alpha) \Sigma L_1 + \dots + x_m(\alpha) \Sigma L_m = \\ &= (x_1(\alpha) + \dots + x_m(\alpha)) \cdot \frac{1}{2} \ln l = \Sigma X(\alpha) \cdot \frac{1}{2} \ln l,\end{aligned}$$

и, следовательно,

$$\Sigma X(\alpha) = \frac{\ln N\alpha}{\ln l} = \log_l N\alpha. \blacksquare$$

Предложение 7. Число $\alpha \in D_l^*$ тогда и только тогда является:

- i) единицей, когда $\Sigma X(\alpha) = 0$;
- ii) корнем из единицы, когда $X(\alpha) = 0$;
- iii) специальной единицей, когда $\Sigma X(\alpha) = 0$ и вектор $X(\alpha)$ целочислен (все его компоненты являются целыми числами).

Доказательство. Мы знаем (см. стр. 68), что число $\alpha \in D_i^*$ тогда и только тогда является единицей, когда $N\alpha = 1$. В силу (42) это доказывает i).

Аналогично $X(\alpha) = 0$ тогда и только тогда, когда $|\sigma^j \alpha| = 1$ для всех $j = 0, 1, \dots, m-1$, т. е. — в других обозначениях — когда $|\alpha^{(k)}| = 1$ для всех $k = 1, \dots, l-1$. Поэтому ii) следует из предложения 2 § 6 (и сделанного в § 5 замечания).

Если для числа $\alpha \in D_i^*$ все числа $x_1(\alpha) = n_1, \dots, x_m(\alpha) = n_m$ целые, то мы можем образовать число

$$(43) \quad \varepsilon = (1 - \sigma \zeta)^{n_1} \dots (1 - \sigma^m \zeta)^{n_m}.$$

Ясно, что $X(\alpha) = X(\varepsilon)$, т. е. $X(\alpha \varepsilon^{-1}) = 0$, и потому (утверждение ii) и предложение 1 § 6) $\alpha = \pm \zeta^a \varepsilon$. Обратно, если $\alpha = \pm \zeta^a \varepsilon$, где ε имеет вид (43), то $X(\alpha) = X(\varepsilon) = (n_1, \dots, n_m)$. Это вместе с i) доказывает iii). ■

Множество (решетку) всех целочисленных векторов из \mathbb{R}^m будем обозначать символом \mathbb{Z}^m .

Для любого вектора $X = (x_1, \dots, x_m) \in \mathbb{R}^m$, положим

$$\|X\| = \max(|x_1|, \dots, |x_m|).$$

Предложение 8. В кольце D_i имеется лишь конечное число вещественных чисел β , для которых $\|X(\beta)\| \leq \text{const}$.

Доказательство. Если $\|X(\beta)\| \leq \text{const}$, то

$$\|L\beta\| \leq \text{const} \cdot \max(\|L_1\|, \dots, \|L_m\|),$$

т. е. $\|L\beta\| \leq \text{const}$, и потому

$$|\sigma^k \beta| \leq \text{const} \text{ для любого } k = 0, 1, \dots, m-1.$$

Следовательно, согласно формуле (24),

$$|lb_k| \leq \text{const} \cdot \max(|\eta_k - 2|, \dots, |\eta_{k+m-1} - 2|),$$

т. е. $|lb_k| \leq \text{const}$, и потому $|b_k| \leq \text{const}$ для любого $k = 0, 1, \dots, m$.

Это доказывает предложение 8, поскольку неравенству $|b| \leq \text{const}$ удовлетворяет лишь конечное число целых чисел b . ■

Следствие. В кольце D_i имеется лишь конечное число единиц ε , для которых $\|X(\varepsilon)\| \leq \text{const}$.

Доказательство. Согласно предложению 3 § 6 имеет место равенство $\varepsilon = \zeta^a \varepsilon_0$, где ε_0 — вещественная единица. При этом $X(\varepsilon) = X(\varepsilon_0)$. Поэтому число всех единиц ε с $\|X(\varepsilon)\| \leq \text{const}$ равно умноженному на $2l$ числу всех вещественных единиц ε_0 с $\|X(\varepsilon_0)\| \leq \text{const}$, а, согласно предложению 8, последнее число конечно. ■

Теперь мы можем доказать основное предложение этого раздела:

Предложение 9. В кольце D_l существует такое конечное множество $\{\varepsilon_1, \dots, \varepsilon_n\}$ единиц, что любая единица $\varepsilon \in D_l$ представляется в виде $\varepsilon_i \eta$, где η — специальная единица.

Доказательство. Пусть $X(\varepsilon) = (x_1, \dots, x_m)$, и пусть n_1, \dots, n_m — такие целые числа, что

$$|x_1 - n_1| \leq \frac{1}{2}, \dots, |x_{m-1} - n_{m-1}| \leq \frac{1}{2}$$

и

$$n_m = -(n_1 + \dots + n_{m-1}).$$

Тогда определена специальная единица

$$\eta = (1 - \sigma \zeta)^{n_1} \dots (1 - \sigma^m \zeta)^{n_m}$$

и для единицы $\varepsilon \eta^{-1}$ имеют место неравенства

$$|x_1(\varepsilon \eta^{-1})| = |x_1 - n_1| \leq \frac{1}{2},$$

.....

$$|x_{m-1}(\varepsilon \eta^{-1})| = |x_{m-1} - n_{m-1}| \leq \frac{1}{2}.$$

$$\begin{aligned} |x_m(\varepsilon \eta^{-1})| &= |x_m - n_m| = \\ &= |(x_1 + \dots + x_{m-1}) - (n_1 + \dots + n_{m-1})| \leq \\ &\leq |x_1 - n_1| + \dots + |x_{m-1} - n_{m-1}| = \frac{m-1}{2}. \end{aligned}$$

Для завершения доказательства осталось заметить, что, согласно следствию из предложения 8, в кольце D_l существует лишь конечное число единиц $\varepsilon_1, \dots, \varepsilon_n$, удовлетворяющих неравенствам

$$|x_1(\varepsilon_i)| \leq \frac{1}{2}, \dots, |x_{m-1}(\varepsilon_i)| \leq \frac{1}{2}, |x_m(\varepsilon_i)| \leq \frac{m-1}{2}. \quad \blacksquare$$

Выбрасывая, если нужно, лишние единицы, мы можем считать, что множество $\{\varepsilon_1, \dots, \varepsilon_n\}$ минимально, т. е., что для представления единиц кольца D_l в виде $\varepsilon\eta$ необходимы все единицы $\varepsilon_1, \dots, \varepsilon_n$. Но тогда легко видеть, что для любой единицы $\varepsilon \in D_l$ представление $\varepsilon = \varepsilon_i\eta$ единственно, т. е. индекс i однозначно определен единицей ε . Действительно, если, например, $\varepsilon_1\eta_1 = \varepsilon_2\eta_2$, где η_1 и η_2 — некоторые специальные единицы, то $\varepsilon_2 = \varepsilon_1\eta'_1$, где $\eta'_1 = \eta_1\eta_2^{-1}$ — специальная единица, и потому любое представление вида $\varepsilon = \varepsilon_2\eta$ мы можем заменить представлением вида $\varepsilon = \varepsilon_1(\eta'_1\eta)$. Значит, без единицы ε_2 мы можем обойтись, что противоречит минимальности множества $\{\varepsilon_1, \dots, \varepsilon_n\}$.

Тем самым доказано, что *условие К из § 6 выполнено для любого простого числа l* и потому в теореме 1 § 9 (и в предложении 7 § 6) его можно не упоминать.

Таким образом, из трех условий, наложенных в теореме 1 § 9 на число l (регулярность, куммеровость и условие К) у нас остались только первые два. Как выше уже было сказано, эти условия на самом деле равносильны (ибо $h = h_1h_2$). Поэтому в силу предложения 3 мы можем эту теорему сформулировать в следующем окончательном виде:

Теорема Куммера. Теорема Ферма справедлива для простого числа l , если это число не делит числителей чисел Бернулли

$$B_2, B_4, \dots, B_{l-3}. \blacksquare$$

Выше мы проверили условия этой теоремы для $l = 5, 7, 11$. Поэтому *при $l \leq 11$ теорема Ферма верна*. При $l = 37$ эти условия не выполнены, и потому на вопрос, верна ли при $l = 37$ теорема Ферма, теорема Куммера ответа не дает.

Аналогичная — по существу автоматическая — проверка выявляет, что, кроме известного уже нам числа 37, среди простых чисел первой сотни нерегулярны (= некуммеровы) еще только два числа 59 и 67 (стоит заметить, что, например, при $l = 67$ число h_1 равно $853\,513 = 67 \cdot 12\,739$, так что здесь мы имеем дело с очень большими числами). Как было сказано на стр. 17, уже сам Куммер специальным рассуждением доказал теорему Ферма и при $l = 37, 59, 67$.

К настоящему же времени найдены все нерегулярные простые числа $\leq 100\,000$, и для них также проверена справедливость теоремы Ферма.

Следует, однако, подчеркнуть, что теорема Куммера у нас на самом деле пока еще не доказана. Чтобы ее доказательство было полным, нужно доказать формулу $h = h_1 h_2$ для числа классов идеалов кольца D_l (и также использованную выше лемму 2 о числах c_1, \dots, c_{m-1}). Мы сделаем это в следующих параграфах. Только после этого теорему Куммера мы сможем считать доказанной.

§ 13. Свойства дивизоров

Доказательство формулы Куммера $h = h_1 h_2$, в целом чисто аналитическое, опирается все же на некоторые арифметические факты о дивизорах в кольце D_l . Мы изложим их в этом параграфе.

Пусть сначала D — произвольное кольцо, допускающее теорию дивизоров (удовлетворяющую аксиомам 1—3 из § 8).

Для упрощения формул мы, как правило, будем в обозначении главных дивизоров опускать скобки, т. е. вместо $(\alpha) = a$ будем писать просто $\alpha = a$. Необходимо четко понимать условный характер этой записи: так, в частности, из $\alpha = a$ и $\beta = a$ следует только, что $\alpha \sim \beta$. Утверждение, что α делится на a , будет, как и выше, означать, что (α) делится на a . Поскольку α делится на β тогда и только тогда, когда (α) делится на (β) , это терминологическое упрощение к недоразумениям привести не должно.

В соответствии с этим соглашением дивизор $(\alpha_1, \dots, \alpha_k)$ будет теперь наибольшим общим делителем элементов $\alpha_1, \dots, \alpha_k$. Если этот дивизор равен e , то элементы $\alpha_1, \dots, \alpha_k$ называются *взаимно простыми* (в кольце D). Это имеет место тогда и только тогда, когда существуют такие числа $\beta_1, \dots, \beta_k \in D$, что

$$(1) \quad \beta_1 \alpha_1 + \dots + \beta_k \alpha_k = 1.$$

Таким образом, это определение взаимной простоты сильнее того, которым мы пользовались в § 4 (но совпадает с ним в случае евклидовых колец, на которые по существу и был ориентирован § 4).

Заметим, что числа $a_1, \dots, a_k \in \mathbb{Z} \subset D$ тогда и только тогда взаимно просты в этом смысле (в D), когда они взаимно просты в обычном смысле (в \mathbb{Z}). Действительно, если эти числа взаимно просты в \mathbb{Z} , то равенство (1) (с $\alpha_i = a_1, \dots, \alpha_k = a_k$), как известно, выполнено (с $\beta_1, \dots, \beta_k \in \mathbb{Z}$). Если же числа a_1, \dots, a_k не взаимно просты в \mathbb{Z} и потому имеют общий делитель $d > 1$, то равенство (1) невозможно ни при каких $\beta_1, \dots, \beta_k \in D$, поскольку его левая часть будет делиться на d . ■

Пусть α — дивизор кольца D , и пусть $\alpha, \beta \in D$. Мы будем писать

$$\alpha \equiv \beta \pmod{\alpha}$$

и говорить, что α *сравнимо с β по модулю α* , если элемент $\alpha - \beta$ делится на дивизор α . Эти сравнения обладают всеми стандартными свойствами равенств (их можно складывать, перемножать и т. д.; только сокращение обоих членов сравнения на общий множитель не всегда допустимо; для этого нужно, чтобы этот множитель был взаимно прост с α).

Следующее предложение в элементарной теории чисел известно как «китайская теорема об остатках»:

Предложение 1. *Для любых попарно взаимно простых дивизоров $\alpha_1, \dots, \alpha_s$ и любых элементов $\alpha_1, \dots, \alpha_s$ кольца D существует такой элемент $\xi \in D$, что*

$$\xi \equiv \alpha_1 \pmod{\alpha_1},$$

$$\dots \dots \dots$$

$$\xi \equiv \alpha_s \pmod{\alpha_s}.$$

Доказательство. Пусть $b_i, i = 1, \dots, s$, — произведение всех дивизоров $\alpha_1, \dots, \alpha_s$, за исключением дивизора α_i . Ясно, что дивизоры b_1, \dots, b_s взаимно просты, и, значит, существуют такие элементы β_1, \dots, β_s , делящиеся соответственно на дивизоры b_1, \dots, b_s , что

$$(2) \quad \beta_1 + \beta_2 + \dots + \beta_s = 1.$$

По построению каждый дивизор α_i делит все дивизоры $b_j, j \neq i$, а значит, делит и все элементы $\beta_j, j \neq i$. Поэтому из равенства (2) вытекает, что $\beta_i \equiv 1 \pmod{\alpha_i}$. Следовательно, элемент

$$\xi = \alpha_1 \beta_1 + \dots + \alpha_s \beta_s$$

обладает тем свойством, что

$$\xi \equiv \alpha_i \beta_i \equiv \alpha_i \pmod{\alpha_i}$$

для любого $i = 1, \dots, s$. ■

Согласно аксиоме 3 § 8 для любого дивизора α существует такой элемент $\gamma \in D$, что $\gamma = \alpha \epsilon$, где ϵ — некоторый дивизор. Оказывается, что дивизор ϵ можно всегда выбрать так, чтобы он был взаимно прост с любым наперед заданным дивизором b .

Предложение 2. Для любых двух дивизоров α и b существует такой элемент $\gamma \in D^*$, что $\gamma = \alpha \epsilon$, где $(b, \epsilon) = e$, т. е. такой, что

$$(ab, \gamma) = \alpha.$$

Доказательство. Пусть p_1, \dots, p_s — все простые дивизоры, на которые делится дивизор ab , и пусть $p_i^{a_i}$ — наивысшая степень дивизора p_i , на которую делится дивизор α (случай $a_i = 0$ не исключается). Для любого $i = 1, \dots, s$ выберем произвольный элемент $\alpha_i \in D^*$, делящийся на $p_i^{a_i}$, но не делящийся на $p_i^{a_i+1}$ (элемент α_i существует — им будет каждый элемент идеала $[p_i^{a_i}]$, не принадлежащий идеалу $[p_i^{a_i+1}]$). Согласно предложению 1 существует такой элемент $\gamma \in D^*$, что

$$\gamma \equiv \alpha_i \pmod{p_i^{a_i+1}}$$

для любого $i = 1, \dots, s$. Так как α_i делится на $p_i^{a_i}$, то γ делится на $p_1^{a_1} \dots p_s^{a_s} = \alpha$, т. е. $\gamma = \alpha \epsilon$.

Ясно, что ни один из дивизоров p_1, \dots, p_s не может делить дивизор ϵ , так как, если p_i делит ϵ , то γ делится на $p_i^{a_i+1}$ и, значит, α_i делится на $p_i^{a_i+1}$, что невозможно. С другой стороны, каждый простой дивизор, делящий дивизор b , делит дивизор ab и потому является одним из дивизоров p_1, \dots, p_s . Следовательно, дивизоры b и ϵ не имеют ни одного общего простого делителя, т. е. $(b, \epsilon) = e$. ■

Для колец D , удовлетворяющих условиям теоремы 4 § 10 (для которых, следовательно, дивизоры могут быть отождествлены с идеалами), из предложения 2 вытекает, что любой идеал A кольца D порождается двумя элементами:

$$A = (\alpha, \beta).$$

Действительно, согласно предложению 2 § 10, существуют такой идеал B и такой элемент α , что $AB = \alpha$, а согласно предложению 2, существует такой элемент β , что $(AB, \beta) = A$. ■

Поскольку отношение «быть сравнимым по модулю дивизора α » является, очевидно, отношением эквивалентности, кольцо D разбивается на непересекающиеся классы сравнимых друг с другом по модулю дивизора α элементов. Ясно, что эти классы являются не чем иным, как *смежными классами* кольца D (рассматриваемого как группа по сложению) по его идеалу $[\alpha]$ (рассматриваемого как подгруппа группы D).

В дополнение к аксиомам 1—3 § 8, определяющим теорию дивизоров, мы потребуем теперь выполнения еще следующей аксиомы:

Аксиома N. Для любого дивизора α кольца D множество всех классов элементов этого кольца, сравнимых друг с другом по модулю α , конечно.

В кольце D , удовлетворяющем условиям теоремы 4 § 10, каждый идеал A имеет ранг n , и потому факторгруппа D/A , т. е. множество смежных классов D по A , конечна (см. стр. 113). При $A = [\alpha]$ мы получаем, следовательно, что аксиома N выполнена в каждом кольце, удовлетворяющем условиям теоремы 1 § 10 (α , значит, в частности, и в кольце D_1).

Число классов кольца D по модулю α обозначается символом $N\alpha$ и называется *нормой дивизора α* .

Аксиома N означает, что в кольце D существует $N = N\alpha$ элементов $\alpha_1, \dots, \alpha_N$, обладающих тем свойством, что любой элемент кольца D сравним по модулю α с одним и только одним из этих элементов. Говорят, что элементы $\alpha_1, \dots, \alpha_N$ составляют *полную систему представителей* классов кольца D по модулю α .

Предложение 3 (мультипликативность нормы). Для любых двух дивизоров α и β кольца D имеет место равенство

$$N(\alpha\beta) = N\alpha \cdot N\beta.$$

Доказательство. Пусть γ — такой элемент кольца D , что

$$\gamma = \alpha c \text{ и } (\beta, c) = e$$

(см. предложение 2). Пусть, далее,

$$\alpha_1, \dots, \alpha_N, \quad N = N\alpha,$$

и

$$\beta_1, \dots, \beta_M, \quad M = M\beta,$$

— полные системы представителей смежных классов кольца D по модулю дивизоров α и β соответственно. Для доказательства предложения 3 достаточно доказать, что NM элементов

$$(3) \quad \alpha_i + \beta_j \gamma, \quad i = 1, \dots, N, \quad j = 1, \dots, M,$$

составляют полную систему представителей смежных классов кольца D по модулю дивизора $\alpha\beta$, т. е. что:

а) никакие два элемента вида (3) не сравнимы по модулю дивизора $\alpha\beta$;

б) любой элемент $\alpha \in D$ сравним по модулю дивизора $\alpha\beta$ с одним (и, согласно а), только с одним) элементом вида (2).

Но если

$$\alpha_i + \beta_j \gamma \equiv \alpha_{i'} + \beta_{j'} \gamma \pmod{\alpha\beta},$$

то, тем более,

$$\alpha_i + \beta_j \gamma \equiv \alpha_{i'} + \beta_{j'} \gamma \pmod{\alpha}.$$

Поскольку $\gamma \equiv 0 \pmod{\alpha}$, отсюда следует, что $\alpha_i \equiv \alpha_{i'} \pmod{\alpha}$ и, значит, $i = i'$. Кроме того,

$$\beta_j \gamma \equiv \beta_{j'} \gamma \pmod{\alpha\beta},$$

т. е. $(\beta_j - \beta_{j'})\gamma = \alpha\beta m$, где m — некоторый дивизор, и потому

$$(\beta_j - \beta_{j'})\alpha c = \alpha\beta m.$$

Следовательно,

$$(\beta_j - \beta_{j'})c = \beta m.$$

Поскольку $(\beta, c) = e$, отсюда следует, что $\beta_j - \beta_{j'} \equiv 0 \pmod{\beta}$ и, значит, $j = j'$. Это доказывает а).

Пусть теперь $\alpha \in D$. По условию существует такой элемент α_i , что $\alpha \equiv \alpha_i \pmod{\alpha}$. Снова применяя предложение 2, найдем такой элемент $\delta \equiv 0 \pmod{c}$, что

$$(\delta, \alpha\beta) = c,$$

т. е. такой, что $\delta = t\delta$, где $(\delta, a\delta) = e$. Так как элемент $(\alpha - \alpha_i)\delta$ делится на дивизор $a\delta = (\gamma)\delta$, то он делится и на элемент γ , т. е.

$$\frac{(\alpha - \alpha_i)\delta}{\gamma} \in D.$$

С другой стороны, так как дивизоры c и δ взаимно просты с дивизором b , то элемент δ также взаимно прост с дивизором b , откуда следует, что все элементы

$$(4) \quad \delta\beta_1, \dots, \delta\beta_M$$

несравнимы друг с другом по модулю b . Действительно, если $\delta\beta_i \equiv \delta\beta_j \pmod{b}$, то элемент $\delta(\beta_i - \beta_j)$ делится на b , и, значит (поскольку элемент δ взаимно прост с b), элемент $\beta_i - \beta_j$ делится на b , что возможно только при $i = j$. Поскольку число элементов (4) равно M , этим доказано, что они также составляют полную систему представителей смежных классов кольца D по модулю дивизора b .

Поэтому, в частности, существует такой индекс j , что

$$\delta\beta_j \equiv \frac{(\alpha - \alpha_i)\delta}{\gamma} \pmod{b}.$$

Но тогда

$$\gamma\delta\beta_i \equiv (\alpha - \alpha_i)\delta \pmod{(\gamma)b},$$

т. е.

$$\gamma\delta\beta_j \equiv (\alpha - \alpha_i)\delta \pmod{a\delta c}.$$

Полагая

$$A = \alpha - \alpha_i - \beta_j\gamma,$$

мы получим отсюда, что

$$A\delta \equiv 0 \pmod{a\delta c},$$

т. е. что дивизор $(A)\delta$ делится на дивизор $a\delta c$. Поэтому дивизор $(A)b$ делится на дивизор $a\delta$, а так как по условию $(b, a\delta) = e$, то на дивизор $a\delta$ делится и элемент A . Таким образом, $A \equiv 0 \pmod{a\delta}$, т. е.

$$\alpha \equiv \alpha_i + \beta_j\gamma \pmod{a\delta}.$$

Это доказывает б). ■

Другое доказательство предложения 3 дано в ТФ на стр. 106—109.

Пусть аддитивная группа кольца D является решеткой ранга n с базисом $\omega_1, \dots, \omega_n$.

Так как элемент

$$\alpha = a_1\omega_1 + \dots + a_n\omega_n$$

кольца D тогда и только тогда делится на целое рациональное число $a \in \mathbb{Z}$, когда все коэффициенты a_1, \dots, a_n делятся на a , то, заставив каждый коэффициент a_1, \dots, a_n пробегать полную систему представителей смежных классов кольца \mathbb{Z} по модулю $|a|$ (например, систему $0, 1, \dots, |a| - 1$), мы получим полную систему представителей смежных классов кольца D по модулю главного дивизора (a) .

Этим доказано, что если $\alpha = (a)$, то $N\alpha = |a|^n$. ■

Задача. Докажите, что для любого главного дивизора (α) кольца D имеет место равенство

$$(5) \quad N(\alpha) = |N\alpha|.$$

Обобщая обозначение, введенное в § 5, мы для любого многочлена

$$F(X) = \alpha_0 X^m + \alpha_1 X^{m-1} + \dots + \alpha_m$$

с коэффициентами из кольца D будем символом $[F]$ обозначать дивизор, являющийся наибольшим общим делителем его коэффициентов:

$$[F] = (\alpha_0, \alpha_1, \dots, \alpha_m).$$

Предложение 4 (лемма Гаусса для кольца D). Для любых двух многочленов $F(X)$ и $G(X)$ имеет место равенство

$$(6) \quad [FG] = [F] \cdot [G].$$

Доказательству этого предложения мы предположим две леммы.

Лемма 1. Если простой дивизор \wp не делит ни дивизор $[F]$, ни дивизор $[G]$, то он не делит и дивизор $[FG]$.

Доказательство (ср. с доказательством леммы 1 § 5). Пусть

$$F(X) = \alpha_0 X^m + \alpha_1 X^{m-1} + \dots + \alpha_m,$$

$$G(X) = \beta_0 X^n + \beta_1 X^{n-1} + \dots + \beta_n,$$

$$F(X)G(X) = \gamma_0 X^{m+n} + \gamma_1 X^{m+n-1} + \dots + \gamma_{m+n},$$

и, следовательно,

$$\gamma_k = \alpha_0 \beta_k + \alpha_1 \beta_{k-1} + \dots + \alpha_k \beta_0, \quad k = 0, 1, \dots, m+n,$$

где мы условно считаем, что $\alpha_i = 0$ при $i > m$ и $\beta_j = 0$ при $j > n$.

Так как p не делит $[F]$, то существуют индексы $i \geq 0$, для которых α_i не делится на p . Пусть i_0 — наименьший из этих индексов, так что коэффициент α_{i_0} не делится на p , а (при $i_0 > 0$) коэффициенты $\alpha_0, \alpha_1, \dots, \alpha_{i_0-1}$ на p делятся. Аналогично, пусть j_0 — наименьший из всех индексов, для которых β_j не делится на p . Тогда

$$\gamma_{i_0+j_0} = \alpha_{i_0} \beta_{j_0} + \dots \equiv \alpha_{i_0} \beta_{j_0} \pmod{p},$$

ибо в невыписанных слагаемых $\alpha_i \beta_j$ либо $i < i_0$, либо $j < j_0$. Но, поскольку дивизор p прост, число $\alpha_{i_0} \beta_{j_0}$ не делится на p . Таким образом, коэффициент $\gamma_{i_0+j_0}$, а, значит, и дивизор $[FG]$, на p не делится. ■

Л е м м а 2. *Для любого многочлена F с коэффициентами из D и любого простого дивизора p кольца D существует такой элемент ξ поля отношений K , что все коэффициенты многочлена ξF лежат в D , а дивизор $[\xi F]$ не делится на p .*

Доказательство. Пусть дивизор $[F]$ делится на p^a , но не делится на p^{a+1} . Поскольку при $a = 0$ утверждение леммы 2 очевидно, мы без ограничения общности можем считать, что $a > 0$.

Пусть α — произвольное, отличное от нуля число, делящееся на p^a , и пусть $\alpha = p^a a$. Согласно предложению 2 существует такой элемент $\beta \in D$, что $\beta = \alpha b$, где $(b, p) = e$. Мы положим $\xi = \frac{\beta}{\alpha}$.

Рассмотрим произвольный коэффициент α_k многочлена $F(X)$. По условию $\alpha_k = p^{a+a_k} a_k$, где $a_k \geq 0$ и $(a_k, p) = e$. Поэтому число $\beta \alpha_k = \alpha p^a \cdot b p^{a_k} a_k$ делится на число $\alpha = \alpha p^a$. Следовательно, каждый коэффициент многочлена ξF лежит в D .

Кроме того, мы видим, что $\xi \alpha_k = p^{a_k} b a_k$, где $(b a_k, p) = e$. Поскольку существует индекс k , для которого $a_k = 0$ (в противном случае дивизор $[F]$ делился бы на p^{a+1}), это доказывает, что наибольший общий делитель $[\xi F]$ коэффициентов $\xi \alpha_k$ не делится на p . ■

Доказательство предложения 4. Пусть \mathfrak{p} — произвольный простой дивизор кольца D , и пусть $[F]$ делится на \mathfrak{p}^a , но не на \mathfrak{p}^{a+1} , а $[G]$ делится на \mathfrak{p}^b , но не на \mathfrak{p}^{b+1} . Нам нужно доказать, что $[FG]$ делится на \mathfrak{p}^{a+b} , но не на \mathfrak{p}^{a+b+1} .

Согласно лемме 2 в поле K существуют такие элементы $\xi, \eta \in K$, что все коэффициенты многочленов ξF и ηG лежат в D , но дивизоры $[\xi F]$ и $[\eta G]$ не делятся на \mathfrak{p} . При этом (см. доказательство леммы 2)

$$\xi = \frac{\beta}{\alpha}, \quad \eta = \frac{\delta}{\gamma},$$

где

$$\beta = a\mathfrak{b}, \quad \alpha = a\mathfrak{p}^a, \quad \delta = c\mathfrak{d}, \quad \gamma = c\mathfrak{p}^b,$$

причем $(\mathfrak{b}, \mathfrak{p}) = \mathfrak{e}$ и $(\mathfrak{d}, \mathfrak{p}) = \mathfrak{e}$. Кроме того, так как $\alpha\gamma [\xi\eta FG] = \beta\delta [FG]$, то $(\alpha\gamma) [\xi\eta FG] = (\beta\delta) [FG]$, и, значит,

$$a\mathfrak{p}^{a+b} [\xi\eta FG] = a\mathfrak{b}c [FG],$$

т. е.

$$\mathfrak{p}^{a+b} [\xi\eta FG] = \mathfrak{b}c [FG].$$

Поскольку $(\mathfrak{b}c, \mathfrak{p}) = \mathfrak{e}$, этим доказано, что дивизор $[FG]$ делится на \mathfrak{p}^{a+b} . С другой стороны, согласно лемме 1, дивизор $[\xi\eta FG]$ не делится на \mathfrak{p} , и потому дивизор $[FG]$ не делится на \mathfrak{p}^{a+b+1} . ■

Ясно, что аналог формулы (6) справедлив и для любого (конечного) числа многочлена.

Предположим теперь, что кольцо D удовлетворяет условиям теоремы 1 § 10, так что, в частности, задано n его мономорфизмов $\alpha \mapsto \alpha^{(i)}$, $i = 1, \dots, n$, в поле \mathbb{C} комплексных чисел, т. е. n изоморфизмов на некоторые подкольца $D^{(i)}$ поля \mathbb{C} . Кольцо D (и его поле отношений K) называется *нормальным*, если эти подкольца совпадают:

$$D^{(1)} = \dots = D^{(n)}.$$

Если (см. § 10) мы отождествим α с $\alpha^{(1)}$, т. е. D с $D^{(1)}$, то это условие будет равносильно требованию, чтобы для любого $i = 1, \dots, n$ и любого $\alpha \in D$ имело место включение $\alpha^{(i)} \in D$. Это показывает, в частности, что кольцо D *нормально*.

Положив $\sigma_i \alpha = \alpha^{(i)}$, $i = 1, \dots, n$, мы получим некоторые автоморфизмы $\sigma_i: D \rightarrow D$ кольца D . (Мы

предполагаем произведенным отождествление $\alpha = \alpha^{(1)}$; в противном случае следует рассмотреть отображения $\sigma_i: \alpha \mapsto \alpha^{(i)} \rightarrow \beta$, где $\beta \in D$ — такой элемент, что $\beta^{(1)} = \alpha^{(i)}$.)

Задача. Покажите, что:

1) Автоморфизмы $\sigma_1, \dots, \sigma_n$ составляют группу (по отношению к композиции).

2) Любой автоморфизм кольца D является одним из автоморфизмов σ_k .

Группа всех автоморфизмов нормального кольца D (или, что равносильно, его поля отношений K) называется *группой Галуа* кольца D (или поля K).

Группа Галуа кольца D является циклической группой порядка $l-1$ с образующей $\sigma: a(\xi) \mapsto a(\xi^g)$. См. задачу на стр. 61.

Согласно теореме 1 § 10 дивизорами кольца D можно считать его идеалы. В более педантичной формулировке это означает, что соответствие $\alpha \mapsto [\alpha]$ между дивизорами и идеалами (см. § 8) для кольца D , удовлетворяющего условиям теоремы 1 § 10, биективно. В частности, это соответствие биективно для любого нормального кольца D .

Пусть теперь α — произвольный дивизор нормального кольца D и $[\alpha]$ — соответствующий идеал. Ясно, что для любого $i = 1, \dots, n$, множество $[\alpha]^{(i)}$, состоящее из всех элементов вида $\alpha^{(i)} = \sigma_i \alpha$, где $\alpha \in [\alpha]$, является идеалом кольца D и потому имеет вид $[\alpha^{(i)}]$ для некоторого однозначно определенного дивизора $\alpha^{(i)}$. Тем самым мы получаем n отображений

$$\alpha \mapsto \alpha^{(i)}, \quad i = 1, \dots, n,$$

моноида дивизоров \mathcal{D} на себя. Очевидно, что *каждое из этих отображений является автоморфизмом*, т. е.

$$(\alpha\beta)^{(i)} = \alpha^{(i)}\beta^{(i)}$$

для любых двух дивизоров α, β и любого $i = 1, \dots, n$.

По определению идеал $[\alpha^{(i)}]$ является образом идеала $[\alpha]$ при автоморфизме σ_i . Поэтому автоморфизм σ_i индуцирует биективное отображение множества смежных классов кольца D по идеалу $[\alpha]$ на множество смежных классов кольца D по идеалу $[\alpha^{(i)}]$. В частности, эти множества имеют одно и то же число элементов. Этим доказано, что

$$(7) \quad N\alpha^{(i)} = N\alpha \quad \text{для любого } i = 1, \dots, n.$$

По построению $\alpha^{(1)} = \alpha$, но равенство $\alpha^{(i)} = \alpha$ возможно и при $i > 1$.

Задача. Покажите, что если среди дивизоров $\alpha^{(1)}, \dots, \alpha^{(n)}$ имеется e различных, то e делит n и каждый из этих e различных дивизоров встречается в ряду дивизоров $\alpha^{(1)}, \dots, \alpha^{(n)}$ ровно $f = \frac{n}{e}$ раз. (Указание. Совокупность всех σ_i , для которых $\alpha^{(i)} = \alpha$, является подгруппой группы Галуа кольца D .)

Для каждого многочлена $F(X)$ с коэффициентами из D мы будем символом $F^{(i)}(X)$ обозначать многочлен, получающийся в результате применения автоморфизма σ_i ко всем коэффициентам многочлена $F(X)$. Очевидно, что

$$[F^{(i)}] = [F]^{(i)} \quad \text{для любого } i = 1, \dots, n.$$

Поэтому, согласно предложению 4, имеет место равенство

$$[F]^{(1)} \dots [F]^{(n)} = [F^{(1)} \dots F^{(n)}].$$

Но ясно, что для каждого коэффициента α многочлена F коэффициенты многочлена $F^{(1)} \dots F^{(n)}$ представляют собой симметрические многочлены от $\alpha^{(1)}, \dots, \alpha^{(n)}$. Поскольку элементарные симметрические многочлены от $\alpha^{(1)}, \dots, \alpha^{(n)}$ являются по условию целыми числами, отсюда следует, что коэффициенты многочлена $F^{(1)} \dots F^{(n)}$ лежат в \mathbb{Z} . Поэтому их наибольший общий делитель $[F^{(1)} \dots F^{(n)}]$ представляет собой некоторое целое рациональное число $a \in \mathbb{Z}$ (т. е., точнее, является главным дивизором вида (a)). Это число однозначно определено с точностью до ассоциированности, т. е. — в данном случае — с точностью до знака. Этим доказано, что для любого дивизора $\alpha = [F]$ кольца D существует такое однозначно определенное положительное целое число a , что

$$(a) = \alpha^{(1)} \dots \alpha^{(n)}.$$

Перейдя в этом равенстве к нормам и учтя, что $a > 0$, мы в силу предложения 3 и формулы (7) получим, что

$$a^n = (Na)^n,$$

и, следовательно, что $a = Na$. Этим доказано следующее предложение:

Предложение 5. Для любого дивизора α нормального кольца D имеет место равенство

$$(8) \quad N\alpha = \alpha^{(1)} \dots \alpha^{(n)}. \blacksquare$$

Предложение 4 объясняет выбор термина «норма» для числа $N\alpha$. Ясно также, что формула (5) немедленно вытекает из формулы (8). Таким образом, для нормальных колец формулу (5) мы можем считать доказанной.

В частности, мы видим, что формула (5) справедлива для любого элемента $\alpha \in D_i$. При этом, так как $N\alpha \geq 0$ в кольце D_i , то мы окончательно получаем, что для любого элемента $\alpha \in D_i$ имеет место формула

$$(9) \quad N(\alpha) = N\alpha.$$

Из формулы (8) следует также, что целое рациональное число $N\alpha$ делится в кольце D на дивизор α .

Впрочем, этот факт можно легко установить и непосредственно, и причем для любого (не обязательно нормального) кольца D , удовлетворяющего лишь аксиоме N.

Действительно, пусть

$$(10) \quad \alpha_1, \dots, \alpha_N, \quad N = N\alpha,$$

— полная система представителей смежных классов кольца D по α . Ясно, что элементы

$$(10') \quad \alpha_1 + 1, \dots, \alpha_N + 1$$

также будут составлять полную систему представителей (если $\alpha_i + 1 \equiv \alpha_j + 1 \pmod{\alpha}$, то $\alpha_i \equiv \alpha_j \pmod{\alpha}$ и, значит, $i = j$; если $\alpha - 1 \equiv \alpha_i \pmod{\alpha}$, то $\alpha \equiv \alpha_i + 1 \pmod{\alpha}$). Это означает, что каждый из элементов (10') сравним по модулю α с одним и только одним из элементов (10). Поэтому сумма всех элементов (10') будет сравнима с суммой всех элементов (10), т. е. разность этих сумм будет делиться на α . Но ясно, что эта разность равна $N = N\alpha$. \blacksquare

Пусть теперь \wp — произвольный простой дивизор кольца D .

Предложение 6. Справедливы следующие утверждения:

1. Существует одно и только одно простое число $p \in \mathbb{Z}$, делящееся на дивизор \wp .

2. Для нормы $N_{\mathfrak{p}}$ дивизора \mathfrak{p} имеет место равенство

$$N_{\mathfrak{p}} = p^f,$$

где f — некоторое целое число, удовлетворяющее неравенствам $1 \leq f \leq n$.

3. Для любого элемента $\alpha \in D$ имеет место сравнение

$$(11) \quad \alpha^{N_{\mathfrak{p}}} \equiv \alpha \pmod{\mathfrak{p}}.$$

4. Число $N_{\mathfrak{p}}$ является наименьшим положительным числом, обладающим свойством (11) (по отношению ко всем элементам $\alpha \in D$).

Доказательство. 1. В кольце \mathbb{Z} существуют отличные от нуля числа, делящиеся на дивизор \mathfrak{p} (таким числом будет, например, норма $N_{\mathfrak{p}}$ дивизора \mathfrak{p}). Поэтому (в виду простоты дивизора \mathfrak{p}) в \mathbb{Z} существуют и простые числа, делящиеся на \mathfrak{p} . Два простых числа p и q дивизор \mathfrak{p} делить не может, так как числа p и q взаимно просты (в \mathbb{Z} , а потому и в D). Следовательно, простое число p , делящееся на \mathfrak{p} , единственно.

2. Если $p = \mathfrak{p}a$, то $N_{\mathfrak{p}} \cdot Na = Np = p^n$, и потому $N_{\mathfrak{p}} = p^f$, где $1 \leq f \leq n$.

3. Так как дивизор \mathfrak{p} прост, то прост и идеал $[\mathfrak{p}]$. Следовательно, этот идеал максимален, откуда непосредственно вытекает, что факторкольцо $D/[\mathfrak{p}]$ не имеет нетривиальных идеалов. Поэтому любой отличный от нуля элемент этого факторкольца обратим (в противном случае он порождал бы нетривиальный идеал) и, значит, факторкольцо $D/[\mathfrak{p}]$ является полем. Следовательно (см. стр. 65), его отличные от нуля элементы составляют циклическую группу порядка $N_{\mathfrak{p}} - 1$. Поскольку при возведении любого элемента конечной группы в степень, равную порядку группы, получается единица группы, этим доказано, что

$$\alpha^{N_{\mathfrak{p}}-1} \equiv 1 \pmod{\mathfrak{p}}$$

для любого элемента $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ кольца D . Умножив это сравнение на α , мы и получим сравнение (11), которое при $\alpha \equiv 0 \pmod{\mathfrak{p}}$ справедливо автоматически.

4. Поскольку группа отличных от нуля элементов поля $D/[\mathfrak{p}]$ циклическа, в ней существует элемент порядка $N_{\mathfrak{p}} - 1$. Поэтому в кольце D существует элемент α , для которого число $N_{\mathfrak{p}}$ является наименьшим положительным числом, обладающим свойством (11). ■

Утверждение 3 этого предложения является обобщением на любые простые идеалы малой теоремы Ферма. Его доказательство повторяет доказательство теоремы Ферма (см стр. 25).

Предусмотренное утверждением 2 число f называется *степенью* простого дивизора \wp .

Предложение 7. Любое простое число $p \in \mathbb{Z}$ является в кольце D произведением не более чем n простых дивизоров (среди которых могут быть и совпадающие).

Доказательство. Если $p = \wp_1 \dots \wp_k$, то $p^n = N\wp = N\wp_1 \dots N\wp_k = p^{f_1} \dots p^{f_k}$, и потому $f_1 + \dots + f_k = n$. Поскольку $f_1 \geq 1, \dots, f_k \geq 1$, это возможно только при $k \leq n$. ■

Пусть теперь $D = D_l$.

Следствие. В кольце D_l главный дивизор $l = (\lambda)$, где $\lambda = 1 - \zeta$, является простым дивизором.

Доказательство. Мы знаем (см. § 5), что $l \sim \lambda^{l-1}$, т. е. что $l = l^{l-1}$. Поэтому, если дивизор l был бы не простым, то число l было бы произведением более чем $l - 1$ простых идеалов, что, согласно предположению 7, невозможно (напомним, что $n = l - 1$ для кольца D_l). ■

Этим свойством мы пользовались в § 9 (см, стр. 102).

Покажем теперь, что в кольце D_l *никакое простое число $p \neq l$ не делится на квадрат простого дивизора.*

Действительно, пусть существует простое число $p \neq l$, делящееся на квадрат простого дивизора \wp . Рассмотрим произвольное число $\alpha = a(\zeta) \in D_l$, делящееся на \wp , но не делящееся на \wp^2 . Так как $a(X)^p \equiv a(X^p) \pmod p$ (см. формулу (11) § 1), то

$$\alpha^{p^{l-1}} = a(\zeta)^{p^{l-1}} \equiv a(\zeta^{p^{l-1}}) \pmod p,$$

а так как $p^{l-1} \equiv 1 \pmod l$, то $\zeta^{p^{l-1}} = \zeta$, и потому $a(\zeta^{p^{l-1}}) = a(\zeta) = \alpha$. Следовательно,

$$\alpha^{p^{l-1}} \equiv \alpha \pmod p,$$

и потому

$$\alpha^{p^{l-1}} \equiv \alpha \pmod{p^2}.$$

Но $p^{l-1} \geq 2$ и, значит, $\alpha^{p^{l-1}}$ делится на α^2 , а поэтому и на p^2 . Следовательно,

$$\alpha \equiv \alpha^{p^{l-1}} \equiv 0 \pmod{p^2},$$

что противоречит выбору α . Полученное противоречие показывает, что простого числа $p \neq l$, делящегося на p^2 , существовать не может. ■

Таким образом, в кольце D_l для любого простого числа $p \neq l$ имеет место равенство вида

$$(12) \quad p = p_1 \dots p_e,$$

где $p_1 \dots p_e$ — различные простые дивизоры, а $e \leq l-1$.

Пусть теперь $p = p_1$ и $Np = p^f$. Возведя равенство (12) в степень f , мы получим, что

$$Np = p_1^f \dots p_e^f.$$

Но, с другой стороны, согласно предложению 5,

$$Np = p^{(1)} \dots p^{(l-1)}.$$

Поскольку разложение любого числа в произведение простых дивизоров единственно, отсюда следует, что каждый из дивизоров $p_1 \dots p_e$ ровно f раз встречается среди дивизоров $p^{(1)}, \dots, p^{(l-1)}$ так, что, в частности, $fe = l-1$. Кроме того, так как $Np^{(i)} = p^f$ для любого $i = 1, \dots, l-1$, то $Np_k = p^f$ для любого $k = 1, \dots, e$.

Этим доказано следующее предложение:

Предложение 8. Любое простое число $p \neq l$ имеет в кольце D_l разложение вида

$$p = p_1 \dots p_e,$$

где p_1, \dots, p_e — различные простые дивизоры. Число e этих дивизоров делит число $l-1$. Все дивизоры p_1, \dots, p_e имеют одну и ту же степень f , равную $\frac{l-1}{e}$.

Степень f произвольного простого дивизора $p \neq l$ кольца D_l делит $l-1$. Если дивизор p делит простое число p , то:

а) число p делят дивизоры $p^{(1)}, \dots, p^{(l-1)}$ и только эти дивизоры;

б) степень каждого дивизора $\mathfrak{p}^{(1)}, \dots, \mathfrak{p}^{(l-1)}$ равна f , и среди них имеется $e = \frac{l-1}{f}$ различных дивизоров.

Мы видим, в частности, что степень f простых дивизоров, делящих простое число p , зависит только от числа p .

Предложение 9. Имеет место равенство

$$f = f_1,$$

где f_1 — наименьший положительный показатель, для которого

$$p^{f_1} \equiv 1 \pmod{l}.$$

Доказательство. Если $\alpha = a(\xi) \in D_l$, то

$$\alpha^p \equiv a(\xi^p) \pmod{p},$$

и потому

$$\alpha^{p^{f_1}} \equiv a(\xi^{p^{f_1}}) \pmod{p}.$$

Но, если $p^{f_1} \equiv 1 \pmod{l}$, то $\xi^{p^{f_1}} = \xi$. Следовательно, $\alpha^{p^{f_1}} \equiv \alpha \pmod{p}$, и, значит,

$$\alpha^{p^{f_1}} \equiv \alpha \pmod{\mathfrak{p}},$$

где \mathfrak{p} — произвольный простой дивизор, делящий (в кольце D_l) простое число p . Так как это верно для любого $\alpha \in D_l$, то, согласно утверждению 4 предложения 6, должно иметь место неравенство

$$p^{f_1} \geq N\mathfrak{p} = p^f,$$

т. е. неравенство $f_1 \geq f$.

С другой стороны, согласно утверждению 3 того же предложения 6, для любого элемента $\alpha \in D_l$ имеет место сравнение

$$\alpha^{N\mathfrak{p}} \equiv \alpha \pmod{\mathfrak{p}}.$$

и, в частности,

$$\xi^{N\mathfrak{p}} \equiv \xi \pmod{\mathfrak{p}}.$$

Если $N\mathfrak{p} \not\equiv 1 \pmod{l}$, то $\xi^{N\mathfrak{p}} \neq \xi$ и, значит, $\xi - \xi^{N\mathfrak{p}} \sim \lambda$, $1 - \xi = \lambda$. Поэтому $\lambda \equiv 0 \pmod{\mathfrak{p}}$, что невозможно, так как дивизор $\mathfrak{p} = (\lambda)$ прост и отличен от p . Таким

образом, $Np = pf \equiv 1 \pmod{l}$, что в силу минимальности числа f_1 возможно только при $f \geq f_1$.

Следовательно, $f = f_1$. ■

Таким образом, вид разложения простого числа $p \in D$ в произведение простых дивизоров кольца D_l (т. е. число этих простых дивизоров и их степени) зависит только от класса числа p по модулю l . На этом основании поле K_l называется *полем классов* (подразумевается по модулю l). Оно является простейшим примером полей, изучаемых в так называемой теории полей классов.

§ 14. ζ -функция поля K_l и ее вычет $s = 1$

В этом и следующем параграфах мы будем предполагать известными простейшие факты о бесконечных рядах и многомерных интегралах.

В теории чисел большую роль играет функция

$$(1) \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

называемая *ζ -функцией Римана* (хотя ее ввел еще Эйлер). Вообще говоря, аргумент s этой функции следует считать комплексным числом, но для наших целей вполне достаточно ограничиться рассмотрением вещественных s .

Из простейших признаков сходимости бесконечных рядов с положительными членами (например, из так называемого интегрального признака сходимости: для невозрастающей неотрицательной функции $f(x)$)

ряд $\sum f(n)$ сходится, если интеграл $\int_1^{\infty} f(x) dx$ сходится)

непосредственно вытекает, что при $s > 1$ ряд (1) сходится. Таким образом, формула (1) определяет функцию $\zeta(s)$ при $s > 1$.

При $s = 1$ ряд (1) расходится (он является известным гармоническим рядом). В соответствии с этим оказывается, что при $s \downarrow 1$ (т. е. при $s \rightarrow 1$ и $s > 1$) функция $\zeta(s)$ стремится к ∞ . Чтобы оценить скорость этого стремления, следует рассмотреть предельное поведение при $s \downarrow 1$ функции $(s - 1)\zeta(s)$.

Предложение 1. Имеет место равенство

$$\lim_{s \downarrow 1} (s - 1)\zeta(s) = 1.$$

Доказательство. Проще всего это утверждение можно доказать, заметив, что по теореме о среднем

$$\frac{1}{(n+1)^s} \leq \int_n^{n+1} \frac{du}{u^s} \leq \frac{1}{n^s}.$$

Поэтому (при $s > 1$)

$$\zeta(s) - 1 = \sum_{n=1}^{\infty} \frac{1}{(n+1)^s} \leq \int_1^{\infty} \frac{du}{u^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s),$$

т. е.

$$\frac{1}{s-1} = \int_1^{\infty} \frac{du}{u^s} \leq \zeta(s) \leq 1 + \int_1^{\infty} \frac{du}{u^s} = 1 + \frac{1}{s-1} = \frac{s}{s-1}.$$

Следовательно,

$$1 \leq (s-1)\zeta(s) \leq s,$$

что доказывает предложение 1. ■

Для любой функции $f(s)$, определенной при $s \geq 1$ и такой, что $\lim_{s \downarrow 1} f(s) = \infty$, предел

$$\lim_{s \downarrow 1} (s-1)f(s)$$

(когда он существует) мы будем называть *вычетом* этой функции при $s = 1$.

Таким образом, предложение 1 утверждает, что вычет функции $\zeta(s)$ при $s = 1$ равен 1.

Обобщением ζ -функции Римана является так называемая ζ -функция Дедекинда $\zeta_K(s)$ произвольного поля K алгебраических чисел, определяющаяся формулой

$$(2) \quad \zeta_K(s) = \sum_a \frac{1}{(Na)^s},$$

где суммирование распространено на все дивизоры a кольца D целых элементов поля K . (При $K = \mathbb{Q}$ и $D = \mathbb{Z}$ мы получаем, очевидно, функцию Римана $\zeta(s)$.) В интересующем нас случае поля $K = K_L$ функцию Дедекинда $\zeta_{K_L}(s)$ мы будем обозначать символом $\zeta_L(s)$.

Заметим, что поскольку ряд (2) состоит из положительных чисел, порядок расположения его членов при

условии, что ряд сходится, значения не имеет (ибо при любой перестановке членов сходящегося ряда положительных чисел его сумма не меняется).

Предложение 2. *Ряд (2) сходится при $s > 1$.*

Мы докажем (при $K = K_I$) это предложение в следующем параграфе.

Аналогично ряду (1) ряд (2) при $s = 1$, как мы увидим, расходится и $\lim_{s \downarrow 1} \xi_K(s) = \infty$. Поэтому уместен вопрос о вычете $\lim_{s \downarrow 1} (s - 1) \xi_K(s)$ функции $\xi_K(s)$ при $s = 1$. Для вычисления этого вычета целесообразно разбить ряд (2) (при $K = K_I$) на h рядов вида

$$(3) \quad \xi_I^C(s) = \sum_{a \in C} \frac{1}{(Na)^s},$$

где C — произвольный класс дивизоров, а суммирование в (3) распространено на все дивизоры класса C . Эти ряды сходятся как части сходящегося ряда $\xi_I(s)$ с положительными членами.

Предложение 3. *Существует такое число κ , что*

$$\lim_{s \downarrow 1} (s - 1) \xi_I^C(s) = \kappa$$

для любого класса C дивизоров кольца D_I .

Другими словами, для любого C вычет функции $\xi_I^C(s)$ при $s = 1$ определен и не зависит от C .

Доказательство этого предложения и будет основной целью этого параграфа.

Следствие. *Вычет функции $\xi_I(s)$ при $s = 1$ равен $h\kappa$:*

$$(4) \quad \lim_{s \downarrow 1} (s - 1) \xi_I(s) = h\kappa. \blacksquare$$

Эта формула служит ключом для явного вычисления числа классов h .

Конечно, чтобы можно было использовать формулу (4), надо предварительно вычислить число κ . Согласно предложению 3 для этого достаточно вычислить, скажем, предел

$$\lim_{s \downarrow 1} (s - 1) \xi_I^E(s),$$

где E — класс главных дивизоров (единица группы \mathcal{H}). Рассмотрим поэтому функцию

$$(5) \quad \zeta_l^E(s) = \sum_{\alpha \in E} \frac{1}{(N\alpha)^s}$$

повнимательнее.

Суммирование в (5) распространено на всевозможные главные дивизоры α , т. е. дивизоры (идеалы) вида (α) , $\alpha \in D_l^*$. Выбрав в каждом таком идеале по представителю и учтя (см. формулу (9) § 13), что $N(\alpha) = N\alpha$, мы можем переписать (5) в следующем виде:

$$(6) \quad \zeta_l^E(s) = \sum_{\alpha}' \frac{1}{(N\alpha)^s},$$

где штрих у знака суммы означает, что суммирование производится по полному набору попарно не ассоциированных чисел из D_l^* (напомним, что $(\alpha) = (\beta)$ тогда и только тогда, когда $\alpha \sim \beta$).

Чтобы вычислить (или хотя бы оценить) сумму (6), хотелось бы явным образом выбрать в D_l^* какой-нибудь полный набор попарно не ассоциированных чисел. Однако это удастся сделать лишь частично.

Л е м м а 1. *Для любых вещественных чисел y_1, \dots, y_m существует единственная система целых чисел n_1, \dots, n_m , обладающих тем свойством, что*

$$n_1 + n_2 + \dots + n_m = 0$$

и такая, что

$$(7) \quad 0 \leq x_i - \frac{x_1 + \dots + x_m}{m} < 1, \quad i = 1, \dots, m-1,$$

где $x_i = n_i + y_i$.

Заметим, что при $i = m$ мы никаких условий не накладываем.

Доказательство. Если числа n_1, \dots, n_m существуют, то

$$\frac{x_1 + \dots + x_m}{m} = \frac{y_1 + \dots + y_m}{m}.$$

Поэтому

$$0 \leq n_i + y_i - \frac{y_1 + \dots + y_m}{m} < 1, \quad i = 1, \dots, m-1,$$

и, значит,

$$(8) \quad n_i = - \left[y_i - \frac{y_1 + \dots + y_m}{m} \right], \quad i = 1, \dots, m-1.$$

Это доказывает единственность чисел n_1, \dots, n_{m-1} , а потому и числа $n_m = -(n_1 + \dots + n_{m-1})$.

Для доказательства существования этих чисел достаточно заметить, что числа n_1, \dots, n_{m-1} , задаваемые формулой (8), вместе с числом $n_m = -(n_1 + \dots + n_{m-1})$ обладают, очевидно, всеми требуемыми свойствами. ■

Как мы знаем, в кольце D_i существует h_2 таких единиц $\varepsilon_1, \dots, \varepsilon_{h_2}$, что любая единица ε кольца D_i единственным образом представляется в виде

$$(9) \quad \varepsilon = \pm \zeta^a (1 - \sigma\zeta)^{n_1} \dots (1 - \sigma^n \zeta)^{n_m} \varepsilon_i,$$

где $0 \leq a < l$, $1 \leq i \leq h_2$, а n_1, \dots, n_m — такие целые числа, что $n_1 + \dots + n_m = 0$. При этом

$$X(\varepsilon) = (n_1, \dots, n_m) + X(\varepsilon_i),$$

где $X(\varepsilon)$ — вектор $X(\alpha)$ (см. § 12) при $\alpha = \varepsilon$.

Пусть $\alpha \in D_i$ и $1 \leq i \leq h_2$. Рассмотрим вектор $(y_1, \dots, y_m) = X(\varepsilon_i) + X(\alpha) = X(\varepsilon_i \alpha)$. Применив к этому вектору лемму 1 и получив тем самым целочисленный вектор (n_1, \dots, n_m) , построим по формуле (9) некоторую единицу ε (с произвольным a). Тогда компоненты x_1, \dots, x_m вектора $X(\varepsilon \alpha)$ будут удовлетворять условиям (7). При этом для любого $\alpha \in D_i$ при выбранном i , $1 \leq i \leq h_2$, единица ε будет однозначно определена с точностью до множителя вида $\pm \zeta^a$, т. е. с точностью до $2l$ различных вариантов. Меняя i , мы увеличим число этих вариантов в h_2 раз.

Обозначив через Γ множество всех чисел $\alpha \in D_i^*$, для которых компоненты $x_1 = x_1(\alpha)$, \dots , $x_m = x_m(\alpha)$ вектора $X(\alpha)$ удовлетворяют условиям (7), мы получаем, следовательно, что *любое число из D_i^* ассоциировано ровно с $2lh_2$ числами из Γ .*

Поэтому, если в (6) мы распространим суммирование на все числа из Γ , то каждое слагаемое повторится $2lh_2$ раз. Таким образом,

$$(10) \quad \zeta_l^E(s) = \frac{1}{2lh_2} \Xi(s),$$

где

$$\Xi(s) = \sum_{\alpha \in \Gamma} \frac{1}{(N\alpha)^s}.$$

Тем самым задача сведена к вычислению вычета функции $\Xi(s)$ при $s = 1$. (Ясно, что ряд $\Xi(s)$ сходится в точности при тех же s , при которых сходится ряд $\zeta_l^E(s)$.)

Выше мы видели, что в вычислении вычета функции Римана $\zeta(s)$ решающую роль играл интеграл

$$\int_1^{\infty} \frac{du}{u^s} = \frac{1}{s-1}, \quad s > 1,$$

являющийся «континуальным аналогом» ряда $\zeta(s)$. Вычисление вычета функции $\Xi(s)$ производится тем же методом с помощью многомерного интеграла $I(s)$, являющегося континуальным аналогом ряда $\Xi(s)$.

Чтобы определить этот интеграл, нужно в первую очередь описать его область интегрирования, которая является континуальным аналогом «области суммирования» Γ ряда $\Xi(s)$.

Каждое число

$$\alpha = a_1 \sigma \zeta + \dots + a_{l-1} \sigma^{l-1} \zeta$$

кольца D_l однозначно определяет целочисленный вектор

$$\vec{\alpha} = (a_1, \dots, a_{l-1}).$$

Имея это в виду, мы рассмотрим пространство \mathbb{R}^{l-1} , точками которого являются $l-1$ -членные последовательности $u = (u_1, \dots, u_{l-1})$ вещественных чисел. Чтобы подчеркнуть его связь с кольцом D_l , мы будем обозначать это пространство символом $\mathbb{R}D_l$. Множество целочисленных точек из $\mathbb{R}D_l$, т. е. точек $u = (u_1, \dots, u_{l-1})$, для которых все числа u_1, \dots, u_{l-1}

являются целыми рациональными числами (принадлежат \mathbb{Z}), мы будем обозначать через $\mathbb{Z}D_l$ или \vec{D}_l . Последнее обозначение оправдывается тем, что отображение $\alpha \mapsto \vec{\alpha}$ является, очевидно, биективным отображением D_l на \vec{D}_l .

Для любой точки $u = (u_1, \dots, u_{l-1}) \in \mathbb{R}D_l$ мы символом ξ обозначим комплексное число

$$\xi = u_1 \sigma \zeta + \dots + u_{l-1} \sigma^{l-1} \zeta.$$

Ясно, что на подмножестве $\mathbb{Z}D_l$ отображение $u \mapsto \xi$ является биективным отображением на \vec{D}_l , обратным к отображению $\alpha \mapsto \vec{\alpha}$. На всем же $\mathbb{R}D_l$ оно, очевидно, не биективно (при $l > 3$).

Отображение $u \mapsto \xi$ является линейным отображением вещественного $(l-1)$ -мерного пространства $\mathbb{R}D_l$ на поле комплексных чисел \mathbb{C} , рассматриваемое как вещественное двумерное пространство. Поэтому ядро этого отображения имеет размерность $l-3$.

Мы положим

$$\xi_1 = u_1 \sigma \zeta + \dots + u_{l-1} \sigma^{l-1} \zeta,$$

$$\xi_2 = u_1 \sigma^2 \zeta + \dots + u_{l-1} \sigma^l \zeta,$$

$$\dots$$

$$\xi_{l-1} = u_1 \sigma^{l-1} \zeta + \dots + u_{l-1} \sigma^{2l-3} \zeta$$

(так что $\xi_1 = \xi = \xi$) и

$$Nu = \xi_1 \xi_2 \dots \xi_{l-1}.$$

Если $u \in \mathbb{Z}D_l$, то $\xi_k = \sigma^{k-1} \xi$ (это имеет смысл, поскольку $\xi \in D_l$ при $u \in \mathbb{Z}D_l$). Поэтому числа ξ_k можно условно обозначать через $\sigma^{k-1} \xi$ и для любого $u \in \mathbb{R}D_l$.

Так как $\sigma^m \zeta = \bar{\zeta}$ (где, как всегда, $m = \frac{l-1}{2}$), то

$$\xi_{m+1} = \bar{\xi}_1, \dots, \xi_{l-1} = \bar{\xi}_m,$$

и, значит,

$$Nu = |\xi_1 \xi_2 \dots \xi_m|^2.$$

Таким образом, Nu является вещественнозначной функцией на $\mathbb{R}D_l$. При этом

$$N\vec{\alpha} = N\alpha \quad \text{для любого } \alpha \in D_l.$$

Как мы знаем, $N\alpha$ является многочленом от коэффициентов a_1, \dots, a_{l-1} разложения $\alpha = a_1\sigma\xi + \dots + a_{l-1}\sigma^{l-1}\xi$. Функция Nu представляет собой тот же многочлен, в котором a_1, \dots, a_{l-1} заменены на u_1, \dots, u_{l-1} .

Если $u \in \mathbb{Z}D_l$, то, как мы знаем, $Nu = 0$ только при $u = (0, \dots, 0)$. Однако при $l > 3$ в $\mathbb{R}D_l$ есть точки $u \neq (0, \dots, 0)$, для которых $Nu = 0$.

При $Nu \neq 0$ формула

$$Lu = (\ln|\xi_1|, \dots, \ln|\xi_n|)$$

определяет вектор Lu пространства \mathbb{R}^m . При этом

$$L\vec{\alpha} = L\alpha \quad \text{для любого } \alpha \in D_l^*,$$

где $L\alpha$ — вектор, построенный в § 13.

Разложив вектор Lu по базису $L_1 = L(1 - \sigma\xi), \dots, L_m = L(1 - \sigma^m\xi)$ пространства \mathbb{R}^m (см. предложение 6 § 12), т. е., найдя такие числа $x_1(u), \dots, x_m(u) \in \mathbb{R}$, что

$$Lu = x_1(u)L_1 + \dots + x_m(u)L_m,$$

мы положим

$$X(u) = (x_1(u), \dots, x_m(u)).$$

Тем самым мы получим отображение $X: u \mapsto X(u) \in \mathbb{R}^m$, где $Nu \neq 0$, связанное с отображением $X: D_l \rightarrow \mathbb{R}^m$ из § 12 формулой

$$X(\vec{\alpha}) = X(\alpha) \quad \text{для любого } \alpha \in D_l^*.$$

Мы обозначим через Γ_R множество всех точек $u \in \mathbb{R}D_l$, для которых $Nu \geq 1$ и координаты $x_1 = x_1(u), \dots, x_m = x_m(u)$ вектора $X(u)$ удовлетворяют условиям (7). Это множество и является нужным нам континуальным аналогом множества Γ . Если обозначить через $\vec{\Gamma}$ множество всех точек вида $\vec{\alpha}$, $\alpha \in \Gamma$, то, очевидно, будет иметь место равенство $\vec{\Gamma} = \Gamma_R \cap \vec{D}_l$.

На первый взгляд кажется, что множество Γ_R устроено безнадежно сложно. Однако это первое впечатление обманчиво, и на самом деле строение множества Γ_R может быть легко описано. Для этого только нужно перейти от координат u_1, \dots, u_{l-1} к другим

Сразу же приходит на ум преобразование

вводящее вместо координат u_1, \dots, u_{l-1} координаты ξ_1, \dots, ξ_{l-1} . Определитель

этого преобразования является (ввиду соотношения $\sigma^{l-1} = 1$) антициркулянтom с последней строкой $(\sigma^{l-1}\xi, \dots, \sigma^{2l-3}\xi) = (\xi, \sigma\xi, \dots, \sigma^{l-2}\xi)$. Поэтому (см. § 13) с точностью до знака этот определитель равен произведению $l - 1$ чисел

где θ — первообразный корень из единицы степени $l-1=2m$. Поскольку при $j=0$ имеет место равенство $\beta = \zeta + \sigma\zeta + \dots + \sigma^{l-2}\zeta = -1$, мы получаем, следовательно, что определитель (12) равен $\pm \beta_1 \beta_2 \dots \beta_{l-2}$.

$$(13) \quad \begin{vmatrix} & b_{11} & \cdots & b_{1,l-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{l-1,1} & \cdots & b_{l-1,l-1} \end{vmatrix}$$

$$b_{ij} = \sum_{k=1}^{l-1} \sigma^{i+k-1} \zeta \cdot \sigma^{k+l-1} \zeta = \sum_{k=1}^{l-1} \sigma^{i+k-1} (\zeta \cdot \sigma^{l-i} \zeta) = \sum_{r=1}^{l-1} \sigma^r (\zeta \cdot \sigma^{l-i} \zeta).$$

184

Так как $\sum_{r=1}^{l-1} \sigma^r \alpha \zeta = \sum_{k=1}^{l-1} \sigma^k \zeta = -1$, этим доказано, что

$$b_{ij} = \begin{cases} l-1, & \text{если } j-i \equiv m \pmod{l-1}, \\ -1, & \text{если } j-i \not\equiv m \pmod{l-1}. \end{cases}$$

Эти формулы означают, что определитель (13) является циркулянтном с первой строкой $(-1, \dots, -1, l-1, -1, \dots, -1)$ и, значит, равен произведению $l-1$ чисел вида

$$\begin{aligned} & (-1) + (-1)\theta^j + \dots + (-1)\theta^{(m-1)j} + (l-1)\theta^{mj} + \\ & + (-1)\theta^{(m+1)j} + \dots + (-1)\theta^{(l-2)j} = \\ & = l\theta^{mj} - (1 + \theta^j + \dots + \theta^{(l-2)j}), \end{aligned}$$

где, как и выше, θ — первообразный корень из единицы степени $l-s=2m$, а $j=0, 1, \dots, l-2$. Поскольку $\theta^m = -1$, то

$$1 + \theta^j + \dots + \theta^{(l-2)j} = \begin{cases} l-1, & \text{если } j \equiv 0 \pmod{l-1}, \\ 0, & \text{если } j \not\equiv 0 \pmod{l-1} \end{cases}$$

и, следовательно, эти множители равны либо $l\theta^{mj}$ (когда $j \not\equiv 0 \pmod{l-1}$), либо $l\theta^{mj} - (l-1) = l - (l-1) = 1$ (когда $j \equiv 0 \pmod{l-1}$). Поэтому определитель (13) равен $\prod_{j=1}^{l-2} l\theta^{mj} = \pm l^{l-2}$. Таким образом,

$$(\beta_1 \dots \beta_{l-2})^2 = \pm l^{l-2}.$$

Этим, во-первых, доказано, что *определитель* (12) *отличен от нуля* и, во-вторых, что он равен

$$\pm \frac{1}{b_1 \dots b_{l-2}},$$

где $b_j = \frac{1}{l} \beta_j$, т. е.

$$(14) \quad b_j = \frac{1}{l} \sum_{k=0}^{l-2} \theta^{kj} \sigma^k \zeta = \frac{1}{l} (\zeta + \theta^j \sigma \zeta + \dots + \theta^{(l-2)j} \sigma^{l-2} \zeta),$$

$$j = 1, \dots, l-2.$$

Заметим, что по доказанному *все числа* b_1, \dots, b_{l-2} *отличны от нуля*. ■

Таким образом, мы видим, что преобразование (11) невырождено и потому описывает переход от одной системы аффинных координат к другой. Определитель обратного преобразования $(\xi_1, \dots, \xi_{l-1}) \rightarrow (u_1, \dots, u_{l-1})$ равен $\pm b_1 \dots b_{l-2}$.

Однако координаты ξ_1, \dots, ξ_{l-1} имеют тот недостаток, что они комплексны. Если же мы хотим оставаться только в вещественной области, мы должны от этих координат перейти к их вещественным и мнимым частям. Поскольку $\xi_{m+1} = \bar{\xi}_1, \dots, \xi_{l-1} = \bar{\xi}_m$ (см. выше), то нам достаточно ограничиться координатами $\xi_1 = x_1 + iy_1, \dots, \xi_m = x_m + iy_m$.

Таким образом, от вещественных координат u_1, \dots, u_{l-1} мы переходим к вещественным же координатам

$$x_1 = \frac{\xi_1 + \xi_{m+1}}{2}, \dots, x_m = \frac{\xi_1 + \xi_{l-1}}{2},$$

$$y_1 = \frac{\xi_1 - \xi_{m+1}}{2i}, \dots, y_m = \frac{\xi_1 - \xi_{l-1}}{2i}.$$

Определитель перехода от координат ξ_1, \dots, ξ_{l-1} к координатам $x_1, \dots, x_m, y_1, \dots, y_m$ равен

$$\begin{vmatrix} \frac{1}{2} & \dots & \frac{1}{2} & \dots \\ & \frac{1}{2} & \dots & \frac{1}{2} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ & & \frac{1}{2} & \dots & \frac{1}{2} \\ \frac{1}{2i} & \dots & -\frac{1}{2i} & \dots & \\ & \frac{1}{2i} & \dots & -\frac{1}{2i} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ & & \frac{1}{2i} & \dots & -\frac{1}{2i} \end{vmatrix} = \frac{1}{(-2i)^m}.$$

Поэтому определитель перехода от координат $x_1, \dots, x_m, y_1, \dots, y_m$ к координатам u_1, \dots, u_{l-1} равен

$$\pm (2i)^m b_1 \dots b_{l-2} = \pm 2^m i^m B,$$

где $B = b_1 \dots b_{l-2}$.

Обычно молчаливо предполагают координаты u_1, \dots, u_{l-1} прямоугольными. Можно считать, что $x_1, \dots, x_m, y_1, \dots, y_m$ являются не новыми (уже, вообще говоря, не прямоугольными) координатами той же точки, что и координаты u_1, \dots, u_{l-1} , а координатами в той же системе прямоугольных координат некоторой другой точки. Другими словами, формулы, выражающие координаты x_1, \dots, y_m через координаты u_1, \dots, u_{l-1} , мы можем интерпретировать как формулы, задающие некоторое аффинное преобразование евклидова пространства \mathbb{R}^l , т. е., наглядно говоря, некоторое «перекашивание» этого пространства (переводящее произвольные кубы в косые параллелепипеды).

В координатах $x_1, \dots, x_m, y_1, \dots, y_m$ область Γ_R определяется, во-первых, неравенством

$$(15) \quad (x_1^2 + y_1^2) \dots (x_m^2 + y_m^2) \geq 1$$

и, во-вторых, тем, что координаты z_1, \dots, z_m вектора

$$\left(\frac{1}{2} \ln |x_1^2 + y_1^2|, \dots, \frac{1}{2} \ln |x_m^2 + y_m^2| \right) \in \mathbb{R}^m$$

в базисе L_1, \dots, L_m удовлетворяют неравенствам

$$(16) \quad 0 \leq z_i - \frac{z_1 + \dots + z_m}{m} < 1, \\ i = 1, \dots, m-1$$

(см. условия (7)).

Круговая симметрия этих условий подсказывает переход к полярным координатам $r_1, \dots, r_m, \varphi_1, \dots, \varphi_m$. По определению

$$x_i = r_i \cos \varphi_i, \quad y_i = r_i \sin \varphi_i, \quad i = 1, \dots, m,$$

причем $r_i \geq 0$ и $0 \leq \varphi_i < 2\pi$. В этих координатах неравенство (15) приобретает вид $r_1 r_2 \dots r_m \geq 1$. В неравенствах же (16) числа z_1, \dots, z_m будут теперь координатами вектора $(\ln r_1, \dots, \ln r_m) \in \mathbb{R}^m$ в базисе L_1, \dots, L_m .

Преобразование координат $(x_1, \dots, x_m, y_1, \dots, y_m) \rightarrow (r_1, \dots, r_m, \varphi_1, \dots, \varphi_m)$ нелинейно. Якобиан обратного преобразования $(r_1, \dots, r_m, \varphi_1, \dots, \varphi_m) \rightarrow (x_1, \dots, x_m, y_1, \dots, y_m)$ равен, как нетрудно видеть, r_1, \dots, r_m .

Вид вектора $(\ln r_1, \dots, \ln r_m)$ подсказывает, что вместо координат r_1, \dots, r_m целесообразно ввести координаты

$$(17) \quad q_1 = \ln r_1, \dots, q_m = \ln r_m,$$

(а координаты $\varphi_1, \dots, \varphi_m$ можно оставить прежними). Тогда в неравенствах (16) числа z_1, \dots, z_m будут координатами вектора (q_1, \dots, q_m) в базисе L_1, \dots, L_m , а неравенство (15) приобретет вид

$$(18) \quad q_1 + \dots + q_m > 0.$$

Якобиан преобразования (17) равен, очевидно, $(r_1 \dots r_m)^{-1}$. Поэтому якобиан сквозного преобразования $(q_1, \dots, q_m, \Phi_1, \dots, \Phi_m) \rightarrow (x_1, \dots, x_m, y_1, \dots, y_m)$ будет равен $(r_1 \dots r_m)^2 = e^{2(q_1 + \dots + q_m)}$.

Координаты q_1, \dots, q_m мы можем считать, подобно координатам r_1, \dots, r_m , полярными координатами, а преобразование (17) представлять себе как логарифмическое изменение масштабов по каждой из полярных осей.

Тот факт, что в описании области Γ_R участвуют координаты z_1, \dots, z_m , подсказывает мысль перейти к этим координатам. По построению они связаны с координатами q_1, \dots, q_m формулами

$$(19) \quad \begin{aligned} q_1 &= \ln|1 - \sigma\xi| \cdot z_1 + \dots + \ln|1 - \sigma^m\xi| \cdot z_m, \\ q_2 &= \ln|1 - \sigma^2\xi| \cdot z_1 + \dots + \ln|1 - \sigma^{m+1}\xi| \cdot z_m, \\ &\vdots \\ q_m &= \ln|1 - \sigma^m\xi| \cdot z_1 + \dots + \ln|1 - \sigma^{2m-1}\xi| \cdot z_m. \end{aligned}$$

Определитель этого преобразования, как мы знаем (см. § 12), равен $\frac{1}{2} \ln l \cdot C$, где C — произведение чисел c_1, \dots, c_{m-1} , определенных формулой (37) § 12 (согласно лемме 2 § 12, которая у нас, правда, еще не доказана, C отлично от нуля).

Кроме того, мы знаем (см. формулу (39) § 12), что суммы элементов каждого столбца определителя преобразования (19) равны $\frac{1}{2} \ln l$. Это означает, что для суммы $q_1 + \dots + q_m$ имеет место равенство

$$(20) \quad q_1 + \dots + q_m = \frac{1}{2} \ln l \cdot (z_1 + \dots + z_m).$$

Следовательно, в координатах $z_1, \dots, z_m, \varphi_1, \dots, \varphi_m$ область Γ_R описывается неравенствами $z_1 + \dots + z_m \geq 0$ и (16).

Здесь напрашиваются координаты

$$(21) \quad \begin{aligned} t_1 &= z_1 - \frac{z_1 + \dots + z_m}{m}, \\ &\dots \dots \dots \\ t_{m-1} &= z_{m-1} - \frac{z_1 + \dots + z_m}{m}, \\ t &= z_1 + \dots + z_m. \end{aligned}$$

Определитель этого преобразования равен единице.

В координатах $t_1, \dots, t_{m-1}, t, \varphi_1, \dots, \varphi_m$ область Γ_R задается неравенствами

$$0 \leq t_1 < 1, \dots, 0 \leq t_{m-1} < 1, \quad t \geq 0,$$

т. е. представляет собой произведение (в том же смысле, как квадрат является произведением двух отрезков, а куб — трех) $m-1$ единичных полуинтервалов $0 \leq t_i < 1$, полупрямой $t > 0$ и m полуинтервалов $0 \leq \varphi_i < 2\pi$. Мы видим, таким образом, что в этих координатах область Γ_R представляет собой не что иное, как «бесконечный брус», основанием которого является параллелепипед размерности $l-2 = 2m-1$.

Впрочем, поскольку $\varphi_1, \dots, \varphi_m$ являются, по построению, угловыми координатами, лучше интерпретировать координаты t_1, \dots, t_{m-1}, t как соответствующие полярные радиусы. Тогда Γ_R будет представлять собой произведение $m-1$ кругов, каждый из которых на плоскости с полярными координатами t_i, φ_i , $i = 1, \dots, m-1$, задается неравенством $t_i < 1$, и полной плоскости с полярными координатами t, φ_m .

При переходе от координат $t_1, \dots, t_{m-1}, t, \varphi_1, \dots, \varphi_m$ к координатам $q_1, \dots, q_m, \varphi_1, \dots, \varphi_m$ происходит лишь аффинное перекашивание по первым m координатам. При переходе к координатам $r_1, \dots, r_m, \varphi_1, \dots, \varphi_m$ происходит логарифмическое изменение масштаба по первым m координатным осям. Затем для любого $i = 1, \dots, m$ полярные координаты r_i, φ_i преобразуются в прямоугольные координаты x_i, y_i , и, наконец, в результате еще одного аффинного перекашивания получается исходная область Γ_R в координатах u_1, \dots, u_{l-1} .

Полученное описание области Γ_R позволяет немедленно вычислить интеграл

$$I(s) = \int_{\Gamma_R} \frac{du}{(Nu)^s}, \quad du = du_1 \dots du_{l-1},$$

являющийся континуальным аналогом ряда $\Xi(s)$. Действительно, при переходе от u_1, \dots, u_{l-1} к x_1, \dots, x_m ,

y_1, \dots, y_m подынтегральная функция $(Nu)^{-s}$ примет, очевидно, вид

$$\frac{1}{(x_1^2 + y_1^2)^s \dots (x_m^2 + y_m^2)^s},$$

а так как (по правилу замены переменных в многомерных интегралах) она должна быть еще умножена на якобиан обратного преобразования $(x_1, \dots, x_m, y_1, \dots, y_m) \rightarrow (u_1, \dots, u_{i-1})$ и так как этот якобиан является просто определителем $\pm 2^m i^m B$ этого преобразования, то

$$I(s) = \pm 2^m i^m B \int_{\Gamma_R} \frac{dx_1 \dots dx_m dy_1 \dots dy_m}{(x_1^2 + y_1^2)^s \dots (x_m^2 + y_m^2)^s}.$$

Затем, при переходе от координат $x_1, \dots, x_m, y_1, \dots, y_m$ к координатам $q_1, \dots, q_m, \varphi_1, \dots, \varphi_m$, подынтегральная функция примет вид $e^{-2s(q_1 + \dots + q_m)}$, а умноженная на якобиан $e^{2(q_1 + \dots + q_m)}$ обратного преобразования — вид $e^{-2(s-1)(q_1 + \dots + q_m)}$. Так как эта функция не зависит от координат $\varphi_1, \dots, \varphi_m$, то по этим координатам можно произвести интегрирование, что даст нам множитель $(2\pi)^m$. Таким образом,

$$I(s) = \pm 2^{2m} i^m \pi^m B \int_{\Delta} e^{-2(s-1)(q_1 + \dots + q_m)} dq_1 \dots dq_m,$$

где Δ — область пространства переменных q_1, \dots, q_m , выделяемая неравенствами (18) и (16) (в которых z_1, \dots, z_m — координаты, связанные с координатами q_1, \dots, q_m соотношениями (19)).

Наконец, в координатах t_1, \dots, t_{m-1}, t (в которых область Δ является бруском $0 \leq t_1 < 1, \dots, 0 \leq t_{m-1} < 1, t \geq 0$) подынтегральная функция приобретет (см. формулу (20)) вид $e^{-(s-1) \ln l \cdot t}$ и умножится на якобиан $\frac{1}{2} \ln l \cdot C$ преобразования $(t_1, \dots, t_{m-1}, t) \rightarrow (q_1, \dots, q_m)$. Производя по t_1, \dots, t_{m-1} интегрирования (что даст множители, равные единице), мы, следовательно, получим, что

$$I(s) = \pm 2^{2m-1} i^m \pi^m \ln l \cdot BC \int_0^\infty e^{-(s-1) \ln l \cdot t} dt.$$

Участвующий здесь несобственный интеграл

$$\int_0^{\infty} e^{-(s-1) \ln l \cdot t} dt$$

при $s > 1$ существует (сходится) и равен

$$\frac{1}{\ln l \cdot (s-1)} \int_0^{\infty} e^{-\tau} d\tau = \frac{1}{\ln l \cdot (s-1)}.$$

Кроме того, ясно, что $I(s) > 0$ при любом s , при котором $I(s)$ существует.

Этим доказано, что при $s > 1$ интеграл $I(s)$ сходится и выражается формулой

$$I(s) = 2^{2m-1} \pi^m \cdot |B| \cdot |C| \cdot \frac{1}{s-1},$$

где B — произведение чисел b_1, \dots, b_{l-2} , определенных формулой (14), а C — произведение чисел c_1, \dots, c_{m-1} , определенных формулой (37) § 12. ■

Поэтому

$$(22) \quad \lim_{s \downarrow 1} (s-1) I(s) = 2^{2m-1} \pi^m |B| \cdot |C|.$$

Чтобы сравнить теперь интеграл $I(s)$ с рядом $\Xi(s)$, мы разобьем область Γ_R на области $\Gamma_R^{(n)}$, $n = 0, 1, \dots$, отнеся к $\Gamma_R^{(n)}$ точки $u \in \Gamma_R$, для которых

$$2^{n(l-1)} \leq Nu \leq 2^{(n+1)(l-1)}.$$

Таким образом, в частности, область $\Gamma_R^{(0)}$ состоит из всех точек $u \in \Gamma_R$, для которых

$$1 \leq Nu \leq 2^{l-1}.$$

В координатах $t_1, \dots, t_{m-1}, t, \varphi_1, \dots, \varphi_m$ область $\Gamma_R^{(n)}$ определяется (как подобласть области Γ_R) неравенствами

$$n \leq \frac{t}{(l-1) \log_2 l} \leq n+1$$

и, следовательно, представляет собой параллелепипед, отрезанный от бруса Γ_R . Таким образом, разложение области Γ_R в объединение областей $\Gamma_R^{(n)}$ можно представлять себе как разложение прямоугольного бесконечного бруса Γ_R в объединение параллелепипедов $\Gamma_R^{(n)}$.

Так как для любого n область $\Gamma_{\mathbb{R}}^{(n)}$ ограничена, то множество $\vec{\Gamma}^{(n)}$ точек из $\Gamma_{\mathbb{R}}^{(n)}$ с целочисленными координатами конечно. Поэтому конечно и множество $\Gamma^{(n)}$ элементов $\alpha \in \Gamma$, для которых $\vec{\alpha} \in \Gamma_{\mathbb{R}}^{(n)}$, находящееся в биективном соответствии с множеством $\vec{\Gamma}^{(n)}$. Мы положим

$$I_n(s) = \int_{\Gamma_{\mathbb{R}}^{(n)}} \frac{du}{(Nu)^s}, \quad \Xi_n(s) = \sum_{\alpha \in \Gamma^{(n)}} \frac{1}{(N\alpha)^s}.$$

Интеграл $I_n(s)$ является обыкновенным (собственным) интегралом, а сумма $\Xi_n(s)$ конечна. Поэтому функции $I_n(s)$ и $\Xi_n(s)$ от s определены при любом s .

Поскольку интеграл $I(s)$ и ряд $\Xi(s)$ при $s > 1$ сходятся (и являются соответственно интегралом от положительной функции и рядом с положительными членами), то при $s > 1$ имеют место разложения в сходящиеся ряды

$$I(s) = I_0(s) + I_1(s) + \dots + I_n(s) + \dots$$

$$\Xi(s) = \Xi_0(s) + \Xi_1(s) + \dots + \Xi_n(s) + \dots$$

Заметим, что утверждение о сходимости интеграла $I(s)$ выше было доказано, а утверждение о сходимости ряда $\Xi(s)$ опирается на еще не доказанное предложение 2.

Мы осуществим сравнение функций $I(s)$ и $\Xi(s)$, сравнив для любого n функции $I_n(s)$ и $\Xi_n(s)$.

При умножении вектора $u = (u_1, \dots, u_{l-1})$ на произвольное вещественное число $c > 0$ число $\xi = u_1 \sigma \xi + \dots + u_{l-1} \sigma^{l-1} \xi$, а значит, и все числа $\xi_1 = \xi$, $\xi_2 = \sigma \xi$, ..., $\xi_{l-1} = \sigma^{l-2} \xi$ также умножаются на c . Отсюда следует, во-первых, что функция $u \mapsto Nu$ является положительно однородной функцией степени $l-1$, т. е. $N(cu) = c^{l-1}Nu$ для любого $c > 0$, и, во-вторых, что $L(cu) = Lu + \ln c \cdot E$, $E = (1, \dots, 1)$.

Поскольку $E = \frac{2}{\ln l} (L_1 + \dots + L_m)$ (см. формулу (39) § 12), отсюда вытекает, что для любого $i = 1, \dots, m$ имеют место равенства

$$x_i(cu) = x_i(u) + d, \quad \text{где} \quad d = \frac{2 \ln c}{\ln l}.$$

Но ясно, что при преобразовании $x_i \mapsto x_i + d$ числа

$$x_i - \frac{x_1 + \dots + x_m}{m}$$

не меняются. Поэтому, если $u \in \Gamma_R$, то $cu \in \Gamma_R$, если, конечно, $N(cu) \geq 1$. Таким образом, если $u \in \Gamma_R$ и $c^{l-1}Nu \geq 1$, то $cu \in \Gamma_R$.

В частности, если $u \in \Gamma_R^{(n)}$, то $2^{-n(l-1)}Nu \geq 1$ и, значит, $2^{-n}u \in \Gamma_R$ и, более того, $2^{-n}u \in \Gamma_R^{(0)}$. Обратно, если $2^{-n}u \in \Gamma_R^{(0)}$, то автоматически $2^{n(l-1)}N(2^{-n}u) \geq 1$ и, значит, $u \in \Gamma_R$ и $u \in \Gamma_R^{(n)}$. Таким образом,

$$u \in \Gamma_R^{(n)} \text{ тогда и только тогда, когда } 2^{-n}u \in \Gamma_R^{(0)}.$$

В наглядных обозначениях

$$\Gamma_R^{(n)} = 2^n \Gamma_R^{(0)}.$$

Отсюда, между прочим, следует, что

$$I_n(s) = 2^{-n(l-1)(s-1)} I_0(s).$$

Однако этот факт нам не понадобится.

Как известно, любая ограниченная область евклидова пространства с кусочно-гладкой границей имеет объем («кубируема») или, другими словами, граница такой области имеет объем, равный нулю. Ключевым пунктом в доказательстве этой теоремы является утверждение о том, что для произвольного ε -кубильяжа пространства (разбиения его на непересекающиеся кубы с ребрами длины ε) число кубов этого кубильяжа, пересекающих границу области, не превосходит $\text{const} \cdot \varepsilon^{-(N-1)}$, где N — размерность пространства. (Действительно, тогда объем всех этих кубов не превосходит $\text{const} \cdot \varepsilon^{-(N-1)} \cdot \varepsilon^N = \text{const} \cdot \varepsilon$ и потому стремится к нулю, когда $\varepsilon \rightarrow 0$.)

Эта теорема применима, в частности, к области $\Gamma_R^{(n)}$, которая, как мы знаем, получается гладкими преобразованиями координат из некоторого параллелепипеда и потому имеет кусочно-гладкую границу.

Рассмотрим кубильяж \mathcal{Q} пространства $\mathbb{R}D_l$, состоящий из единичных кубов с центрами в целочисленных точках. (Каждый такой куб Q однозначно определяет своим центром $a = (a_1, \dots, a_{l-1})$ и состоит из всех

точек $u = (u_1, \dots, u_{l-1})$, для которых $|u_1 - a_1| \leq \frac{1}{2}, \dots$
 $\dots, |u_{l-1} - a_{l-1}| \leq \frac{1}{2}$. При гомотетии $u \mapsto 2^{-n}u$ этот кубильяж переходит в 2^{-n} -кубильяж $2^{-n}Q$, состоящий из кубов $2^{-n}Q$.

Согласно сказанному выше число кубов кубильяжа $2^{-n}Q$, пересекающих границу области $\Gamma_R^{(0)} = 2^{-n}\Gamma_R^{(n)}$, не превосходит $\text{const} \cdot 2^{-n(l-2)}$ и, следовательно, число кубов кубильяжа Q , пересекающих границу области $\Gamma_R^{(n)}$, не превосходит $\text{const} \cdot 2^{-n(l-2)}$.

Для любого куба Q кубильяжа Q мы положим

$$I_n^Q(s) = \int_{Q \cap \Gamma_R^{(n)}} \frac{du}{(Nu)^s}, \quad \Xi_n^Q(s) = \sum_{a \in Q \cap \Gamma^{(n)}} \frac{1}{(Na)^s}.$$

Ясно, что

$$I_n(s) = \sum_{Q \in Q} I_n^Q(s), \quad \Xi_n(s) = \sum_{Q \in Q} \Xi_n^Q(s),$$

причем, поскольку $I_n^Q(s) = 0$ и $\Xi_n^Q(s) = 0$, если $Q \cap \Gamma_R^{(n)} = \emptyset$, число отличных от нуля слагаемых в обоих суммах конечно, и потому эти суммы имеют смысл. Следовательно,

$$|I_n(s) - \Xi_n(s)| \leq \sum_{Q \in Q} |I_n^Q(s) - \Xi_n^Q(s)| = \\ = \sum^I |I_n^Q(s) - \Xi_n^Q(s)| + \sum^{II} |I_n^Q(s) - \Xi_n^Q(s)|,$$

где сумма \sum^I распространена на все кубы Q , целиком лежащие в области $\Gamma_R^{(n)}$, а сумма \sum^{II} — на кубы Q , пересекающие границу области $\Gamma_R^{(n)}$.

Оценка суммы \sum^{II} труда не представляет. Действительно, ясно, что функция $\Xi_n^Q(s)$ равна либо нулю (когда центр a куба Q не лежит в $\Gamma_R^{(n)}$), либо $(Na)^{-s}$ (когда $a \in \Gamma_R^{(n)}$). В обоих случаях

$$0 \leq \Xi_n^Q(s) \leq \frac{1}{(2^n(l-1))^s} \leq \frac{1}{2^{n(l-1)}} \quad \text{при } s \geq 1.$$

Аналогично

$$0 \leq I_n^Q(s) \leq \int_Q \frac{du}{(Na)^s} \leq \frac{1}{(2^n(l-1))^s} \leq \frac{1}{2^{n(l-1)}} \quad \text{при } s \geq 1.$$

Поэтому

$$|I_n^Q(s) - \Xi_n^Q(s)| \leq \frac{2}{2^{n(l-1)}} \quad \text{при } s \geq 1$$

и, значит,

$$(23) \quad \sum^{\text{II}} |I_n^Q(s) - \Xi_n^Q(s)| \leq \text{const} \cdot \frac{1}{2^n} \quad \text{при } s \geq 1,$$

поскольку число слагаемых в этой сумме не превосходит, как мы знаем, $\text{const} \cdot 2^{n(l-2)}$.

Заметим, что эта оценка имеет место не только при $s > 1$, но и при $s = 1$.

Оценка суммы \sum^{I} более деликатна.

Пусть a — центр куба $Q \subset \Gamma_R^{(n)}$. Тогда

$$(24) \quad \Xi_n^Q(s) = \frac{1}{(Na)^s} = \int_Q \frac{du}{(Nu)^s},$$

и потому

$$\begin{aligned} |I_n^Q(s) - \Xi_n^Q(s)| &= \left| \int_Q \left(\frac{1}{(Nu)^s} - \frac{1}{(Na)^s} \right) du \right| \leq \\ &\leq \max_Q \left| \frac{1}{(Nu)^s} - \frac{1}{(Na)^s} \right|. \end{aligned}$$

Но

$$\begin{aligned} \left| \frac{1}{(Nu)^s} - \frac{1}{(Na)^s} \right| &= \left| \int_I d \left(\frac{1}{(Nu)^s} \right) \right| = \left| s \int_I \frac{d \ln Nu}{(Nu)^s} \right| \leq \\ &\leq s \cdot \max_I \frac{1}{(Nu)^s} \cdot \left| \int_I d \ln Nu \right|. \end{aligned}$$

где I — прямолинейный отрезок, соединяющий в кубе Q его центр a с точкой u . При этом, так как

$$\frac{Na}{Nu} \leq \frac{2^{(n+1)(l-1)}}{2^{n(l-1)}} = 2^{l-1},$$

в кубе $Q \subset \Gamma_R^{(n)}$, то

$$s \cdot \max \frac{1}{(Nu)^s} \leq \frac{s \cdot 2^{(l-1)s}}{(Na)^s} \leq \frac{2^{2(l-1)+1}}{Na} \quad \text{при } 1 \leq s \leq 2.$$

С другой стороны, в силу однородности функции Nu , имеет место равенство

$$\int_I d \ln Nu = \int_{2^{-n}I} d \ln Nu,$$

где $2^{-n}I$ — отрезок в кубе $2^{-n}Q$ (а значит, и в области $\Gamma_R^{(0)}$), соединяющий точку $2^{-n}a$ с точкой $2^{-n}u$. Поскольку длина отрезка $2^{-n}I$ не превосходит, очевидно, $\text{const} \cdot 2^{-n}$, отсюда следует, что

$$\left| \int_I d \ln Nu \right| \leq \text{const} \cdot 2^{-n},$$

где константа очевидным образом выражается через верхнюю грань частных производных функций $\ln Nu$ в (ограниченной!) области $\Gamma_R^{(0)}$. Так как $Na \leq 2^{(n+1)(l-1)}$, то $2^{-n} \leq 2(Na)^{-\frac{1}{l-1}}$ и, следовательно,

$$\left| \int_I d \ln Nu \right| \leq \text{const} \cdot \frac{1}{(Na)^{\frac{1}{l-1}}}.$$

Этим доказано, что для любого куба $Q \subset \Gamma_R^{(n)}$ имеет место оценка

$$|I_n^Q(s) - \Xi_n^Q(s)| \leq \text{const} \cdot \frac{1}{(Na)^{1+\frac{1}{l-1}}} \quad \text{при } 1 \leq s \leq 2,$$

где a — центр куба Q . Поэтому

$$(25) \quad \sum^I |I_n^Q(s) - \Xi_n^Q(s)| \leq \text{const} \sum_a \frac{1}{(Na)^{1+\frac{1}{l-1}}},$$

где правая сумма распространена на все целочисленные точки $a \in \vec{\Gamma}^{(n)}$, обладающие тем свойством, что соответствующий куб Q целиком содержится в $\Gamma_R^{(n)}$. Ясно, что неравенство только усилится, если мы распространим суммирование вообще на все целочисленные точки $a \in \vec{\Gamma}^{(n)}$. Поскольку тогда эта сумма будет по определению равна $\Xi_n \left(1 + \frac{1}{l-1}\right)$, этим доказано, что при $1 \leq s \leq 2$ имеет место оценка

$$\sum^I |I_n^Q(s) - \Xi_n^Q(s)| \leq \text{const} \cdot \Xi_n \left(1 + \frac{1}{l-1}\right).$$

Следовательно, при $1 \leq s \leq 2$

$$|I_n(s) - \Xi_n(s)| \leq \text{const} \cdot \frac{1}{2^n} + \text{const} \cdot \Xi_n \left(1 + \frac{1}{l-1}\right)$$

и, значит, при $1 < s \leq 2$

$$|I(s) - \Xi(s)| \leq \text{const} \cdot \frac{1}{1 - \frac{1}{2}} + \text{const} \cdot \Xi \left(1 + \frac{1}{l-1}\right),$$

т. е.

$$|I(s) - \Xi(s)| \leq \text{const}.$$

(Заметим, что в этой оценке мы пользуемся еще недоказанной сходимостью ряда $\Xi(s)$ при $s > 1$.) Полученное неравенство означает, что

$$I(s) - \text{const} \leq \Xi(s) \leq I(s) + \text{const} \quad \text{при} \quad 1 < s \leq 2.$$

Умножив эти неравенства на $s - 1$ и перейдя к пределу, мы немедленно получим, что функции $I(s)$ и $\Xi(s)$ имеют при $s = 1$ одинаковые вычеты:

$$\lim_{s \downarrow 1} (s - 1) \Xi(s) = \lim_{s \downarrow 1} (s - 1) I(s).$$

Учитывая формулу (22), мы видим, что тем самым нами доказано следующее предложение:

Предложение 4. *Вычет функции $\Xi(s)$ при $s = 1$ равен*

$$2^{2m-1} \pi^{m_1} |B| \cdot |C|,$$

где

$$B = b_1 \dots b_{l-2}, \quad C = c_1, \dots, c_{m-1}$$

и

$$b_j = \frac{1}{l} \sum_{k=0}^{l-2} \theta^{jk} \sigma^k \zeta, \quad j = 1, \dots, l-2,$$

$$c_r = \sum_{k=0}^{m-1} \theta^{2rk} \ln |1 - \sigma^k \zeta|, \quad r = 1, \dots, m-1$$

(θ — первообразный корень из единицы степени $l-1 = 2m$).

Следствие. Вычет κ функции $\zeta_l^E(s)$ при $s = 1$ выражается формулой

$$(26) \quad \kappa = \frac{2^{2m-2} \pi^m}{lh_2} |B| \cdot |C|. \quad \blacksquare$$

Очевидно, что в оценке (25) можно не предполагать, что точки a являются центрами кубов Q . Все, понятно, полностью сохранится, если эти точки произвольно выбрать в этих кубах. То же самое верно и для всех остальных оценок. Поэтому, если в каждом кубе Q кубильяжа \mathcal{Q} выбрано по точке a_Q и введена в рассмотрение функция

$$(27) \quad \widehat{\Xi}(s) = \sum_{a_Q \in \Gamma_R} \frac{1}{(Na_Q)^s},$$

где суммирование распространено на все кубы из \mathcal{Q} , для которых $a_Q \in \Gamma_R$, то при условии, что ряд (27) при $s > 1$ сходится, будет иметь место равенство

$$\lim_{s \downarrow 1} (s-1) \widehat{\Xi}(s) = \lim_{s \downarrow 1} (s-1) I(s).$$

Более того, рассмотрим вместо кубильяжа \mathcal{Q} произвольный кубильяж \mathcal{Q}^* пространства $\mathbb{R}D_l$ на кубы со стороной $c > 0$. Тогда в равенстве (24) нужно будет правую часть разделить на объем c^{l-1} этих кубов:

$$\Xi_n^Q(s) = \frac{1}{c^{l-1}} \int_Q \frac{du}{(Na)^s}.$$

Поэтому все дальнейшие оценки вплоть до оценки (25) будут иметь место не для разности $|I_n^Q(s) - \Xi_n^Q(s)|$, а для разности $|I_n^Q(s) - c^{l-1} \Xi_n^Q(s)|$. Это доказывает, что для функции (27), построенной по кубильяжу \mathcal{Q} (и произвольно выбранным точкам $a_Q \in Q$) имеет место равенство

$$(28) \quad \lim_{s \downarrow 1} (s-1) \widehat{\Xi}(s) = \frac{1}{c^{l-1}} \lim_{s \downarrow 1} (s-1) I(s).$$

Дальнейшее обобщение состоит в том, что в каждом кубе Q кубильяжа \mathcal{Q}^* выбирается не одна, а не-

сколько точек $a_Q^{(1)}, \dots, a_Q^{(v)}$, число v которых одно и то же для всех кубов, и рассматривается функция:

$$(29) \quad H(s) = \sum_{i=1}^v \sum_{a_Q^{(i)} \in \Gamma_R} \frac{1}{(Na_Q^{(i)})^s} = \\ = \Xi^{(1)}(s) + \dots + \Xi^{(v)}(s).$$

где

$$\Xi^{(i)}(s) = \sum_{a_Q^{(i)} \in \Gamma_R} \frac{1}{(Na_Q^{(i)})^s}, \quad i = 1, \dots, v,$$

— функция (27), построенная для точек $a_Q^{(i)}$. Поскольку для каждой функции $\Xi^{(i)}(s)$ имеет место соотношение (28), то, суммируя по i , мы получаем, что *вычет функции $H(s)$ при $s = 1$ выражается формулой*

$$\lim_{s \downarrow 1} (s-1)H(s) = \frac{v}{c^{l-1}} \lim_{s \downarrow 1} (s-1)I(s) = \\ = \frac{v}{c^{l-1}} \cdot 2^{2m-1} \pi^m |B| \cdot |C|.$$

(Конечно, здесь также предполагается, что ряд (29) при $s > 1$ сходится.)

Эту общую формулу мы применим к вычислению вычета функции

$$(30) \quad \Xi_{(c)}(s) = \sum_{\alpha \in \Gamma \cap [c]} \frac{1}{(N\alpha)^s} = \sum_{a \in \Gamma_{\mathbb{P}} \cap \vec{c}} \frac{1}{(Na)^s},$$

где суммирование распространено на все числа $\alpha \in \Gamma$, делящиеся на данный дивизор c (т. е. принадлежащие идеалу $[c]$).

Справа в формуле (30) символом \vec{c} обозначено подмножество пространства $\mathbb{R}D_l$, состоящее из всех векторов вида $\vec{\alpha}$, где $\alpha \in [c]$. Ясно, что это множество является группой по сложению.

Пусть Q_0 — куб в пространстве $\mathbb{R}D_l$, определяемый неравенствами

$$-\frac{1}{2} < u_i < c - \frac{1}{2}, \quad i = 1, \dots, l-s,$$

где $c = Nt$, и пусть $Q(c)$ — кубильяж, состоящий из трансляций куба Q на всевозможные целочисленные

векторы кратные c , т. е. такие, что все их координаты делятся на c .

Поскольку \vec{c} целые числа, делящиеся на c , делятся и на c , группа \vec{c} инвариантна относительно трансляций на векторы, кратные c . Поэтому для любого целочисленного вектора $a \in \mathbb{Z}D_l$ куб $a + Q_0$, получающийся из куба Q_0 трансляцией на вектор a , и, в частности, любой куб Q кубильяжа $\vec{Q}(c)$ содержит столько же точек $a_Q^{(1)}, \dots, a_Q^{(v)}$ из группы \vec{c} , сколько и куб Q_0 . (Заметим, что на границе куба Q_0 вообще нет точек из \vec{c}). Это показывает, что функция $\Xi_{(c)}(s)$ представляет собой функцию (29), построенную для кубильяжа $\vec{Q}(c)$ и точек $a_Q^{(1)}, \dots, a_Q^{(v)}$. Поэтому (если, конечно, ряд (30) при $s > 1$ сходится)

$$\lim_{s \downarrow 1} (s-1) \Xi_{(c)}(s) = \frac{v}{(Nc)^{l-1}} \cdot 2^{2m-1} \pi^m |B| \cdot |C|,$$

где v — число точек множества $\vec{c} \cap Q_0$.

Впрочем, число v легко вычисляется. Действительно, так как для любого целочисленного вектора $a \in \mathbb{Z}D_l$ куб $a + Q_0$ содержит столько же (т. е. v) точек группы \vec{c} , сколько и куб Q_0 , то каждый смежный класс $a + \vec{c}$ группы $\mathbb{Z}D_l = \vec{D}_l$ по подгруппе \vec{c} также имеет в кубе Q ровно v точек. Число же всех смежных классов группы \vec{D}_l по подгруппе \vec{c} равно числу смежных классов группы D_l по подгруппе $[c]$ (ибо соответствие $\alpha \mapsto \vec{\alpha}$ является изоморфным отображением D_l на \vec{D}_l и $[c]$ на \vec{c}), и значит, равно норме Nc дивизора c . Следовательно, общее число всех точек из $\mathbb{Z}D_l$ (т. е. всех целочисленных точек из $\mathbb{R}D_l$), содержащихся в кубе Q_0 , равно vNc . С другой стороны, это число равно объему $c^{l-1} = (Nc)^{l-1}$ куба Q_0 . Следовательно, $v = (Nc)^{l-2}$.

Этим доказано, что для любого дивизора c кольца D_l вычет функции $\Xi_{(c)}(s)$ при $s = 1$ выражается формулой

$$(31) \quad \lim_{s \downarrow 1} (s-1) \Xi_{(c)}(s) = \frac{2^{2m-1} \pi^m}{Nc} \cdot |B| \cdot |C|,$$

отличаясь, таким образом, от вычета функции $\Xi(s)$ лишь множителем $(Nc)^{-1}$.

Этот результат можно было бы предугадать, поскольку вычет функции $\Xi_{(c)}(s)$ в определенном смысле характеризует долю чисел, делящихся на дивизор c , среди всех чисел кольца D_I , а эта доля как раз и равна $(Nc)^{-1}$.

Теперь мы уже без труда можем доказать предложение 3.

Доказательство предложения 3. Пусть c — произвольный дивизор класса C^{-1} , обратного к классу C . Тогда для любого дивизора $a \in C$ дивизор ac будет главным дивизором, делящимся на дивизор c . Обратно, для любого главного дивизора, делящегося на дивизор c , т. е. имеющего вид ac , дивизор a принадлежит классу C . Поэтому мы можем считать, что в формуле (3) суммирование производится по всем главным дивизорам, делящимся на дивизор c . Конечно (ср. формулу (6)), вместо того чтобы суммировать по главным дивизорам, мы можем суммировать по всем попарно не ассоциированным числам из D_I^* , делящимся на c , или (ср. выше переход от формулы (6) к формуле (10)) по всем числам из Γ , делящимся на c , отчего сумма только увеличится в $2lh_2$ раз. Кроме того, поскольку $N(ac) = Na \cdot Nc$, то от замены слагаемых вида $(Na)^{-s}$ на слагаемые вида $(N\alpha)^{-s}$, где $\alpha = ac$, вся сумма умножится на $(Nc)^{-s}$. Поэтому, чтобы остался прежний результат, полученную сумму (являющуюся, очевидно, как раз суммой $\Xi_{(c)}(s)$) нужно умножить на $(Nc)^s$. Этим доказано, что

$$(32) \quad \zeta_I^C(s) = \frac{(Nc)^s}{2lh_2} \Xi_{(c)}(s).$$

Так как мы считаем (опираясь на предложение 2), что при $s > 1$ ряд $\zeta_I^C(s)$ сходится, то из формулы (32), во-первых, следует, что при $s > 1$ сходится ряд $\Xi_{(c)}(s)$. Во-вторых, умножая формулу (32) на $s - 1$, переходя к пределу при $s \downarrow 1$ и применяя формулу (31) (полностью обоснованную предыдущим заключением), мы для вычета функции $\zeta_I^C(s)$ при $s = 1$ получим (поскольку $(Nc)^s \rightarrow Nc$ при $s \downarrow 1$) формулу

$$\begin{aligned} \lim_{s \downarrow 1} (s - 1) \zeta_I^C(s) &= \frac{Nc}{2lh_2} \cdot \frac{2^{2m-1} \pi^m}{Nc} |B| \cdot |C| = \\ &= \frac{2^{2m-2} \pi^m}{lh_2} |B| \cdot |C|. \end{aligned}$$

Для завершения доказательства предложения 3 осталось сравнить эту формулу с формулой (26). ■

Подчернем, что мы не только доказали предложение 3, но нашли явную формулу (26) для числа κ .

Конечно, справедливость всех наших выводов опирается на предложение 2, которое остается пока не доказанным. Мы докажем его в следующем параграфе.

§ 15. Формула Эйлера и L -ряды Дирихле

Рассмотрим бесконечное произведение

$$(1) \quad \prod_p \frac{1}{1 - \frac{1}{(Np)^s}},$$

распространенное на все простые дивизоры p кольца D_I . Так как

$$(2) \quad \frac{1}{1 - \frac{1}{(Np)^s}} = 1 + \frac{1}{(Np)^s} + \dots + \frac{1}{(Np)^{ns}} + \dots,$$

то (мы пока игнорируем вопросы сходимости) произведение (1) равно сумме всевозможных выражений вида

$$(3) \quad \frac{1}{(Np_1^{n_1})^s \dots (Np_k^{n_k})^s} = \frac{1}{N(p_1^{n_1} \dots p_k^{n_k})^s},$$

где p_1, \dots, p_k — произвольные простые дивизоры кольца D_I , а n_1, \dots, n_k — целые положительные числа. Поскольку любой дивизор a кольца D_I единственным образом представляется в виде $p_1^{n_1} \dots p_k^{n_k}$, этим доказано, что произведение (1) равно сумме

$$(4) \quad \zeta_I(s) = \sum_a \frac{1}{(Na)^s}.$$

Таким образом, для тех s , для которых сходятся и ряд $\zeta_I(s)$, и произведение (1), имеет место равенство

$$(5) \quad \zeta_I(s) = \prod_p \frac{1}{1 - \frac{1}{(Np)^s}}.$$

Это рассуждение годится для кольца целых чисел D любого поля алгебраических чисел. В частности, при

$D = \mathbb{Z}$ мы получаем равенство

$$(6) \quad \zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

Эта формула принадлежит Эйлеру. Более общую формулу (5) также обычно называют *формулой Эйлера*.

Формула (6) допускает и другое обобщение. Пусть $f(n)$ — такая функция на \mathbb{Z} (со значениями в \mathbb{C}), что

$$(7) \quad f(nm) = f(n)f(m)$$

для любых $n, m \in \mathbb{Z}$ (в теории чисел такие функции называются *вполне мультипликативными*). Тогда то же рассуждение, что и выше, докажет справедливость формулы

$$(8) \quad \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - \frac{f(p)}{p^s}}$$

(конечно, опять в предположении, что ряд слева и произведение справа сходятся).

Обсудим теперь проблему сходимости.

Известная теорема анализа утверждает, что бесконечное произведение вида $\prod (1 + u_n)$, где $|u_n| < 1$, абсолютно сходится, если сходится бесконечный ряд $\sum |u_n|$. Поскольку произведение (1) абсолютно сходится тогда и только тогда, когда сходится произведение

$$\prod_{p \neq 1} \left(1 + \frac{1}{(Np)^s}\right),$$

мы видим, что произведение (1) абсолютно сходится, если сходится ряд

$$(9) \quad \sum_{p \neq 1} \frac{1}{(Np)^s}.$$

Для каждого простого $p \neq 1$ (здесь и только здесь мы используем специфику кольца D_l) ряд (9) содержит $e \leq l-1$ членов вида $\frac{1}{p^{fs}} \leq \frac{1}{p^s}$, где $f = \frac{l-1}{e}$, а e — число простых дивизоров, на которые число p разлагается в кольце D_l . Поэтому ряд (9) мажори-

руется рядом

$$(l-1) \sum_{p \neq l} \frac{1}{p^s},$$

а значит, и рядом

$$(l-1) \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Поскольку последний ряд при $s > 1$ сходится, то произведение (1) при $s > 1$ абсолютно сходится.

Теперь мы уже можем доказать предложение 2 § 14, т. е. доказать, что при $s > 1$ ряд (4) сходится и тем самым заполнить пробел в рассуждениях § 14.

Доказательство предложения 2 § 14. Ясно, что если в формуле (5) мы справа ограничимся произведением, распространенным на произвольное конечное число простых дивизоров, то слева получится часть ряда (4), в которой участвуют те и только те слагаемые $(Na)^{-s}$, для которых дивизор a делится лишь на данные простые идеалы. Эта часть (также являющаяся бесконечным рядом) представляет собой произведение конечного числа рядов вида (2). Так как все ряды (2) при $s > 1$ сходятся (ибо $Np > 1$), то рассматриваемая часть ряда (4) также сходится.

С другой стороны, очевидно, что любая частичная (конечная) сумма ряда (4) является частичной суммой некоторой такой части (а именно, части, отвечающей всем простым дивизорам p , делящим дивизоры a , участвующие в данной сумме). Этим доказано, что любая частичная сумма ряда (4) не превосходит произведения некоторого конечного числа членов произведения (1), а потому (поскольку произведение (1) абсолютно сходится) не превосходит и этого произведения.

Таким образом, частичные суммы ряда (4) ограничены и, значит, этот ряд сходится. ■

Это рассуждение показывает также, что сумма $\zeta_l(s)$ ряда (4) не больше произведения (1). Но выше мы видели, что для любого конечного множества членов произведения (1) в ряде (4) найдется часть, равная их произведению. Поэтому сумма ряда (4) не меньше предела такого рода произведений, т. е. не меньше бесконечного произведения (1).

Этим доказано следующее предложение:

Предложение 1. Для любого $s > 1$ имеет место равенство

$$(10) \quad \zeta_l(s) = \prod_p \frac{1}{1 - \frac{1}{(Np)^s}},$$

где произведение справа абсолютно сходится. ■

Из этого предложения вытекает, в частности, что

$$(11) \quad \lim_{s \downarrow 1} \zeta_l(s) \neq 0.$$

Действительно, каждый член произведения (10) при $s > 1$ больше единицы и, значит, $\zeta_l(s) \geq 1$ при $s > 1$.

Ввиду предложений 7 и 8 § 13 мы можем формулу (10) переписать в виде

$$\left(1 - \frac{1}{l^s}\right) \zeta_l(s) = \prod_{p \neq l} \left(1 - \frac{1}{p^{fs}}\right)^{-e},$$

где f — наименьший показатель, для которого

$$p^f \equiv 1 \pmod{l},$$

$$a \quad e = \frac{l-1}{f}.$$

Пусть, как всегда, θ — первообразный корень из единицы степени $l-1$. Тогда θ^e будет первообразным корнем из единицы степени f и, значит, будет иметь место формула

$$1 - X^f = \prod_{j=0}^{f-1} (1 - \theta^{je} X).$$

В частности,

$$1 - \frac{1}{p^{fs}} = \prod_{j=0}^{f-1} \left(1 - \frac{\theta^{je}}{p^s}\right),$$

и потому

$$\left(1 - \frac{1}{l^s}\right) \zeta_l(s) = \prod_{p \neq l} \prod_{j=0}^{f-1} \left(1 - \frac{\theta^{je}}{p^s}\right)^{-e}.$$

Пусть, далее, так же как всегда, g — произвольный, но фиксированный, первообразный корень по

модулю l , и пусть $p \equiv g^a \pmod{l}$, где $1 \leq a \leq l-1$. Тогда $g^{af} \equiv 1 \pmod{l}$, и потому $af \equiv 0 \pmod{l-1}$. С другой стороны, очевидно, что наименьшее число $f \geq 1$, удовлетворяющее этому сравнению, равно $\frac{l-1}{d}$, где d — наибольший общий делитель чисел a и $l-1$.

Поэтому для любого простого $p \neq l$ показатель e равен наибольшему общему делителю чисел a и $l-1$, где a — такое число, что $p \equiv g^a \pmod{l}$.

Следовательно, если r пробегает $l-1$ чисел от 0 до $l-2$, то остатки от деления произведения ga на $l-1$ будут повторяться ровно e раз, а чтобы получить все остатки по одному разу, достаточно r изменять от 0 до $f-1$. Кроме того, ясно, что все эти остатки будут делиться на e и, значит, будут иметь вид je , где $j = 0, \dots, f-1$.

Этим доказано, что для любого простого числа $p \equiv g^a \pmod{l}$ имеет место равенство

$$\prod_{j=0}^{f-1} \left(1 - \frac{\theta^{je}}{p^s}\right)^{-e} = \prod_{r=0}^{l-2} \left(1 - \frac{\chi_r(p)}{p^s}\right)^{-1},$$

где

$$\chi_r(p) = \theta^{ra}.$$

Следовательно,

$$\left(1 - \frac{1}{l^s}\right) \zeta_l(s) = \prod_{r=0}^{l-2} \prod_{p \neq l} \left(1 - \frac{\chi_r(p)}{p^s}\right)^{-1},$$

где внутреннее произведение распространено на все простые числа $p \neq l$.

Полагая

$$(12) \quad L(s, \chi_r) = \prod_p \left(1 - \frac{\chi_r(p)}{p^s}\right)^{-1}, \quad s > 1,$$

мы это равенство можем переписать в следующем виде:

$$(13) \quad \left(1 - \frac{1}{l^s}\right) \zeta_l(s) = L(s, \chi_0) L(s, \chi_1) \dots L(s, \chi_{l-2}).$$

При этом мы можем считать, что в формуле (12) произведение распространено на все простые числа p , положив, по определению, $\chi(l) = 0$. Это произведение

абсолютно сходится (при $s > 1$), потому что сходится произведение

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Для каждого $r = 0, \dots, l-2$ мы определим функцию $\chi_r(n)$ при любом $n \in \mathbb{Z}$ формулой

$$\chi_r(n) = \begin{cases} 0, & \text{если } n \equiv 0 \pmod{l}, \\ \theta^{ra}, & \text{если } n \equiv g^a \pmod{l}. \end{cases}$$

Ясно, что

$$\chi_r(nm) = \chi_r(n)\chi_r(m) \quad \text{для любых } n \text{ и } m,$$

т. е. каждая функция χ_r вполне мультипликативна.

Кроме того, $\chi_r(1) = 1$ и

$$\chi_r(n) = \chi_r(m), \quad \text{если } n \equiv m \pmod{l}.$$

Обладающие этими свойствами функции $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ называются *характерами по модулю l* . Таким образом, для любого $r = 0, \dots, l-2$ функция χ_r является *характером по модулю l* .

Легко, впрочем, видеть, что верно и обратное, т. е. любой характер χ по модулю l имеет вид χ_r для некоторого r . Действительно, если $n \equiv g^a \pmod{l}$, то $\chi(n) = \chi(g)^a$. При этом, так как $g^{l-1} \equiv 1 \pmod{l}$, то $\chi(g)^{l-1} = \chi(1) = 1$, и потому $\chi(g) = \theta^r$ при некотором r .

Ввиду того, что характер χ вполне мультипликативен, к бесконечному произведению (12) применима формула (8) (обе части которой при $s > 1$ абсолютно сходятся, если $|f(n)| = 1$ для всех n). Поэтому

$$(14) \quad L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

для любого характера χ по модулю l .

Ряд (14) называется *L-рядом Дирихле* для характера χ , а его сумма $L(s, \chi)$ называется *L-функцией Дирихле*. Областью определения *L-функции* $L(s, \chi)$ мы будем считать множество всех s , для которых *L-ряд Дирихле* (14) сходится (хотя бы и не абсолютно). Таким образом, эта область вполне может быть больше полуоси $s > 1$.

Заметим, что разложение (12) функции $L(s, \chi_r)$ в бесконечное произведение доказано нами только при $s > 1$, и потому утверждать, что оно имеет место для всех s из области определения этой функции, у нас нет никаких оснований. (Тогда как разложение (14) функции $L(s, \chi)$ в бесконечный ряд справедливо, по определению, во всей этой области).

Ясно, что $\chi_0(n) = 1$ для всех $n \equiv 0 \pmod{l}$. Такой характер называется *главным характером*. Сравнение формулы (12) (при $\chi = \chi_0$) с формулой (6) показывает, что соответствующая L -функция Дирихле $L(s, \chi_0)$ отличается от ζ -функции Римана $\zeta(s)$ только множителем $\left(1 - \frac{1}{l^s}\right)^{-1}$:

$$L(s, \chi_0) = \zeta(s) \left(1 - \frac{1}{l^s}\right)^{-1}.$$

Отсюда следует, что *областью определения функции $L(s, \chi_0)$ является полуось $s > 1$* . Действительно, при $s \leq 1$ ряд $\zeta(s)$ мажорирует расходящийся гармонический ряд $\sum \frac{1}{n}$ и потому сам расходится.

Кроме того, основную формулу (13) мы можем теперь, сократив на $\left(1 - \frac{1}{l^s}\right)$, переписать в следующем виде:

$$(15) \quad \zeta_l(s) = \zeta(s) L(s, \chi_1) \dots L(s, \chi_{l-2}).$$

Найдем теперь область определения L -функции $L(s, \chi)$ при $\chi \neq \chi_0$.

Поскольку при $s = 0$ ряд (14) заведомо расходится (его общий член не стремится к нулю), эта область содержится в полуоси $s > 0$. Покажем, что она совпадает с этой полуосью.

Рассмотрим сумму

$$S(n) = \chi(1) + \dots + \chi(n).$$

Пусть, как и выше, $n \equiv g^a \pmod{l}$ (мы предполагаем, что $n \not\equiv 0 \pmod{l}$). Ясно, что когда n пробегает все числа от 1 до $l-1$, показатель a пробегает все числа от

0 до $l-2$. Поэтому (при $\chi = \chi_r$, где $r \neq 0$)

$$(16) \quad S(l) = S(l-1) = \sum_{a=0}^{l-2} \theta^{ar} = \frac{1 - \theta^{(l-1)r}}{1 - \theta^r} = 0.$$

(Заметим, что $S(l) = l$ при $\chi = \chi_0$.) Следовательно,

$$\begin{aligned} S(l+n) &= S(l) + \chi(l+1) + \dots + \chi(l+n) = \\ &= 0 + \chi(1) + \dots + \chi(n) = S(n), \end{aligned}$$

и, значит,

$$S(n) = S(m), \quad \text{если } n \equiv m \pmod{l}.$$

В частности, отсюда следует, что функция $S(n)$ ограничена, т. е.

$$|S(n)| \leq \text{const}$$

для всех $n \in \mathbb{Z}$.

С другой стороны, $\chi(n) = S(n) - S(n-1)$, и потому для любого $N > 1$ имеет место равенство

$$\begin{aligned} \sum_{n=1}^N \frac{\chi(n)}{n^s} &= \sum_{n=1}^N \frac{S(n) - S(n-1)}{n^s} = \\ &= \sum_{n=1}^N \frac{S(n)}{n^s} - \sum_{n=1}^N \frac{S(n-1)}{n^s} = \\ &= \frac{S(N)}{N^s} + \sum_{n=1}^{N-1} S(n) \left[\frac{1}{n^s} - \frac{1}{(n+1)^s} \right], \end{aligned}$$

ибо $S(0) = 0$. Так как $|S(N)| \leq \text{const}$, то при $s > 0$ первое слагаемое справа стремится к нулю:

$$\frac{S(N)}{N^s} \rightarrow 0, \quad \text{когда } N \rightarrow \infty.$$

Что же касается второго слагаемого, то при $s > 0$ оно мажорируется частичной суммой сходящегося ряда

$$\text{const} \cdot \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

и потому само является частичной суммой абсолютно сходящегося ряда

$$\sum_{n=1}^{\infty} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right).$$

Этим доказано, что для любого неглавного характера $\chi \neq \chi_0$ ряд Дирихле

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

сходится при $s > 0$. Следовательно, при $\chi \neq \chi_0$ функция $L(s, \chi)$ определена и непрерывна (даже дифференцируема) для всех $s > 0$.

В частности,

$$\lim_{s \rightarrow 1} L(s, \chi) = L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \quad \chi \neq \chi_0,$$

где ряд справа условно сходится.

Умножив теперь формулу (15) на $s - 1$, перейдя к пределу при $s \downarrow 1$ и учтя, что, согласно предложению 1 § 14,

$$\lim_{s \downarrow 1} (s - 1) \zeta(s) = 1,$$

мы немедленно получим следующее предложение:

Предложение 2. Вычет функции $\zeta_1(s)$ при $s = 1$ выражается формулой

$$(17) \quad \lim_{s \downarrow 1} (s - 1) \zeta_1(s) = L(1, \chi_1) \dots L(1, \chi_{l-2}). \quad \blacksquare$$

Чтобы вычислить числа $L(1, \chi_1), \dots, L(1, \chi_{l-2})$ в явном виде, мы введем в рассмотрение ряд

$$(18) \quad z + \frac{z^2}{2} + \dots + \frac{z^n}{n} + \dots,$$

который сходится при $|z| \leq 1$ и $z \neq 1$ к функции $-\ln(1 - z)$ (точнее, к аналитической ветви этой функции, мнимая часть которой находится в пределах от $-\frac{\pi}{2}$ до $\frac{\pi}{2}$).

Этот факт проще всего доказывается тем же методом (принадлежащим, кстати сказать, Абелю), которым выше была доказана сходимость L -рядов с $\chi \neq \chi_0$ при $s > 0$.

Пусть

$$S(n) = z + z^2 + \dots + z^n = \frac{z - z^{n+1}}{1 - z}$$

и, значит,

$$|S(n)| < \frac{2}{\varepsilon}$$

при $|z| \leq 1$ и $|1 - z| \geq \varepsilon$, где $\varepsilon > 0$. Так как

$$\sum_{n=1}^N \frac{z^n}{n} = \frac{S(N)}{n} + \sum_{n=1}^{N-1} S(n) \left(\frac{1}{n} - \frac{1}{n+1} \right),$$

и так как ряд

$$\sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1} \right)$$

сходится, отсюда уже известным нам рассуждением выводится, что ряд (18) при $|z| \leq 1$ и $|1 - z| \geq \varepsilon$ равномерно сходится. Поскольку $\varepsilon > 0$ произвольно, этим доказано, что при $|z| \leq 1$ и $z \neq 1$ ряд (18) сходится к непрерывной функции.

С другой стороны, классическая формула Маклорена, примененная к функции $-\ln(1 - z)$, показывает, что в круге $|z| < 1$ ряд (18) сходится к этой функции. Поскольку функция $-\ln(1 - z)$ непрерывна при $|z| \leq 1$ и $z \neq 1$, этим все доказано.

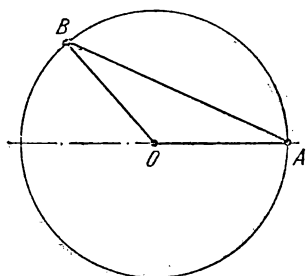
Теперь, в отличие от всего предыдущего, нам необходимо точно фиксировать число ξ . Мы будем считать, что

$$\xi = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l}.$$

Тогда для любого $k = 1, \dots, l-1$ комплексное число $-\ln(1 - \xi^k)$ будет иметь вещественной частью число

$$-\ln|1 - \xi^k| = -\ln \left| 2 \sin \frac{\varphi_k}{2} \right|, \text{ а мнимой частью —}$$

число $\frac{\pi - \varphi_k}{2}$, где $\varphi_k = \frac{2k\pi}{l}$ (см. рисунок). Что же



O — точка 0 , A — точка 1 , B — точка ξ^k

$$|OA| = |OB| = 1, \quad |AB| = \left| 2 \sin \frac{\varphi_k}{2} \right|,$$

$$\angle AOB = \varphi_k, \quad \angle OAB = \angle OBA = \frac{\pi - \varphi_k}{2}.$$

касается ряда (18), то при $z = \xi, \xi^2, \dots, \xi^{l-1}$ он будет сходиться, так что будут иметь место равенства

$$\sum_{n=1}^{\infty} \frac{\xi^k}{n} = -\ln(1 - \xi^k), \quad k = 1, 2, \dots, l-1.$$

Пусть теперь

$$d_k = \frac{1}{l} \sum_{j=1}^{l-1} \xi^{-jk} \chi(j), \quad k = 1, 2, \dots, l-1,$$

где χ — фиксированный неглавный характер. Тогда

$$\begin{aligned} -\sum_{k=1}^{l-1} d_k \ln(1 - \xi^k) &= \frac{1}{l} \sum_{k=1}^{l-1} \sum_{j=1}^{l-1} \sum_{n=1}^{\infty} \xi^{(n-j)k} \frac{\chi(j)}{n} = \\ &= \frac{1}{l} \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{j=1}^{l-1} \chi(j) \sum_{k=1}^{l-1} \xi^{(n-j)k} \right) = \\ &= \frac{1}{l} \sum_{n=1}^{\infty} \frac{1}{n} \left(\chi(n) l - \sum_{j=1}^{l-1} \chi(j) \right) = \\ &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = L(1, \chi), \end{aligned}$$

ибо

$$\sum_{k=1}^{l-1} \xi^{(n-j)k} = \begin{cases} l-1, & \text{если } n \equiv j \pmod{l}, \\ -1, & \text{если } n \not\equiv j \pmod{l}, \end{cases}$$

и (см. формулу (16))

$$\sum_{j=1}^{l-1} \chi(j) = 0$$

(перестановка порядка суммирования, несмотря на условную сходимость рассматриваемых рядов, как легко видеть, законна). Тем самым доказано, что

$$L(1, \chi) = -\sum_{k=1}^{l-1} d_k \ln(1 - \xi^k), \quad \chi \neq \chi_0.$$

Таким образом, для $L(1, \chi)$ получено конечное выражение, не использующее бесконечных процессов. Даль-

нейшие преобразования этой формулы уже будут чисто алгебраическими.

Пусть $k \equiv g^r \pmod l$. Тогда $\xi^k = \sigma^r \xi$ и потому, положив $a_r = d_k$, т. е. положив

$$a_r = \frac{1}{l} \sum_{j=1}^{l-1} (\sigma^r \xi)^{-j} \chi(j), \quad r = 0, 1, \dots, l-2,$$

мы получим для $L(1, \chi)$ формулу

$$L(1, \chi) = - \sum_{r=0}^{l-2} a_r \ln(1 - \sigma^r \xi)$$

(когда k меняется от 1 до $l-1$, показатель r пробегает в некотором порядке числа от 0 до $l-2$).

Учитывая, что для любого j , $1 \leq j \leq l-1$, существует единственное s , $0 \leq s \leq l-2$, для которого $g^s \equiv -j \pmod l$, и, значит, $\xi^{-j} = \sigma^s \xi$, а также что $-1 \equiv g^m \pmod l$, где, как всегда, $m = \frac{l-1}{2}$, мы видим, что

$$la_0 = \sum_{j=1}^{l-1} \xi^{-j} \chi(j) = \sum_{s=0}^{l-2} \sigma^s \xi \cdot \chi(-g^s) = \chi(g^m) \sum_{s=0}^{l-2} \sigma^s \xi \cdot \chi(g^s),$$

т. е. что

$$(19) \quad la_0 = \chi(g)^m \sum_{s=0}^{l-2} \sigma^s \xi \cdot \chi(g)^s.$$

Условно можно считать (предполагая, что σ не действует на $\chi(j)$), что $a_r = \sigma^r a_0$ для любого r . Поэтому, согласно формуле (19),

$$\begin{aligned} la_r &= l\sigma^r a_0 = \chi(g)^m \sum_{s=0}^{l-2} \sigma^{s+r} \xi \cdot \chi(g)^s = \\ &= \chi(g)^m \chi(g)^{-r} \sum_{t=0}^{l-2} \sigma^t \xi \cdot \chi(g)^t = \chi(g)^{-r} la_0. \end{aligned}$$

Следовательно, $a_r = \chi(g)^{-r} a_0$ и значит,

$$L(1, \chi) = -a_0 \sum_{r=0}^{l-2} \chi(g)^{-r} \ln(1 - \sigma^r \xi).$$

Если $\chi = \chi_j$, $j \neq 0$, то $\chi(g) = \theta^j$. Этим доказано, что

$$L(1 - \chi_j) = -a_0 \sum_{r=0}^{l-2} \theta^{-jr} \ln(1 - \sigma^r \xi),$$

где (см. формулу (19))

$$a_0 = \frac{(-1)^j}{l} \sum_{s=0}^{l-2} \theta^{sj} \sigma^s \xi$$

(так как $\chi(g) = \theta^j$, то $\chi(g)^m = (\theta^m)^j = (-1)^j$). Но, сравнив это выражение для a_0 с формулой (14) § 14, мы немедленно обнаружим, что $a_0 = (-1)^j b_j$. Таким образом,

$$(20) \quad L(1, \chi_j) = (-1)^{j+1} b_j \sum_{r=0}^{l-2} \theta^{-jr} \ln(1 - \sigma^r \xi),$$

где b_j — число, определенное формулой (14) § 14.

Предложение 3. Числа

$$L(1, \chi_1), \dots, L(1, \chi_{l-2})$$

отличны от нуля.

Доказательство. Так как функция $L(s, \chi)$, $\chi \neq \chi_0$, в точке $s = 1$ дифференцируема, то при $L(1, \chi) = 0$ предел

$$\lim_{s \rightarrow 1} \frac{L(s, \chi)}{s-1} = L'(1, \chi)$$

существует и конечен. Поэтому существует и конечен предел

$$\lim_{s \rightarrow 1} \frac{|L(s, \chi)|^2}{(s-1)^2} = |L'(1, \chi)|^2.$$

Но $\overline{L(s, \chi)} = L(s, \bar{\chi})$, причем, если $\chi = \chi_r$, где $1 \leq r \leq l-2$, то $\bar{\chi} = \chi_{2m-r}$. Следовательно, если $r \neq m$, то существует и конечен предел

$$\lim_{s \rightarrow 1} \frac{L(s)}{(s-1)^2} = |L'(1, \chi_r)|^2 \cdot L_r,$$

где $L(s) = L(s, \chi_1) \dots L(s, \chi_{l-2})$, а L_r — произведение всех чисел $L(1, \chi_j)$ при $j \neq r$, $2m - r$. Поскольку, согласно формуле (15),

$$\lim_{s \downarrow 1} \xi_l(s) = \lim_{s \downarrow 1} (s-1) \cdot \lim_{s \downarrow 1} (s-1) \xi(s) \cdot \lim_{s \downarrow 1} \frac{L(s)}{(s-1)^2},$$

отсюда следует (в силу предложения 1 § 14), что

$$\lim_{s \downarrow 1} \xi_l(s) = 0,$$

что противоречит формуле (11). Этим доказано, что $L(1, \chi_r) \neq 0$ при $r \neq m$.

Осталось рассмотреть случай $r = m$. Здесь мы воспользуемся формулой (20). Согласно этой формуле

$$L(1, \chi_m) = (-1)^{m+1} b_m \sum_{r=0}^{l-2} (-1)^r \ln(1 - \sigma^r \xi),$$

где $b_m \neq 0$. Поэтому $L(1, \chi_m) = 0$ тогда и только тогда, когда

$$\sum_{r=0}^{l-2} (-1)^r \ln(1 - \sigma^r \xi) = 0,$$

т. е. когда

$$\sum_{a=0}^{m-1} \ln(1 - \sigma^{2a} \xi) = \sum_{b=0}^{m-1} \ln(1 - \sigma^{2b+1} \xi).$$

Потенцируя это соотношение, мы получим тождество вида

$$\prod_{a=0}^{m-1} (1 - \sigma^{2a} \xi) = \prod_{b=0}^{m-1} (1 - \sigma^{2b+1} \xi) + 2N\pi i,$$

где N — некоторое целое число. При $N \neq 0$ из этого тождества следует, что число π является алгебраическим числом, что, как известно (см., например, Постников М. М. Теория Галуа. — М.: Физматгиз, 1963,

с. 205—211), неверно. Поэтому $N = 0$ и, значит,

$$\prod_{a=0}^{m-1} (1 - \sigma^{2a}\xi) = \prod_{b=0}^{m-1} (1 - \sigma^{2b+1}\xi).$$

Поскольку при воздействии σ левая часть этого тождества переходит в правую, элемент

$$A = \prod_{a=0}^{m-1} (1 - \sigma^{2a}\xi) = \prod_{b=0}^{m-1} (1 - \sigma^{2b+1}\xi)$$

кольца D_l обладает тем свойством, что $\sigma A = A$. Поэтому он лежит в \mathbb{Z} (см. § 5). Но, с другой стороны,

$$\begin{aligned} A^2 &= \prod_{a=0}^{m-1} (1 - \sigma^{2a}\xi) \prod_{b=0}^{m-1} (1 - \sigma^{2b+1}\xi) = \prod_{k=0}^{l-2} (1 - \sigma^k\xi) = \\ &= N(1 - \xi) = l, \end{aligned}$$

что при целом A невозможно. Полученное противоречие показывает, что $L(1, \chi_m) \neq 0$. ■

На первый взгляд кажется, что доказательство предложения 3 излишне осложнено и что — на основе той же идеи — это предложение может быть доказано следующим более простым рассуждением, не требующим специального рассмотрения случая $r = m$:

Если $L(1, \chi_r) = 0$, и, значит, предел

$$\lim_{s \rightarrow 1} \frac{L(s, \chi_r)}{s-1} = L'(1, \chi_r)$$

существует и конечен, то предел

$$\begin{aligned} \lim_{s \downarrow 1} \xi_l(s) &= \lim_{s \downarrow 1} (s-1) \xi(s) \lim_{s \downarrow 1} \frac{L(s, \chi_1) \dots L(s, \chi_{l-2})}{s-1} = \\ &= L'(1, \chi_r) \prod_{\substack{j=1 \\ j \neq r}}^{l-2} L(1, \chi_j) \end{aligned}$$

также существует и конечен. Но в предыдущем параграфе мы видели, что этот предел бесконечен (ибо вычет $\lim_{s \downarrow 1} (s-1) \xi_l(s) = h\chi$ существует и конечен). Следовательно, $L(1, \chi_r) \neq 0$ для всех r .

Однако это рассуждение содержит в себе порочный круг, поскольку в доказательстве равенства $\lim_{s \downarrow 1} (s-1) \xi_l(s) = h\chi$ мы существенно пользовались леммой 2 § 12, которая у нас пока еще не доказана и которую мы ниже выведем как раз из предложения 3.

Если $j = 2k$ чётно, то для любого $r = 0, \dots, m-1$ слагаемые

$$(21) \quad \theta^{-jr} \ln(1 - \sigma^r \xi) \quad \text{и} \quad \theta^{-j(m+r)} \ln(1 - \sigma^{m+r} \xi)$$

формулы (20) после сокращения на θ^{-jr} будут комплексно сопряжены (ибо $\theta^{-jm} = \theta^{-2km} = 1$ и $\sigma^{m+r} \xi = \overline{\sigma^r \xi}$). Поэтому их сумма будет равна

$$2\theta^{-jr} \operatorname{Re} \ln(1 - \sigma^r \xi) = 2\theta^{-jr} \ln |1 - \sigma^r \xi|$$

и, значит, будет иметь место формула

$$\sum_{r=0}^{l-2} \theta^{-2kr} \ln(1 - \sigma^r \xi) = 2 \sum_{j=0}^{m-1} \theta^{-2jk} \ln |1 - \sigma^j \xi| = 2\bar{c}_k,$$

где c_k , $1 \leq k \leq m-1$, — числа, определенные формулой (37) § 12. Поскольку, как легко видеть, $\bar{c}_k = c_{m-k}$, этим доказано, что

$$(22) \quad \begin{aligned} L(1, \chi_2) &= -2b_2 c_{m-1}, \\ L(1, \chi_4) &= -2b_4 c_{m-2}, \\ &\dots \dots \dots \\ L(1, \chi_{2m-2}) &= -2b_{2m-2} c_1. \end{aligned}$$

Доказательство леммы 2 § 12. Согласно предложению 3 из формул (22) вытекает, что $c_k \neq 0$ при $k = 1, \dots, m-1$. ■

Это рассуждение порочного круга не содержит, поскольку все, что мы делали в этом параграфе, никак не опиралось на материал § 12. Вообще, из материала всех предыдущих параграфов мы в этом параграфе пока воспользовались только предложениями 7 и 8 § 13, описывающими разложения простых чисел из Z в произведение простых дивизоров кольца D_l (а также предложением 1 § 14).

Пусть теперь $j = 2k + 1$. В этом случае слагаемые (21) (после сокращения на θ^{-jk}) будут иметь одинаковые мнимые части и противоположные по знаку вещественные. Поэтому в формулу (20) можно вместо $\ln(1 - \sigma^r \xi)$ подставить

$$\begin{aligned} \operatorname{Im} \ln(1 - \sigma^r \xi) &= i \left(\frac{\pi}{2} - \frac{1}{2} \cdot \frac{2\pi g_r}{l} \right), \\ r &= 0, 1, \dots, l-2. \end{aligned}$$

Это доказывает, что

$$\begin{aligned} L(1, \chi_{2k+1}) &= ib_{2k+1} \sum_{r=0}^{l-2} \theta^{-(2k+1)r} \left(\frac{\pi}{2} - \frac{\pi g_r}{l} \right) = \\ &= -\frac{i\pi}{l} b_{2k+1} \sum_{r=0}^{l-2} g_r \theta^{-(2k+1)r}, \end{aligned}$$

ибо

$$\sum_{r=0}^{l-2} \theta^{-(2k+1)r} = 0.$$

Вводя снова многочлен

$$\mathfrak{W}(X) = \sum_{r=0}^{l-2} g_r X^r$$

(см. § 6) и учитывая, что $\theta^{-(2k+1)} = \theta^{2(m-k)-1}$, мы окончательно получаем, что

$$\begin{aligned} (23) \quad L(1, \chi_{2k+1}) &= -\frac{i\pi}{l} b_{2k+1} \mathfrak{W}(\theta^{2(m-k)-1}), \\ k &= 0, \dots, m-1. \end{aligned}$$

Теперь осталось собрать плоды нашего тяжелого труда. Подставив выражения (22) и (23) в формулу (17), мы получим равенство

$$\begin{aligned} \lim_{s \downarrow 1} (s-1) \zeta_l(s) &= \left(-\frac{i\pi}{l} \right)^m \cdot (-2)^{m-1} b_1 \dots b_{l-2} c_1 \dots \\ &\dots c_{m-1} \mathfrak{W}(\theta) \mathfrak{W}(\theta^3) \dots \mathfrak{W}(\theta^{l-2}) = \frac{2^{m-1} \pi^m}{l^m} BC \cdot W(\mathfrak{W}). \end{aligned}$$

Переходя к модулям и учитывая, что согласно формуле (4) § 14 вычет $\lim_{s \downarrow 1} (s-1) \zeta_l(s)$ равен $h\kappa$, мы в силу формулы (6) § 12 получаем отсюда формулу:

$$h\kappa = \frac{2^{2m-2} \pi^m}{l} \cdot |B| \cdot |C| \cdot h_1.$$

Но, согласно формуле (26) § 14,

$$h\kappa = \frac{2^{2m-2} \pi^m}{lh_2} \cdot |B| \cdot |C| \cdot h.$$

Приравнивая эти два выражения и сокращая общие множители, мы и получаем нужную нам формулу для числа классов

$$h = h_1 h_2,$$

которая, таким образом, выскакивает из всех наших вычислений как чертик из шляпки.

Этим доказано совпадение куммеровых и регулярных чисел и тем самым, наконец-то, полностью доказана теорема Куммера.

ДОБАВЛЕНИЕ

Теорема Дирихле о простых числах в арифметических прогрессиях

Теорию L -рядов сам Дирихле создал для доказательства следующей теоремы:

Теорема Дирихле. В любой арифметической прогрессии

$$(1) \quad b, a + b, 2a + b, \dots, na + b, \dots$$

для которой числа a и b взаимно просты, содержится бесконечно много простых чисел.

Хотя эта теорема никак не связана с теоремой Ферма, мы все же изложим здесь ее доказательство, поскольку все, что для него нужно, мы фактически уже знаем (по крайней мере в случае, когда a является простым числом l), и было бы грешно этими знаниями не воспользоваться.

Идея Дирихле состоит в том, чтобы рассмотреть ряд

$$(2) \quad \sum \frac{1}{p},$$

распространенный на все простые числа вида (1), и доказать, что этот ряд расходится. Поскольку тогда число простых чисел вида (1) заведомо бесконечно, этим все будет доказано.

Для реализации этой идеи нам нужно перенести на случай произвольного модуля a понятие характера, введенное в § 15 для случая простого модуля l .

Для каждого целого $a > 1$ *характером по модулю a* называется не равная тождественно нулю, вполне мультипликативная (т. е. такая, что $\chi(mn) =$

$= \chi(m)\chi(n)$ для любых m и n) функция $\chi: \mathbb{Z} \rightarrow \mathbb{C}$, обладающая тем свойством, что

$$(3) \quad \chi(n) = \chi(m), \text{ если } n \equiv m \pmod{a},$$

и $\chi(n) = 0$, если n и a не взаимно просты.

Из условия полной мультипликативности следует, что $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$, т. е. что либо $\chi(1) = 1$, либо $\chi(1) = 0$. С другой стороны, если $\chi(1) = 0$, то $\chi(n) = \chi(n \cdot 1) = \chi(n) \cdot \chi(1) = 0$ для любого n , а по условию χ не обращается тождественно в нуль. Поэтому

$$\chi(1) = 1$$

для любого характера χ .

Класс числа n по модулю a тогда и только тогда обратим в кольце \mathbb{Z}/a (т. е. существует такое число v , что $nv \equiv 1 \pmod{a}$), когда число n взаимно просто с числом a (ибо $nv \equiv 1 \pmod{a}$ тогда и только тогда, когда существует такое число u , что $au + nv = 1$). Поэтому порядок мультипликативной группы $(\mathbb{Z}/a)^*$ обратимых элементов кольца \mathbb{Z}/a равен числу $\varphi(a)$ членов ряда $1, 2, \dots, a-1$, взаимно простых с числом a . Следовательно,

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

для любого числа n , взаимно простого с числом a . Это утверждение называется теоремой Эйлера.

Ясно, что $\varphi(p) = p-1$ для любого простого p . Поэтому для простых a теорема Эйлера сводится к малой теореме Ферма.

Из теоремы Эйлера следует, что

$$\chi(n)^{\varphi(a)} = \chi(n^{\varphi(a)}) = \chi(1) = 1$$

для любого характера χ . Мы видим, таким образом, что значения $\chi(n)$ произвольного характера χ по модулю a на числах n , взаимно простых с a , являются корнями степени $\varphi(a)$ из единицы.

В частности,

$$|\chi(n)| = 1,$$

и, значит, $\chi(n) \neq 0$ для любого характера χ и любого числа n , взаимно простого с числом a .

Характер χ_0 , для которого $\chi_0(n) = 1$ при любом n , взаимно простом с a , называется *главным*.

Для любого характера χ мы рассмотрим сумму

$$\sum_n \chi(n),$$

распространенную на полную систему представителей по модулю a , т. е. на все попарно не сравнимые друг с другом по модулю a числа n (или, что равносильно, только на те из этих чисел, которые взаимно просты с a).

Оказывается, что

$$(4) \quad \sum_n \chi(n) = \begin{cases} \varphi(a), & \text{если характер } \chi \text{ главный,} \\ 0 & \text{в противном случае.} \end{cases}$$

Действительно, при $\chi = \chi_0$ это равенство очевидно (имеется ровно $\varphi(a)$ отличных от нуля слагаемых и каждое из них равно единице). Если же $\chi \neq \chi_0$, то, по определению, существует такое m , взаимно простое с a (и значит, такое, что $\chi(m) \neq 0$), что $\chi(m) \neq 1$. Но, так как m взаимно просто с a , то при n , пробегающем полную систему представителей по модулю a , произведение mn также будет пробегать такую систему. Поэтому будет иметь место равенство

$$\sum_n \chi(n) = \sum_n \chi(nm) = \chi(m) \sum_n \chi(n)$$

при $\chi(m) \neq 0, 1$, возможное только тогда, когда $\sum_n \chi(n) = 0$. ■

Теперь легко видеть, что для любого неглавного характера χ ряд

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

сходится при всех $s > 0$ (и потому определяет непрерывную и дифференцируемую при $s > 0$ функцию).

Действительно (ср. с доказательством аналогичного утверждения для случая $a = p$ в § 15), пусть

$$S(n) = \chi(1) + \dots + \chi(n),$$

где n произвольно. Из второй формулы (4) немедленно следует, что функция S периодична с периодом a , т. е.

$$S(n+a) = S(n)$$

для любого n . Поэтому эта функция ограничена и, следовательно, ряд

$$\sum_{n=1}^{\infty} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

при $s > 0$ сходится. Поскольку же

$$\sum_{n=1}^N \frac{\chi(n)}{n^s} = \frac{S(N)}{N^s} + \sum_{n=1}^{N-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right),$$

значит, сходится и ряд

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \quad \square$$

Произведение $\chi_1 \chi_2$ двух характеров χ_1 и χ_2 (по одному и тому же модулю a) определяется формулой

$$\chi_1 \chi_2: n \mapsto \chi_1(n) \chi_2(n).$$

Легко видеть, что это произведение также является характером по модулю a и что все характеры образуют по отношению к этому умножению группу, единицей которой служит главный характер χ_0 .

Каждый характер определяется значениями, которые он принимает на $\varphi(a)$ попарно не сравнимых числах взаимно простых с a . Поскольку эти значения, являясь корнями степени $\varphi(a)$ из единицы, могут быть выбраны только $\varphi(a)$ способами, *число всех характеров по модулю a конечно*.

Поэтому для любого n имеет смысл сумма

$$\sum_{\chi} \chi(n),$$

распространенная на все характеры χ по модулю a .

Оказывается, что

$$(5) \quad \sum_{\chi} \chi(n) = \begin{cases} \bar{\varphi}(a), & \text{если } n \equiv 1 \pmod{a}, \\ 0 & \text{в противном случае,} \end{cases}$$

где $\bar{\varphi}(a)$ — число всех характеров по модулю a .

Действительно, при $n \equiv 1 \pmod{a}$ это равенство очевидно (имеется $\bar{\varphi}(a)$ слагаемых, каждое из которых равно единице). Чтобы рассмотреть случай $n \not\equiv 1 \pmod{a}$, нам понадобится следующая лемма, доказательство которой мы пока, — чтобы не прерывать изложения, — отложим:

Л е м м а 1. *Для любого числа n , взаимно простого с a и такого, что $n \not\equiv 1 \pmod{a}$, существует характер χ_1 по модулю a , обладающий тем свойством, что $\chi_1(n) \neq 1$.*

Так как характеры по модулю a образуют группу, то, когда χ пробегает все характеры, произведение $\chi_1\chi$ также пробегает все характеры. Следовательно,

$$\sum_{\chi} \chi(n) = \sum_{\chi} (\chi_1\chi)(n) = \chi_1(n) \sum_{\chi} \chi(n),$$

что при $\chi_1(n) \neq 0$, 1 возможно только, когда $\sum_{\chi} \chi(n) = 0$. В силу леммы 1 это доказывает формулу (5) при $n \not\equiv 1 \pmod{a}$ в случае, когда n взаимно просто с a . (Ср. с доказательством формулы (4)).

Для завершения доказательства остается заметить, что при n , не взаимно простом с a , формула (5) очевидна (все слагаемые равны нулю и потому их сумма также равна нулю). ■

Теперь легко можно показать, что фигурирующее в формуле (5) число $\bar{\varphi}(a)$ всех характеров по модулю a равно числу $\varphi(a)$ всех классов по модулю a чисел, взаимно простых с a :

$$\bar{\varphi}(a) = \varphi(a).$$

Действительно, вычисляя двумя способами сумму

$$\sum_{n, \chi} \chi(n),$$

распространенную на все характеры по модулю a и на полную систему представителей классов чисел по модулю a , мы получим, что

$$\sum_{n, \chi} \chi(n) = \sum_{\chi} \sum_a \chi(n) = \varphi(a) \quad (\text{в силу соотношений (4)})$$

$$\sum_{n, \chi} \chi(n) = \sum_n \sum_{\chi} \chi(n) = \bar{\varphi}(a) \quad (\text{в силу соотношений (5)}).$$

Следовательно, $\bar{\varphi}(a) = \varphi(a)$. ■

Что же касается леммы 1, то при $a = l$ простым и нечетным эта лемма нам уже известна: если g — первообразный корень по нечетному простому модулю l , то характер χ_1 , определенный (при n , не делящихся на l) формулой $\chi_1(n) = \theta^r$, где θ — первообразный корень из единицы степени $l-1 = \varphi(l)$, а r — такой показатель, что $n \equiv g^r \pmod{l}$, обладает, очевидно, тем свойством, что $\chi_1(n) \neq 1$, когда $n \not\equiv 1 \pmod{l}$.

Оказывается, что та же конструкция годится и при $a = l^s$ (если только $l > 2$). Нужно только доказать, что для любого числа n , взаимно простого с l^s (т. е. не делящегося на l), существует такой показатель r , что $n \equiv g^r \pmod{l^s}$. Действительно, тогда формула

$$\chi_1(n) = \begin{cases} \theta^r, & \text{если } n \text{ взаимно просто с } l^s \text{ и } n \equiv g^r \pmod{l^s}, \\ 0, & \text{если } n \text{ не взаимно просто с } l^s, \end{cases}$$

будет, как легко видеть, определять характер χ_1 по модулю l^s , обладающий тем свойством, что $\chi_1(n) \neq 1$ для любого числа $n \not\equiv 1 \pmod{l^s}$.

Итак, нам нужно при $a = l^s$ (и $l > 2$) доказать лишь существование показателя r . Мы сделаем это в предположении (когда это только и верно), что первообразный корень g удовлетворяет условию (6) § 6. Согласно этому условию

$$g^{l-1} = 1 + bl,$$

где число b не делится на l . Поэтому для любого $t \geq 0$ будет иметь место равенство

$$\begin{aligned} g^{(l-1)t} &= (1 + bl)^t = \\ &= 1 + t \cdot bl + \frac{t^t(t-1)}{2} \cdot (bl)^2 + \dots = 1 + cl^{t+1}, \end{aligned}$$

где

$$c = b + \frac{t^t - 1}{2} \cdot b^2 l + \dots \equiv b \pmod{l}$$

не делится на l . В частности, мы видим, что

$$(6) \quad g^{(l-1)t} \not\equiv 1 \pmod{l^s} \quad \text{при} \quad t+1 < s.$$

Утверждение о существовании для любого n , взаимно простого с l^s , показателя r означает, что мультипликативная группа $(\mathbb{Z}/l^s)^*$ обратимых элементов кольца \mathbb{Z}/l^s является циклической группой, образующей которой служит класс первообразного корня g . Поэтому для доказательства этого утверждения достаточно доказать, что порядок класса числа g равен порядку $\varphi(l^s)$ группы $(\mathbb{Z}/l^s)^*$, т. е. что если r — наи-

меньшее положительное число, для которого имеет место сравнение

$$(7) \quad g^r \equiv 1 \pmod{l^s},$$

то $r = \varphi(l^s)$. Но поскольку порядок любого элемента группы делит порядок группы (равный в нашем случае $\varphi(l^s)$), из этого сравнения следует, что r делит $\varphi(l^s)$. С другой стороны, так как из (7) следует, что $g^r \equiv 1 \pmod{l}$, и так как g — первообразный корень по модулю l , то r делится на $l-1$. Таким образом, r делит $\varphi(l^s)$ и делится на $l-1$.

Вычислим теперь число $\varphi(l^s)$. По определению оно равно числу членов ряда $0, 1, \dots, l^s - 1$, взаимно простых с l^s , т. е. не делящихся на l . Но каждый член этого ряда, делящийся на l , имеет вид lq , где q — член ряда $0, 1, \dots, l^{s-1} - 1$. Поэтому число этих членов равно l^{s-1} , а, значит, число членов ряда $0, 1, \dots, l^s - 1$, не делящихся на l , равно $l^s - l^{s-1} = l^{s-1}(l-1)$. Таким образом,

$$\varphi(l^s) = l^{s-1}(l-1).$$

(Заметим, что эта формула верна и при $l = 2$, когда она приобретает вид $\varphi(2^s) = 2^{s-1}$.)

Тем самым доказано, что показатель r делит $l^{s-1}(l-1)$ и делится на $l-1$. Значит, он имеет вид

$$r = l^t(l-1), \quad \text{где } t \leq s-1.$$

Но если $t < s-1$, то, согласно формуле (6),

$$g^r \not\equiv 1 \pmod{l^s},$$

что противоречит сравнению (7). Следовательно, $t = s-1$, и потому $r = l^{s-1}(l-1) = \varphi(l^s)$. ■

Тем самым при $a = l^s$, $s \geq 1$, $l \geq 2$, лемма полностью доказана.

Заметим, что характер χ_1 мы нашли один и тот же для всех чисел $n \not\equiv 1 \pmod{l}$. Ниже мы увидим, что для других значений a это сделать невозможно (потому что группа $(\mathbb{Z}/a)^*$ является циклической группой только тогда, когда $a = l^s$ и $l > 2$).

При $a = 2^s$ лемма содержательна только при $s > 1$ (при $s = 1$ чисел n , взаимно простых с a и таких, что $n \not\equiv 1 \pmod{a}$, попросту нет).

Пусть $s > 1$. Легко видеть, что формула

$$\chi_1(n) = \begin{cases} 1, & \text{если } n \equiv 1 \pmod{4}, \\ -1, & \text{если } n \equiv 3 \pmod{4} \end{cases}$$

определяет характер χ_1 по модулю $a = 2^s$, обладающий тем свойством, что $\chi(n) \neq 1$ при $n \equiv 3 \pmod{4}$.

Таким образом, нам осталось подобрать характер χ_1 лишь для чисел $n \equiv 1 \pmod{4}$. Классы таких чисел n по модулю $a = 2^s$ интересны только при $s > 2$ и они, очевидно, составляют подгруппу группы $(\mathbb{Z}/2^s)^*$, имеющую половинный порядок $\frac{\varphi(2^s)}{2} = 2^{s-2}$.

Оказывается, что эта подгруппа циклична и ее образующей служит класс числа 5.

Чтобы доказать это, достаточно, как мы знаем, доказать, что класс числа 5 по модулю 2^s имеет порядок 2^{s-2} . С этой целью заметим, что для любого $r \geq 0$ имеет место сравнение

$$5^{2^r} \equiv 1 + 2^{r+2} \pmod{2^{r+3}}.$$

Действительно, при $r = 0$ это верно (имеет место даже равенство $5 = 1 + 4$), а если это верно для $r - 1$, т. е. если $5^{2^{r-1}} = 1 + 2^{r+1} + 2^{r+2}N$, то

$$\begin{aligned} 5^{2^r} &= (5^{2^{r-1}})^2 = (1 + 2^{r+1} + 2^{r+2}N)^2 = \\ &= 1 + 2 \cdot 2^{r+1} + 2^{r+3}(N + 2^{r-1} + 2^{r+1}N + 2^{r+1}N^2) \end{aligned}$$

Поэтому, в частности, $5^{2^{s-3}} \equiv 1 + 2^{s-1} \pmod{2^s}$ и, значит, $5^{2^{s-3}} \not\equiv 1 \pmod{2^s}$, тогда как $5^{2^{s-2}} \equiv 1 + 2^s \pmod{2^{s+1}}$ и, следовательно, $5^{2^{s-2}} \equiv 1 \pmod{2^s}$. Таким образом, порядок класса числа 5 по модулю 2^s на самом деле равен 2^{s-2} . ■

Таким образом, для каждого числа $n \equiv 1 \pmod{4}$ существует такой показатель r , что $n \equiv 5^r \pmod{2^s}$. Если же $n \equiv 3 \pmod{4}$, то $-n \equiv 1 \pmod{4}$, и потому существует такой показатель r , что $n \equiv -5^r \pmod{2^s}$.

Теперь легко видеть, что, положив

$$\chi_1(n) = \theta^r,$$

где r — такой показатель, что

$$n \equiv 5^r \pmod{2^s}, \text{ если } n \equiv 1 \pmod{4}$$

и

$$n \equiv -5^r \pmod{2^s}, \text{ если } n \equiv 3 \pmod{4},$$

a — первообразный корень из единицы степени 2^{s-2} , мы получим характер по модулю 2^s , обладающий тем свойством, что $\chi_1(n) \neq 1$, если $n \equiv 1 \pmod{4}$ и $n \not\equiv 1 \pmod{2^s}$.

Тем самым лемма 1 доказана для любого $a = l^s$.

При $a \neq l^s$ группа классов по модулю a чисел, взаимно простых с a , не будет, вообще говоря, циклической группой, и потому единого характера χ_1 , пригодного для всех $n \not\equiv 1 \pmod{a}$, найти мы не сможем (этот феномен возник у нас уже при $a = 2^s$, $s > 1$). Нам придется поэтому подбирать для каждого n свой характер χ_1 . Для этого мы воспользуемся следующей общей конструкцией.

Пусть d — произвольный делитель числа a , и пусть χ^* — произвольный характер по модулю d . Так как из $n \equiv m \pmod{a}$ вытекает, что $n \equiv m \pmod{d}$, то функция χ^* обладает свойством (3) характеров по модулю a . Тем не менее характером по модулю a она, вообще говоря, не будет, поскольку могут существовать числа, взаимно простые с d , но не с a , и на этих числах функция χ^* будет отлична от нуля. Чтобы исправить это, достаточно умножить χ^* на главный характер χ_0 по модулю a . Ясно, что получающаяся функция $\chi = \chi^* \chi_0$ уже будет характером по модулю a .

По построению, для любого числа n , взаимно простого с a , имеет место равенство $\chi(n) = \chi^*(n)$, так что, в частности, $\chi(n) \neq 1$, если $\chi^*(n) \neq 1$. Таким образом, для доказательства леммы 1 в случае $a \neq l^s$ нам достаточно для любого числа n , взаимно простого с a , и такого, что $n \not\equiv 1 \pmod{a}$, подобрать такой делитель d числа a и такой характер χ^* по модулю d , что $\chi^*(n) \neq 1$. Для существования характера χ^* необходимо, чтобы было выполнено условие $n \not\equiv 1 \pmod{d}$, а если d является степенью l^s некоторого простого числа l , то, согласно доказанному выше, это условие и достаточно. Следовательно, все будет доказано, если мы покажем, что для любого числа n , взаимно простого с a , и такого, что $n \not\equiv 1 \pmod{a}$, существует такой делитель числа a , являющийся степенью l^s некоторого простого числа l , что $n \not\equiv 1 \pmod{l^s}$. Иначе говоря, нам нужно показать, что если $n \equiv 1 \pmod{l^s}$ для любого числа вида l^s , деля-

щего число a , то $n \equiv 1 \pmod{a}$. В свою очередь это утверждение выводится очевидной индукцией из того, что если $n \equiv 1 \pmod{a}$ и $n \equiv 1 \pmod{b}$, где a и b — два взаимно простых числа, то $n \equiv 1 \pmod{ab}$. Но это последнее утверждение очевидно, поскольку из равенств $n = 1 + Aa$ и $n = 1 + Bb$ вытекает, что $Aa = Bb$ и, значит, (ввиду взаимной простоты чисел a и b), что $A = Cb$, $B = Ca$ для некоторого C . Следовательно, $n = 1 + Cab \equiv 1 \pmod{ab}$. ■

Тем самым лемма 1 полностью доказана.

Вернемся теперь к ряду (2). Тот факт, что число p принадлежит арифметической прогрессии (1), в точности равносильно тому, что $p \equiv b \pmod{a}$, а значит, тому, что

$$cp \equiv 1 \pmod{a},$$

где c — такое число, что $cb \equiv 1 \pmod{a}$ (такое число c существует, так как по условию числа a и b взаимно просты). Поскольку, согласно соотношениям (5),

$$\sum_{\chi} \chi(cp) = \begin{cases} \varphi(a), & \text{если } cp \equiv 1 \pmod{a}, \\ 0 & \text{если } cp \not\equiv 1 \pmod{a}, \end{cases}$$

отсюда следует, что ряд (2) мы можем переписать в виде

$$(8) \quad \frac{1}{\varphi(a)} \sum_p \frac{1}{p} \sum_{\chi} \chi(cp),$$

где суммирование распространено уже на все простые числа p .

Рассуждая от противного, предположим, что ряд (2), а значит, и ряд (8) сходятся. Тогда, меняя порядок суммирования (и отбрасывая множитель $\varphi(a)^{-1}$), мы получим ряд

$$(9) \quad \sum_{\chi} \chi(c) \sum_p \frac{\chi(p)}{p} = \sum_p \frac{1}{p} + \sum_{\chi \neq \chi_0} \chi(c) \sum_p \frac{\chi(p)}{p}.$$

Предположим, мы доказали, что для любого неглавного характера $\chi \neq \chi_0$ ряд

$$(10) \quad \sum_p \frac{\chi(p)}{p},$$

где суммирование распространено на все простые числа, сходится. Тогда из формулы (9) будет следовать, что ряд (2) сходится тогда и только тогда, когда сходится ряд

$$(11) \quad \sum_p \frac{1}{p}.$$

Но еще Эйлер доказал, что ряд (11) расходится. Поэтому ряд (2) расходится, и, значит, арифметическая прогрессия (1) содержит бесконечно много простых чисел.

Таким образом, для доказательства теоремы Дирихле нам нужно только доказать сходимость рядов (10) и расходимость ряда (11).

Последнее утверждение доказывается легко. Действительно, из формулы Эйлера (формула (6) § 15) и того факта, что ряд (18) § 15 сходится к функции $-\ln(1-z)$, следует, что при любом $s > 1$ имеет место равенство

$$(12) \quad \ln \zeta(s) = \sum_p \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \dots + \frac{1}{np^{ns}} + \dots \right) = \\ = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}}.$$

Но так как при $n \geq 2$

$$np^{ns} \geq 2p^{2s} \cdot p^{(n-2)s},$$

то ряд $\sum_{n=2}^{\infty} \frac{1}{np^{ns}}$ мажорируется рядом

$$\frac{1}{2p^s} \sum_{m=0}^{\infty} \frac{1}{p^{ms}} = \frac{1}{2p^s} \cdot \frac{1}{1 - \frac{1}{p^s}} < \frac{1}{p^{2s}},$$

и, значит, ряд

$$(13) \quad \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}}$$

— рядом

$$\sum_p \frac{1}{p^{2s}} < \sum_n \frac{1}{n^{2s}} = \zeta(2s).$$

Следовательно, при $s > \frac{1}{2}$ ряд (13) сходится. В частности, этот ряд сходится при $s = 1$. Поэтому, если бы ряд (11) сходил, то из формулы (12) вытекало бы, что функция $\ln \zeta(s)$ имеет при $s \downarrow 1$ конечный предел. Поскольку это явно не так (ибо $\zeta(s) \rightarrow \infty$ при $s \downarrow 1$), ряд (11), следовательно, расходится.

Аналогичное рассуждение можно применить и для доказательства сходимости рядов (10). Действительно, по обобщенной формуле Эйлера (формула (8), § 15)

$$\begin{aligned} \ln L(s, \chi) &= - \sum_p \ln \left(1 - \frac{\chi(p)}{p^s} \right) = \\ &= \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}} = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}. \end{aligned}$$

Для второго ряда справа модули его членов составляют уже знакомый нам ряд (13). Поэтому этот ряд при $s > \frac{1}{2}$ (и, значит, при $s = 1$) абсолютно сходится. Следовательно, ряд (10) тогда и только тогда сходится, когда существует конечный предел $\lim_{s \downarrow 1} \ln L(s, \chi)$. Но так как при $\chi \neq \chi_0$ функция $L(s, \chi)$, как было замечено выше, непрерывна при $s > 0$, этот предел равен $\ln L(1, \chi)$. Поэтому ряд (10) *сходится тогда и только тогда, когда $L(1, \chi) \neq 0$* .

Таким образом, все сводится к доказательству следующего предложения (представляющего собой ключевой пункт рассуждения Дирихле, подобно тому как его частный случай при $a = 1$ — предложение 3 § 15 — был ключевым пунктом в выводе формулы Куммера для числа классов идеалов кольца целых чисел поля деления круга):

Предложение 1. Для любого неглавного характера $\chi \neq \chi_0$

$$L(1, \chi) \neq 0.$$

Поскольку при $a = l$ простом этот факт нам уже известен, тем самым теорема Дирихле нами доказана для любой арифметической прогрессии с простой разностью $a = l$.

Чтобы доказать предложение 1, в общем случае нам понадобятся некоторые простейшие сведения о рядах вида

$$(14) \quad \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

где a_n — произвольные (вообще говоря, комплексные) числа. Такие ряды называются *рядами Дирихле*, а числа a_n — их *коэффициентами*.

Хотя нам эти ряды будут нужны только для вещественных значений s , но для лучшего понимания их аналитического поведения целесообразно считать s произвольным комплексным числом.

Лемма 2. *Если ряд (14) сходится при $s = s_0$, то он равномерно сходится в замкнутой угловой области, определяемой неравенством вида*

$$(15) \quad |\arg(s - s_0)| \leq \gamma < \frac{\pi}{2}.$$

Доказательство. Мы воспользуемся уже известным нам преобразованием Абеля. Пусть

$$A_m = \sum_{n=1}^m \frac{a_n}{n^{s_0}}$$

— частичные суммы ряда (11) в точке $s = s_0$ и

$$A = \lim_{m \rightarrow \infty} A_m$$

— его сумма. Тогда для любых N и $M > N$ будет иметь место равенство

$$\begin{aligned} \sum_{n=N}^M \frac{a_n}{n^s} &= \sum_{n=N}^M \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^{s-s_0}} = \sum_{n=N}^M (A_n - A_{n-1}) \cdot \frac{1}{n^{s-s_0}} = \\ &= \sum_{n=N}^M (A_n - A) \frac{1}{n^{s-s_0}} - \sum_{n=N}^M (A_{n-1} - A) \frac{1}{n^{s-s_0}} = \end{aligned}$$

$$= \frac{A_M - A}{M^{s-s_0}} - \frac{A_{N-1} - A}{N^{s-s_0}} + \\ + \sum_{n=N}^{M-1} (A_n - A) \left(\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right).$$

Пусть $\varepsilon > 0$. Так как $A_m \rightarrow A$, то существует такое N , что $|A_n - A| < \varepsilon$ при $n \geq N-1$. Поэтому для любого $M > N$ будет иметь место оценка

$$\left| \sum_{n=N}^M \frac{a_n}{n^s} \right| \leq 2\varepsilon + \varepsilon \sum_{n=N}^{M-1} \left| \frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right|.$$

С другой стороны, полагая $s = \sigma + it$, $s_0 = \sigma_0 + it_0$ и замечая, что условие (15) равносильно неравенствам

$$\sigma \geq \sigma_0, \quad |t - t_0| \leq (\sigma - \sigma_0) \operatorname{tg} \gamma,$$

мы для любого s из области (15) получим, что

$$\left| \frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right| = (s - s_0) \left| \int_{n+1}^n \frac{du}{u^{s+1}} \right| \leq \\ \leq |s - s_0| \int_{n+1}^n \frac{dx}{x^{(\sigma-\sigma_0)+1}} = \\ = (1 + \operatorname{tg} \gamma) \left(\frac{1}{n^{\sigma-\sigma_0}} - \frac{1}{(n+1)^{\sigma-\sigma_0}} \right),$$

поскольку

$$\frac{|s - s_0|}{\sigma - \sigma_0} \leq \frac{|\sigma - \sigma_0| + |t - t_0|}{\sigma - \sigma_0} \leq 1 + \operatorname{tg} \gamma.$$

Следовательно,

$$\left| \sum_{n=N}^M \frac{a_n}{n^s} \right| \leq 2\varepsilon + \varepsilon (1 + \operatorname{tg} \gamma) \sum_{n=N}^{M-1} \left(\frac{1}{n^{\sigma-\sigma_0}} - \frac{1}{(n+1)^{\sigma-\sigma_0}} \right) = \\ = 2\varepsilon + \varepsilon (1 + \operatorname{tg} \gamma) \left(\frac{1}{N^{\sigma-\sigma_0}} - \frac{1}{M^{\sigma-\sigma_0}} \right) \leq \\ \leq \left(2 + \frac{1 + \operatorname{tg} \gamma}{N^{\sigma-\sigma_0}} \right) \varepsilon = \operatorname{const} \cdot \varepsilon.$$

Это доказывает лемму 2. \square

Следствие 1. Если ряд (11) сходится при $s = \sigma_0 + it_0$, то он сходится при любом $s = \sigma + it$ с $\sigma > \sigma_0$ и его сумма является функцией, аналитической в полуплоскости $\sigma > \sigma_0$. ■

При этом каждая производная этой функции является суммой ряда Дирихле, полученного почленным дифференцированием ряда (14).

Следствие 2. Существует такое вещественное число σ_c (случаи $\sigma_c = -\infty$ и $\sigma_c = +\infty$ не исключаются), что при $\sigma > \sigma_c$ ряд (11) сходится, а при $\sigma < \sigma_c$ расходится. ■

Число σ_c называется абсциссой сходимости ряда (11). Согласно следствию 1 сумма ряда (11) является функцией, аналитической в полуплоскости $\sigma > \sigma_c$.

Пусть

$$S(n) = a_1 + a_2 + \dots + a_n.$$

Лемма 3. Если $|S(n)| \leq \text{const}$, то ряд (11) сходится при $\text{Re } s > 0$, т. е. его абсцисса сходимости не положительна:

$$\sigma_c \leq 0.$$

Доказательство. Так как

$$\sum_{n=N}^M \frac{a_n}{n^s} = \frac{S(M)}{M^s} - \frac{S(N-1)}{N^s} + \sum_{n=N}^{M-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right),$$

то для любого $s = \sigma + it$ с $\sigma > 0$

$$\begin{aligned} \left| \sum_{n=N}^M \frac{a_n}{n^s} \right| &\leq \frac{|S(M)|}{M^\sigma} + \frac{|S(N-1)|}{N^\sigma} + \\ &+ \frac{|s|}{\sigma} \sum_{n=N}^{M-1} |S(n)| \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) \leq \\ &\leq \text{const} \cdot \left(2 + \frac{|s|}{\sigma} \right) \cdot \frac{1}{N^\sigma} \rightarrow 0 \quad \text{при } N \rightarrow \infty. \quad \blacksquare \end{aligned}$$

Применим эту лемму к ряду

$$\begin{aligned} \left(1 - \frac{1}{2^{s-1}} \right) \zeta(s) &= \\ &= \left(1 - \frac{2}{2^s} \right) \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \frac{2}{(2n)^s} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}. \end{aligned}$$

Для этого ряда

$$S(n) = \begin{cases} 1, & \text{если } n \text{ нечетно,} \\ 0, & \text{если } n \text{ четно.} \end{cases}$$

Следовательно, согласно лемме 3, этот ряд сходится при $\sigma > 0$.

Обозначая сумму этого ряда через $A(s)$, мы определим функцию $\zeta(s)$ для всех $s \neq 1$ из полуплоскости $\sigma > 0$ формулой

$$\zeta(s) = \left(1 - \frac{1}{2^{s-1}}\right)^{-1} A(s).$$

Тем самым функцию $\zeta(s)$ мы аналитически продолжили на всю полуплоскость $\sigma > 0$. Эта функция аналитична во всех точках этой полуплоскости, за исключением точки $s = 1$, где она имеет простой полюс с вычетом 1.

Функция $L(s, \chi_0)$ для главного характера χ_0 по модулю a связана с функцией $\zeta(s)$ формулой

$$\begin{aligned} L(s, \chi_0) &= \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p \nmid a} \left(1 - \frac{1}{p^s}\right)^{-1} = \\ &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{p \mid a} \left(1 - \frac{1}{p^s}\right) = \\ &= \zeta(s) \cdot \prod_{p \mid a} \left(1 - \frac{1}{p^s}\right), \end{aligned}$$

где знак \prod_p означает произведение, распространенное на все простые числа p , знак $\prod_{p \nmid a}$ — произведение, распространенное на все простые числа p , не делящие числа a ; а знак $\prod_{p \mid a}$ — напротив, произведение, распространенное на все простые делители p числа a . Поэтому, подобно функции $\zeta(s)$, функция $L(s, \chi_0)$ также аналитически продолжается на полуплоскость $\sigma > 0$ без точки $s = 1$. При $s = 1$ эта функция имеет простой полюс с вычетом

$$\lim_{s \rightarrow 1} (s-1) L(s, \chi_0) = \prod_{p \mid a} \left(1 - \frac{1}{p^s}\right).$$

Введем теперь в рассмотрение функцию

$$P(s) = \prod_{\chi} L(s, \chi),$$

где произведение распространено на все характеры χ по модулю a . Согласно сказанному выше эта функция аналитична в полуплоскости $\sigma > 0$ за возможным исключением точки $s = 1$. Точнее, если ни одно из чисел $L(1, \chi)$, $\chi \neq \chi_0$, не равно нулю, то $P(s) \rightarrow \infty$ при $s \rightarrow 1$, так что точка $s = 1$ будет особой точкой (полюсом) функции $P(s)$. Если же существует такой характер $\chi^* \neq \chi_0$, что $L(1, \chi^*) = 0$ и, значит (см. § 15),

$$\lim_{s \rightarrow 1} \frac{L(s, \chi^*)}{s-1} = L'(1, \chi^*),$$

то предел

$$\lim_{s \rightarrow 1} P(s) =$$

$$= \lim_{s \rightarrow 1} (s-1) L(s, \chi_0) \cdot \lim_{s \rightarrow 1} \frac{L(s, \chi^*)}{s-1} \cdot \prod_{\chi \neq \chi_0, \chi^*} L(1, \chi)$$

существует и конечен. Поэтому функцию $P(s)$ можно доопределить при $s = 1$, чтобы получилась функция, не имеющая при $\sigma > 0$ особых точек. Следовательно, предложение 1 равносильно утверждению, что *в полуплоскости $\sigma > 0$ функция $P(s)$ имеет хотя бы одну особую точку*. В этой форме мы и будем это предложение доказывать.

Рассмотрим с этой целью функцию $Q(s) = \ln P(s)$. Так как

$$\begin{aligned} \ln P(s) &= \sum_{\chi} \ln L(s, \chi) = \sum_{\chi} \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}} = \\ &= \sum_{n=1}^{\infty} \sum_p \frac{1}{np^{ns}} \sum_{\chi} \chi(p^n) = \\ &= \varphi(a) \sum_{n=1}^{\infty} \sum' \frac{1}{np^{ns}} = \sum_{n=1}^{\infty} \frac{q_n}{n^s}, \end{aligned}$$

где штрих у знака суммы обозначает, что суммирование распространено на все простые числа p , для которых $p^n \equiv 1 \pmod{a}$, а

$$q_n = \begin{cases} \frac{\varphi(a)}{n}, & \text{если } n \text{ имеет вид } p^k \text{ и } p^k \equiv 1 \pmod{a}, \\ 0 & \text{во всех остальных случаях,} \end{cases}$$

то функция $Q(s)$ является суммой ряда Дирихле

$$(16) \quad Q(s) = \sum_{n=1}^{\infty} \frac{q_n}{n^s}$$

с вещественными и неотрицательными коэффициентами. Найдем абсциссу сходимости этого ряда.

Сохранив в формуле

$$Q(s) = \varphi(a) \sum_{n=1}^{\infty} \sum' \frac{1}{np^{ns}}$$

лишь слагаемые с $n = \varphi(a)$, мы получим неравенство

$$(17) \quad Q(s) \geq \sum \frac{1}{p^{\varphi(a)s}},$$

где суммирование распространено на все простые числа p , для которых

$$p^{\varphi(a)} \equiv 1 \pmod{a},$$

т. е., согласно теореме Эйлера, на все простые числа, не делящие a . Поэтому из неравенства (17) следует, что ряд (16) заведомо расходится для тех s , для которых расходится ряд

$$(18) \quad \sum_p \frac{1}{p^{\varphi(a)s}}.$$

При этом суммирование в ряде (18) можно считать распространенным на все простые числа, поскольку добавление конечного числа членов, соответствующих простым делителям числа a , не влияет на сходимость и расходимость ряда.

Поскольку ряд (18) при $\varphi(a)s = 1$, как мы знаем, расходится, этим доказано, что абсцисса сходимости σ_c ряда Дирихле (16) положительна:

$$\sigma_c > 0$$

(она не меньше числа $\frac{1}{\varphi(a)}$).

Поскольку

$$(19) \quad P(s) = e^{Q(s)} = 1 + Q(s) + \frac{Q^2(s)}{2!} + \dots + \frac{Q^n(s)}{n!} + \dots,$$

ряд Дирихле для $P(s)$ можно получить формальной подстановкой в ряд (19) ряда (16). Так как все коэффициенты ряда (16) вещественны и неотрицательны, то коэффициенты ряда Дирихле для $P(s)$ также будут вещественны и неотрицательны. Кроме того, этот ряд будет мажорировать ряд (13) для $Q(s)$, и, значит, его абсцисса сходимости будет не меньше абсциссы сходимости σ_c ряда (16) и потому также будет положительна.

Теперь предложение 1 вытекает из следующей общей леммы:

Л е м м а 3. Пусть σ_c — абсцисса сходимости ряда Дирихле (14) с неотрицательными вещественными коэффициентами, и пусть при $\sigma > \sigma_c$ функция $f(s)$ является суммой этого ряда. Тогда точка вещественной оси $s = \sigma_c$ является особой точкой функции $f(s)$.

Доказательство. Пусть точка $s = \sigma_c$ не является особой точкой функции $f(s)$. Это означает, что существуют такие вещественные числа $s_0 > \sigma_c$ и $s_1 < \sigma_c$, что ряд Тейлора функции $f(s)$ в точке s_0 сходится при $s = s_1$, т. е. имеет место равенство

$$f(s_1) = \sum_{k=0}^{\infty} \frac{f^{(k)}(s_0)}{k!} (s_1 - s_0)^k,$$

где

$$f^{(k)}(s_0) = (-1)^k \sum_{n=1}^{\infty} \frac{a_n \ln n^k}{n^{s_0}}.$$

Иными словами,

$$f(s_1) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{a_n \ln^k n}{n^{s_0} k!} (s_0 - s_1)^k.$$

Поскольку все члены этого ряда по условию неотрицательны, в нем может быть изменен порядок суммирования. Следовательно,

$$\begin{aligned} f(s_1) &= \sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} \sum_{k=0}^{\infty} \frac{\ln^k n}{k!} (s_0 - s_1)^k = \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} e^{(s_0 - s_1) \ln n} = \sum_{n=1}^{\infty} \frac{a_n}{n^{s_1}}, \end{aligned}$$

что невозможно, ибо при $s_1 < \sigma_c$ ряд (14) расходится. ■

Согласно этой лемме, примененной к функции $P(s)$, положительное число σ_c будет особой точкой этой функции. Как было сказано выше, это доказывает предложение 1.

Михаил Михайлович Постников

ВВЕДЕНИЕ В ТЕОРИЮ
АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Редакторы *В. Л. Попов, Ф. И. Кизнер*

Техн. редактор *Л. В. Лихачева*

Корректор *М. Л. Медведская*

ИБ № 12012

Сдано в набор 17.06.81. Подписано к печати 10.03.82.
Т-00394. Формат $84 \times 108 \frac{1}{32}$. Бумага тип. № 1. Лите-
ратурная гарнитура. Высокая печать. Условн. печ. л.
12,6. Уч.-изд. л. 12,14. Тираж 150 000 экз. Заказ № 1186.
Цена 40 коп.

Издательство «Наука»

Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие
ордена Трудового Красного Знамени Ленинградского
объединения «Техническая книга» им. Евгении Соко-
ловой Союзполиграфпрома при Государственном
комитете СССР по делам издательств, полиграфии
и книжной торговли, 198052, г. Ленинград, Л-52,
Измайловский проспект, 29,

40 коп.