МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА

Механико-математический факультет

Эллиптические кривые и криптография
Семестр 1

Ю.Г. Прохоров

Москва 2007 год

Ю.Г. Прохоров

Эллиптические кривые и криптография. Семестр 1.

Настоящие записки являются частью курса лекций, прочитанных автором на механико-математическом факультете МГУ. Курс ориентирован на студентов, не имеющих специальной алгебраической и алгебро-геометрической подготовки. Требуются лишь стандартные знания университетского курса алгебры.

Работы выполнена при частичной поддержке грантов РФФИ № 05-01-00353-а, РФФИ № 06-01-72017, НШ-5-666.2006.1 и НШ-9969.2006.1

Для студентов и аспирантов.

Рецензент – д. ф.-м. н., профессор В.А. Исковских.

Печатается по решению Ученого совета механико-математического факультета МГУ

Оглавление

Глава 1.

Введение в криптографию

1.1. Простейшие системы шифрования

Стандартная *криптосистема* состоит из

(i) двух множеств M и N – элементов открытого текста и шифротекста (для простоты мы будем предполагать, что $M = N$);

(ii) *шифрующего преобразования* $\Phi\colon M \to N$ (чаще всего – взаимно однозначного отображения);

(iii) *ключа шифрования* K – множества параметров, от которых зависит преобразование Φ.

Отметим, что M и N необязательно состоят только из алфавита. Они могут содержать дополнительные символы или соответствовать парам или блокам из k букв. Рассмотрим простейший пример такого, *классического* шифрования.

Пример 1.1.1 Отождествим множества M и N с кольцом вычетов $\mathbb{Z}_n$ по подходящему модулю n и зададим преобразование $\Phi\colon \mathbb{Z}_n \to \mathbb{Z}_n$ формулой $\Phi(x) = ax + b$, где константы a, $b \in \mathbb{Z}_n$ – ключ шифрования, т.е. $K = (a, b)$. Если НОД $(a, n) = 1$, то преобразование Φ будет взаимно однозначным и обратное (*дешифрующее*) преобразование задается формулой $\Phi^{-1}(y) = a'y + b'$, где $aa' \equiv 1 \mod n$ и $b' = -a'b$.

Отметим однако, что здесь Φ и Φ^{-1} – аффинно-линейные функции и поэтому они полностью восстанавливаются по своим значениям в двух точках. Такая криптосистема, очевидно, не является надежной. Действительно, пусть, например, наиболее часто употребляемым символом языка является $x_1 \in M$. Имея

достаточно длинное шифрованное сообщение, методом *частотного анализа* можно выяснить, что наиболее часто встречающимся символом сообщения является, например, $y_1 \in N$. Таким образом, $\Phi(x_1) = y_1$. Аналогично можно получить $\Phi(x_2) = y_2$. Отсюда уже легко найти константы a, b и a', b'.

Приведенный выше пример можно усовершенствовать двумя способами. Во-первых, можно разбить весь текст на блоки из пар букв и занумеровать эти блоки элементами $\mathbb{Z}_{n^2}$, где n – число элементов алфавита. Далее, как и выше, определим шифрующее преобразование формулой $\Phi(x) = ax + b$, где НОД $(a, n^2) = 1$. Ясно, что предложенная двухбуквенная система лучше простейшей, однобуквенной. Однако она имеет недостатки. Грубо говоря, для того, чтобы вскрыть данную систему методом частотного анализа нужно выделить в некотором отрезке шифротекста два двухбуквенных блока, встречающихся чаше других. Это затруднительно, если шифротекст короток и не составляет большого труда для объемного шифротекста.

Другой способ, усовершенствовать криптосистему из примера 1.1.1 состоит в сопоставлении парам букв вектора $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{Z}_n^2$, $x_i \in \mathbb{Z}_n$. Зафиксируем матрицу $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ и вектор $\mathbf{v} := \begin{pmatrix} e \\ f \end{pmatrix}$, где $a, \ldots, f \in \mathbb{Z}_n$. Это – ключ шифрования. Шифрующее преобразование задается аффинным преобразованием

$$\Phi\colon \mathbb{Z}_n^2 \longrightarrow \mathbb{Z}_n^2, \qquad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A \begin{pmatrix} x \\ y \end{pmatrix} + v. \tag{1.1.2}$$

Предложение 1.1.3 *Преобразование* (1.1.2) *взаимно однозначно тогда и только тогда, когда определитель матрицы A взаимно прост с n.*

Доказательство. Положим $\Delta := \det A$. Обратное преобразование $\Phi^{-1}(\mathbf{y})$ находится при помощи решения системы линейных уравнений

$$A\mathbf{x} + \mathbf{v} = \mathbf{y}$$

относительно $\mathbf{x}$. Эта система имеет решение для любых $\mathbf{y}$ тогда и только тогда, когда матрица A обратима (над $\mathbb{Z}_n$). Последнее

же эквивалентно тому, что $\det A$ взаимно прост с n. $\square$

1.2. Открытый ключ. RSA

Криптографические системы с открытым ключом основаны на понятии односторонней функции. Функция $y = \Phi(x)$ называется *односторонней*, если сложность вычисления $\Phi^{-1}(y)$ существенно выше, чем сложность вычисления $\Phi(x)$. Большинство односторонних функций, рассматриваемых в криптографии, – это те, для которых значения $\Phi(x)$ могут быть вычислены при помощи полиномиального алгоритма, а значения $\Phi^{-1}(y)$ не могут. Близким понятием является понятие *функции с секретом*. Такая функция $y = \Phi(x) = \Phi_K(x)$ зависит от ключа K и алгоритм вычисления ее значений является полиномиальным. Алгоритм вычисления обратной функции $\Phi^{-1}(y) = \Phi^{-1}_{K'}(y)$ зависит от ключа (параметра) K' и также является полиномиальным (при известном K'). Считается также, что не существует полиномиального алгоритма вычисления $\Phi^{-1}(y)$ (или такой алгоритм пока не известен), если значение K' засекречено. Системы шифрования, основанные на применении функций с секретом, называются системами с *открытым ключом*. Такие системы *асимметричны* в том смысле, что сложность вычисления $y = \Phi(x)$ и $\Phi^{-1}(y)$ при неизвестном K' существенно различается.

Одной из наиболее распространенных в настоящее время криптосистем с открытым ключом является система RSA[1)]. Опишем вкратце как работает эта система.

Обозначим через $\mathbb{Z}_n^*$ подмножество кольца вычетов $\mathbb{Z}_n$, состоящее из классов, представители которых взаимно просты с n. Число элементов в $\mathbb{Z}_n^*$ обозначается через $\varphi(n)$ и называется *функцией Эйлера*. Иначе говоря, $\varphi(n)$ – это количество натуральных чисел, не превосходящих n и взаимно простых с n. Ясно, что $\varphi(n) = n - 1$, если $n = p$ – простое число. Если же $n = pq$ – произведение двух различных простых чисел, то

[1)] Сокращение имен создателей системы – R. L. Rivest, A. Shamir и L. M. Adleman

$\varphi(n) = (p-1)(q-1)$. Отметим, что множество $\mathbb{Z}_n^*$ замкнуто относительно умножения и является группой (проверьте!).

Система RSA работает следующим образом. Пользователь выбирает два простых числа p и q. Полагаем $n := pq$. Далее генерируется случайное число r, взаимно простое с $\varphi(n) = (p-1)(q-1)$. Затем вычисляется s такое, что $rs \equiv 1 \mod \varphi(n)$. Таким образом, $rs = \varphi(n)k + 1$ для некоторого $k \in \mathbb{Z}$. Ключ шифрования $K = (n, r)$ делается открытым, а ключ дешифрования $K' = (s)$ – закрытым. Естественно, секретными также являются p и q. Полагаем $M = N = \mathbb{Z}_n$. Шифрующее преобразование имеет вид $\Phi(x) = x^r$, а дешифрующее – $\Phi'(y) = y^s$. Так как порядок группы $\mathbb{Z}_n^*$ равен $\varphi(n)$, то по теореме Лагранжа значения y^r и y^s не зависят от выбора представителей r и s по модулю $\varphi(n)$.

Проверим, что преобразования Φ и Φ' взаимно обратны. Действительно, утверждение эквивалентно тому, что $x^{rs} \equiv x \mod n$ для любого $x \in \mathbb{Z}_n$. Иначе говоря,

$$x^{\varphi(n)k+1} \equiv x \mod n.$$

Если НОД $(n, x) = 1$, то x может быть рассмотрен как элемент мультипликативной группы $\mathbb{Z}_n^*$ обратимых элементов кольца $\mathbb{Z}_n$. Эта группа имеет порядок $\varphi(n)$. По теореме Лагранжа порядок x в $\mathbb{Z}_n^*$ делит $\varphi(n)$. Следовательно, $x^{\varphi(n)} \equiv 1 \mod n$, что и дает наше сравнение в этом случае. Пусть НОД $(n, x) \neq 1$. Мы можем считать, что $x = pl$, где $q \nmid l$. Требуемое сравнение перепишется в виде

$$(pl)^{(p-1)(q-1)k} \equiv 1 \mod q. \tag{1.2.1}$$

Согласно малой теореме Ферма, $(pl)^{q-1} \equiv 1 \mod q$ (см. следствие 2.3.15). Отсюда

$$(pl)^{(p-1)(q-1)k} \equiv ((pl)^{q-1})^{(p-1)k} \equiv 1 \mod q.$$

Сравнение (1.2.1) доказано.

Остается заметить, что пользователь, не знающий ключа $K' = (s)$ имеет определенные трудности в дешифровании сообщений: не зная s, довольно сложно вычислить $\Phi^{-1}(y) = y^s$ (при условии, что p и q – достаточно большие). Нахождение же s, в свою очередь, связано с задачей дискретного логарифмирования, которую мы обсудим в следующем параграфе.

1.3. Дискретное логарифмирование в абелевой группе

Система Диффи-Хэллмана (Diffie-Hellman) обмена ключами

Считается, что фиксирована некоторая группа G и ее элемент g порядка N, которые считаются общеизвестными. Предположим, что Иванов и Петров хотят согласовать секретный ключ K (например, для простейшей системы шифрования, описанной в примере 1.1.1). Они действуют следующим образом. Иванов выбирает секретное число $n \in \{1, \ldots, N-1\}$ и вычисляет g^n. Петров выбирает секретное число $m \in \{1, \ldots, N-1\}$ и вычисляет g^m. Они пересылают друг другу элементы g^n и g^m по открытым каналам. Таким образом, g^n и g^m считаются общеизвестными. В качестве секретного ключа выбирается g^{nm}. Очевидно, что оба, Иванов и Петров, могут легко вычислить g^{nm} по правилам $(g^m)^n$ и $(g^n)^m$. Однако постороннему для вычисления g^{nm} нужно знать n или m. Следующая проблема носит название *проблемы дискретного логарифмирования* (DLP).

Проблема 1.3.1 Для данных элементов $g, h \in G$ таких, что $h \in \langle g \rangle$, найти наименьшее положительное x такое, что

$$g^x = h. \tag{1.3.2}$$

Решение проблемы 1.3.1 дает возможность злоумышленнику найти секретный ключ g^{nm}. Однако следует отметить, что, возможно, существует алгоритм вычисления g^{nm} по g^n и g^m, не основанный на дискретном логарифмировании.

Преимущество обсуждаемой системы связано с тем, что сложность нахождения x в уравнении (1.3.2) (а значит и вычисления g^{nm} в системе Диффи-Хэллмана) чрезвычайно велика.

На практике удобно за группу G взять мультипликативную группу $\mathbb{F}_q$ конечного поля или аддитивную группу точек эллиптической кривой X над полем $\mathbb{F}_q$.

Редукция проблемы дискретного логарифмирования к случаю простого порядка

Теперь мы обсудим возможность решения уравнения (1.3.2). Пусть N – порядок элемента g. Мы предложим алгоритм, позволяющий сводить проблему к случаю простого N. Ясно, что нас интересует лишь значение x по модулю N Зафиксируем простой делитель p числа N. Пусть $p^k \mid N$ и $p^{k+1} \nmid N$. Найдем остаток от деления x на p^k. Рассмотрим следующее разложение (запись в p-ичной системе счисления):

$$x = x_0 + x_1 p + \cdots + x_{r-1} p^{r-1} + x_r p^r, \tag{1.3.3}$$

где $0 \le x_i < p$ при $i = 0, \ldots, r$. Здесь $x_0 + \cdots + x_{j-1} p^{j-1}$ – остаток от деления x на p^j. Найдем последовательно x_i для $i = 0, \ldots, k-1$. Положим $N_i := N/p^i$, $i = 0, \ldots, k-1$. Тогда $g^{N_i p^i} = 1$. В частности, g^{N_1} – элемент порядка p. Из (1.3.2) получаем $g^{N_1 x} = h^{N_1}$. Это дает нам

$$(g^{N_1})^{x_0} = g^{(x_0 + x_1 p + \cdots + x_{k+1} p^{k+1}) N_1} = g^{x N_1} = h^{N_1}. \tag{1.3.4}$$

Мы предполагаем, что проблема дискретного логарифмирования разрешима для случая, когда основание имеет простой прядок. Поэтому мы можем найти x_0. Далее действуем по индукции: пусть уже найдены $x_0, \ldots, x_{i-1}$, $i - 1 < k$. Как и выше

$$g^{N_{i+1} x} = h^{N_{i+1}} \quad \Rightarrow \quad g^{(x_0 + x_1 p + \cdots + x_i p^i) N_{i+1}} = g^{x N_{i+1}} = h^{N_{i+1}}.$$

Отсюда

$$(g^{N_1})^{x_i} = (g^{p^i N_{i+1}})^{x_i} = h^{N_{i+1}} g^{-(x_0 + x_1 p + \cdots + x_{i-1} p^{i-1}) N_{i+1}}. \tag{1.3.5}$$

Выражение в правой части нам известно, а g^{N_1} – также известный нам элемент порядка p. Следовательно, мы можем найти x_i. Продолжая процесс, мы найдем все $x_0, \ldots, x_{k-1}$, а значит и x по модулю p^k.

Далее пусть $N = p_1^{k_1} \cdots p_s^{k_s}$ – разложение N в произведение различных простых чисел. Для каждого p_l мы можем вычислить q_l такое, что $x \equiv q_l \mod p_l^{k_l}$. Практически, этот алгоритм реализуется следующим образом. Для каждого простого делителя $p = p_l$ числа N мы должны решать уравнение $(g^{N/p})^{x_i} = h'$

относительно x_i, где h' – выражение в правой части (1.3.4) или (1.3.5), а x_i – число из разложения (1.3.3) для $p = p_l$. Находим элементы $u_j := g^{jN/p} = (g^{N/p})^j$ для $j = 0, 1, \ldots, p-1$. Это все элементы порядка p в циклической группе $\langle g \rangle$. Мы видим, что $u_{x_i} = h'$. Сравнивая h' и $u_0, \ldots, u_{p-1}$, находим x_i. Заметим, что разумно элементы u_j для всех $p = p_i$ объединить в таблицу. Эта таблица вычисляется один раз и сохраняется в памяти.

Теперь x находится при помощи *китайской теоремы об остатках.*

Теорема 1.3.6 (Китайская теорема об остатках) *Пусть $a_1, \ldots, a_s$ взаимно простые целые числа. Для любых $b_1, \ldots, b_s \in \mathbb{Z}$ существует $x \in \mathbb{Z}$ такое, что*

$$x \equiv b_i \mod a_i, \qquad \forall i = 1, \ldots, s.$$

Алгоритм-Доказательство. Положим $A := a_1 \cdots a_s$ и $A_i := A/a_i$. Тогда НОД $(a_i, A_i) = 1$ и, согласно алгоритму Евклида, существуют целые числа α_i и β_i такие, что $\alpha_i a_i + \beta_i A_i = 1$. Нетрудно проверить, что $x = \sum \beta_i A_i b_i$ является решением нашей системы. □

Описанный выше алгоритм был предложен Полигом и Хэллманом (G. C. Pohlig, M. E. Hellman). Он очень хорошо работает для тех N, у которых все простые множители малы.

Система Эль-Гамаля (ElGamal)

Как и в системе Диффи-Хэллмана выбирается некоторая группа G и ее элемент g порядка N. Это – открытая информация. Желательно, чтобы группа была циклической, а элемент g – ее порождающим. Элементы открытого и шифрованного текста отождествляются с элементами G. Иванов (пользователь 1) выбирает секретное число $n_1 \in \{1, \ldots, N-1\}$, являющееся его ключом дешифрования. Открытым ключом шифрования является g^{n_1}. Аналогично поступает пользователь i: он выбирает $n_i \in \{1, \ldots, N-1\}$ и вычисляет g^{n_i}. Для того, чтобы передать Иванову элемент x, Петров (пользователь 2) выбирает случайное число m и посылает ему по открытым каналам

пару $(g^m,\, b = g^{n_1 m} \cdot x)$. Иванов получит элемент x по формуле $x = b/(g^m)^{n_1}$ (n_1 ему известно). Для того, чтобы раскрыть описанную систему нужно решать проблему дискретного логарифмирования.

Пересылка сообщений с открытым ключом нуждается в *цифровой подписи*. Опишем схему цифровой подписи, также предложенную *Эль-Гамалем*. Мы полагаем, что $G = \mathbb{F}_p^*$ – мультипликативная группа конечного поля из простого числа элементов, а g – ее порождающий. Таким образом, $N = p - 1$. Остальные данные n_i и g^{n_i} и предположения о них – те же, что и выше. Для посылки подписи s Иванову, Петров (пользователь 2) сначала выбирает случайное число $m \in \{1, \ldots, N-2\}$ и вычисляет целое $r \equiv g^m \mod p$. Затем он решает сравнение

$$s \equiv n_2 r + my \mod p - 1 \tag{1.3.7}$$

относительно y и посылает пару (g^m, y), а также подпись s Иванову. Получив эти данные, Иванов проверяет условие (1.3.7) следующим образом

$$g^s \equiv (g^{n_2})^r (g^m)^y \mod p$$

Если оно выполнено, то он может быть уверен, что именно Петров послал сообщение.

Упражнения. **(1)** Является ли 5 порождающим элементом в группе $\mathbb{Z}_{311}^*$?

(2) Найдите все порождающие элементы в группах $\mathbb{Z}_{29}^*$, $\mathbb{Z}_{31}^*$, $\mathbb{Z}_{37}^*$.

(3) Применив метод Поллига-Хэллмана, найдите дискретный логарифм от 22 по основанию 3 в группе $\mathbb{Z}_{31}^*$.

Глава 2.

Алгебраическая подготовка

В этой главе мы обсудим некоторые факты из алгебры, которые необходимы для дальнейшего изложения, но часто не входят в стандартные университетские курсы. Читатель, предпочитающий более систематическое изложение предмета, может изучать его по книгам [Лен68], [Кос01].

2.1. Кольца

Под *кольцом* R мы будем понимать ассоциативное коммутативное кольцо с единицей 1. Такое кольцо называется *полем*, если любой ненулевой элемент обратим: $a \neq 0 \Longrightarrow \exists b \in R \quad ab = 1$. Ясно, что в поле уравнение $ax = b$ имеет решение для любых $a \neq 0$ и b. Простейшими примерами являются хорошо известные поля рациональных $\mathbb{Q}$, действительных $\mathbb{R}$ и комплексных чисел $\mathbb{C}$. В настоящем курсе для нас наиболее интересными будут *конечные* поля, т.е. поля, состоящие из конечного числа элементов.

Подмножество R' кольца (поля) R называется подкольцом (*подполем*), если R' является кольцом (полем) с теми же операциями (сложения и умножения), что и в R. Единичные элементы в кольце и подкольце должны совпадать.

Напомним, что *идеалом* в кольце R называется подмножество $\mathfrak{a} \subset R$ такое, что

(i) $\forall a, b \in \mathfrak{a} \quad a \pm b \in \mathfrak{a}$,

(ii) $\forall a \in \mathfrak{a}, \forall b \in R \quad ab \in \mathfrak{a}$.

Для любых элементов $a_1, \ldots, a_n \in R$ множество

$$\Big\{ \sum_i a_i b_i \mid b_i \in R \Big\}$$

является идеалом. Он называется идеалом, порожденным элементами $a_1, \ldots, a_n$ и обозначается $(a_1, \ldots, a_n)$. Ясно, что $(a_1, \ldots, a_n)$ совпадает с пересечением всех идеалов, содержащих $\mathfrak{a}$. Идеал (a), порожденный одним элементом, называется *главным*. Если в кольце R каждый идеал главный, то R называется *кольцом главных идеалов*. В любом кольце R имеются тривиальные идеалы – нулевой (0) и единичный $(1) = R$. Если R – поле, то любой идеал в R совпадает с (0) или (1). Отметим, что идеал $\mathfrak{a} \subsetneq R$ не является подкольцом в нашем определении: он не содержит единичного элемента.

Пример 2.1.1 Поскольку подгруппа циклической группы – также циклическая, то кольцо целых чисел $\mathbb{Z}$ является кольцом главных идеалов. Из существования алгоритма деления с остатком несложно выводится, что кольцо многочленов $\Bbbk[x]$ от одной переменной над полем также кольцо главных идеалов. Кольцо многочленов $\Bbbk[x, y]$ от двух переменных таковым не является: идеал (x, y) не может быть порожден одним элементом.

Гомоморфизмом колец называется отображение $f\colon R \to R'$ такое, что $f(a + b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$. Из определения следует, что тогда $f(0) = 0$ и $f(-a) = -f(a)$. Мы будем рассматривать только гомоморфизмы такие, что $f(1) = 1$.

Для любого идеала $\mathfrak{a} \subsetneq R$ рассмотрим факторгруппу $R/\mathfrak{a}$ аддитивной группы R по подгруппе $\mathfrak{a}$. Введем на $R/\mathfrak{a}$ умножение по правилу $(a+R)(b+R) = ab+R$. Несложно показать, что это умножение не зависит от выбора представителей смежных классов: если $a+R = a'+R$ и $b+R = b'+R$, то $ab+R = a'b'+R$. Мы получим, что $R/\mathfrak{a}$ является ассоциативным коммутативным кольцом с единицей. Оно называется *факторкольцом*. Имеется канонический гомоморфизм $\pi\colon R \to R/\mathfrak{a}$, $\pi(a) = a + R$.

Если $f\colon R \to R'$ – гомоморфизм колец, то его образ $\operatorname{Im} f$ является подкольцом в R'. *Ядром* называется подмножество

$$\operatorname{Ker} f = \{a \in R \mid f(a) = 0\}.$$

Теорема 2.1.2 (о гомоморфизме) *Пусть $f\colon R \to R'$ – гомоморфизм колец. Тогда $\operatorname{Ker} F$ – идеал в R и имеется естественный изоморфизм колец $\operatorname{Im} f \simeq R/\operatorname{Ker} f$.*

Пример 2.1.3 Пусть $R = \mathbb{Z}$ и $\mathfrak{a} = (n)$, $n \in \mathbb{N}$. Тогда $\mathbb{Z}/(n)$ – кольцо классов вычетов по модулю n.

Идеал $\mathfrak{p}$ кольца R называется *простым*, если из того, что $ab \in \mathfrak{p}$ следует или $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Легко видеть, что идеал $\mathfrak{p}$ является простым тогда и только тогда, когда факторкольцо $R/\mathfrak{p}$ не имеет делителей нуля. Идеал $\mathfrak{m} \subset R$ называется *максимальным*, если любой идеал, содержащий $\mathfrak{m}$ или совпадает с $\mathfrak{m}$, или является единичным.

Предложение 2.1.4 (i) *Идеал $\mathfrak{m} \subset R$ является максимальным тогда и только тогда, когда факторкольцо $R/\mathfrak{m}$ – поле.*

(ii) *Каждый максимальный идеал является простым.*

Доказательство. (i) Пусть $a \in R \setminus \mathfrak{m}$. Рассмотрим идеал $\mathfrak{a}$, порожденный $\mathfrak{m}$ и a. Так как $a \notin \mathfrak{m}$, то $\mathfrak{a} = R$. Следовательно, $1 = ac + d$ для некоторых $c \in R$, $d \in \mathfrak{m}$. Тогда образ элемента c в факторкольце $R/\mathfrak{m}$ является обратным к образу элемента a.

(ii) Следует из (i). □

Пример 2.1.5 (i) Нулевой идеал является простым тогда и только тогда, когда в кольце R нет делителей нуля. Нулевой идеал является максимальным тогда и только тогда, когда любой элемент $R \setminus 0$ обратим, т.е. R – поле.

(ii) В *факториальном кольце* (т.е. в кольце без делителей нуля и с однозначным разложением на простые множители) ненулевой главный идеал является простым тогда и только тогда, когда он порожден простым элементом.

(ii) Согласно сказанному выше простые идеалы в кольце $\mathbb{Z}$ – это главные идеалы (0) и (p), где p – простое. Идеалы (p) также являются максимальными, поэтому $\mathbb{Z}_p = \mathbb{Z}/(p)$ – поле. Это поле также обозначается $\mathbb{F}_p$ (для простого p).

(ii) Так как кольцо многочленов $\Bbbk[x]$ над полем – кольцо главных идеалов, то любой максимальный идеал имеет вид (f), где f – неприводимый многочлен. Любой простой идеал или максимален или является нулевым. Таким образом, если f –

неприводимый многочлен, то $\Bbbk[x]/(f)$ – поле. Ясно, что $\Bbbk[x]/(f)$ содержит подполе, изоморфное $\Bbbk$ и многочлен f имеет корень в $\Bbbk[x]/(f)$. Эта процедура называется *присоединением к полю корня неприводимиго многочлена.* Например, $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

(iii) В кольце многочленов от нескольких переменных $\Bbbk[x_1, \ldots, x_n]$ идеал $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ максимален (он состоит из всех многочленов, обращающихся в нуль в точке $(\alpha_1, \ldots, \alpha_n)$). В этом кольце есть также много простых немаксимальных идеалов. Например, любой идеал, порожденный неприводимым многочленом прост.

Упражнения. **(1)** Являются ли следующие кольца кольцами главных идеалов: $\mathbb{Z}_n$, $\mathbb{Z}[\sqrt{-3}]$?

(2) Докажите, что кольцо $\mathbb{Z}[i]$ является кольцом главных идеалов. *Указание.* Используйте то, что оно евклидово, т.е. в нем имеет место алгоритм деления с остатком: для любых $a, b \in \mathbb{Z}[i]$ существуют $q, r \in \mathbb{Z}[i]$ такие, что $a = bq + r$ и $|r| < |b|$. Для доказательства последнего оцените $|r/b| = |a/b - q|$.

(3) Докажите, что кольцо $\mathbb{Z}[\omega]$, где ω – первообразный корень степени 3 из 1, является кольцом главных идеалов. *Указание.* Воспользуйтесь указаниями предыдущей задачи.

(4) Докажите, что кольцо формальных степенных рядов $\Bbbk[[x]]$ над полем $\Bbbk$ является кольцом главных идеалов. Докажите то же самое для кольца сходящихся степенных рядов $\mathbb{C}\{x\}$.

(5) Пусть R – кольцо без делителей нуля, являющееся кольцом главных идеалов. Докажите, что оно факториально.

(6) Пусть $f\colon R \to R'$ – сюръективный гомоморфизм колец. Докажите, что если R – кольцо главных идеалов, то таковым же является и R'. Верно ли обратное?

(7) Докажите, что кольцо функций дифференцируемых в точке не является кольцом главных идеалов. Опишите максимальные идеалы в этом кольце.

(8) Пусть $\Bbbk$ поле алгебраически замкнуто и $\operatorname{char}\Bbbk \neq 2$. Рассмотрим факторкольцо $R := \Bbbk[x, y]/(y^2 - x^3 + x)$. Докажите, что в кольце R нет делителей нуля. Докажите, что обратимые элементы кольца R – в точности ненулевые элементы $\Bbbk$. Докажите, что кольцо R не является факториальным.

2.2. Алгебраические расширения полей

Пусть $\mathbb{K}$ – поле и пусть $\Bbbk$ – его подполе. В этом случае говорят, что $\mathbb{K}/\Bbbk$ – *расширение полей*. Ясно, что $\mathbb{K}$ является векторным пространством над $\Bbbk$. Расширение $\mathbb{K}/\Bbbk$ называется *конечным*, если $\mathbb{K}$ конечномерно над $\Bbbk$. Размерность $\mathbb{K}$ как векторного пространства над $\Bbbk$ называется *степенью* расширения $\mathbb{K}/\Bbbk$ и обозначается $[\mathbb{K} : \Bbbk]$.

Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей. Для элементов $\vartheta_1, \ldots, \vartheta_n \in \mathbb{K}$ обозначим через $\Bbbk[\vartheta_1, \ldots, \vartheta_n]$ (соответственно, через $\Bbbk(\vartheta_1, \ldots, \vartheta_n)$) – наименьшее подкольцо (соответственно подполе) в $\mathbb{K}$, содержащее $\Bbbk$ и все $\vartheta_1, \ldots, \vartheta_n$. Ясно, что

$$\Bbbk[\vartheta_1, \ldots, \vartheta_n] = \Big\{ \sum \alpha_{k_1,\ldots,k_n} \vartheta_1^{k_1} \cdots \vartheta_n^{k_n} \mid \alpha_{k_1,\ldots,k_n} \in \Bbbk,\ k_j \geq 0 \Big\},$$

$$\Bbbk(\vartheta_1, \ldots, \vartheta_n) = \Big\{ \tfrac{\beta}{\gamma} \mid \beta, \gamma \in \Bbbk[\vartheta_1, \ldots, \vartheta_n], \quad \gamma \neq 0 \Big\}.$$

Определение 2.2.1 Мы скажем, что элемент $\vartheta \in \mathbb{K}$ *алгебраичен* над $\Bbbk$, если существует ненулевой многочлен $f(x) \in \Bbbk[x]$, для которого $f(\vartheta) = 0$. В противном случае элемент ϑ называется *трансцендентным* над $\Bbbk$. Расширение полей $\mathbb{K}/\Bbbk$ называется *алгебраическим*, если каждый элемент $\vartheta \in \mathbb{K}$ алгебраичен над $\Bbbk$.

Пример 2.2.2 (i) Пусть $\Bbbk = \mathbb{Q}$, а $\mathbb{K} = \mathbb{C}$. Хорошо известно, что множество $\mathbb{Q}[t]$ всех многочленов над $\mathbb{Q}$ счетно. Поэтому и счетно множество всех алгебраических элементов $A \subset \mathbb{C}$. Однако поле $\mathbb{C}$ несчетно. Это показывает, что трансцендентных над $\mathbb{Q}$ элементов множества $\mathbb{C}$ "существенно больше" чем алгебраических.

(ii) Для независимой переменной t через $\Bbbk(t)$ мы будем обозначать поле рациональных дробей над $\Bbbk$. Любой элемент $f \in \Bbbk(t) \setminus \Bbbk$ является трансцендентным.

Как и выше, пусть $\mathbb{K}/\Bbbk$ – любое расширение полей и пусть $\vartheta \in \mathbb{K}$ – алгебраический над $\Bbbk$ элемент.

Определение 2.2.3 Ненулевой многочлен $\mu_\vartheta^{\Bbbk}(x) \in \Bbbk[x]$ минимальной степени, для которого ϑ является корнем, называется

минимальным многочленом элемента ϑ над $\Bbbk$. Если это не приводит к путанице, вместо $\mu_\vartheta^\Bbbk(x)$ мы будем писать просто $\mu_\vartheta(x)$ или даже $\mu(x)$.

Следствие 2.2.4 *Если $\mathbb{K}/\Bbbk$ – конечное расширение, то любой элемент $\beta \in \mathbb{K}$ является алгебраическим над $\Bbbk$.*

Доказательство. Пусть n – степень расширения $\mathbb{K}/\Bbbk$. Тогда $n+1$ элементов 1, β, β^2,..., β^n линейно зависимы над $\Bbbk$. Таким образом, $\sum_{i=0}^n \lambda_i \beta^i = 0$ для некоторых $\lambda_i \in \Bbbk$ и β является корнем многочлена $\sum_{i=0}^n \lambda_i x^i \in \Bbbk[x]$. □

Отметим также, что отображение $\mathscr{A}_\vartheta \colon \mathbb{K} \to \mathbb{K}$, заданное формулой $\mathscr{A}_\vartheta(\beta) = \vartheta\beta$, является линейным оператором. Здесь $\mathbb{K}$ рассматривается как (возможно бесконечномерное) векторное пространство над $\Bbbk$. Многочлен $\mu_\vartheta(x)$ совпадает с минимальным многочленом этого линейного оператора. Поэтому следствие 2.2.4 является также следствием теоремы Гамильтона-Кэли из линейной алгебры.

Предложение 2.2.5 (i) *Если $f(x) \in \Bbbk[x]$ – многочлен такой, что $f(\vartheta) = 0$, то $f(x)$ делится на минимальный многочлен $\mu_\vartheta(x)$. В частности, минимальный многочлен определен однозначно с точностью до постоянного множителя.*

(ii) *Минимальный многочлен $\mu(x)$ элемента ϑ неприводим в $\Bbbk[x]$.*

Доказательство. Разделим $f(x)$ на $\mu(x) = \mu_\vartheta(x)$ с остатком: $f(x) = \mu(x)g(x) + r(x)$. Тогда

$$0 = f(\vartheta) = \mu(\vartheta)g(\vartheta) + r(\vartheta) = r(\vartheta).$$

Так как $\deg r(x) < \deg \mu(x)$, то $r(x) = 0$. Это доказывает (i).

Для доказательства (ii) предположим, что $\mu(x) = \mu_1(x)\mu_2(x)$. Тогда $\mu_1(\vartheta) = 0$ или $\mu_2(\vartheta) = 0$. Это противоречит минимальности многочлена $\mu(x)$. □

Предложение 2.2.6 *Если ϑ алгебраичен над $\Bbbk$, то поле $\Bbbk(\vartheta)$, рассматриваемое как векторное пространство над $\Bbbk$, имеет размерность равную степени многочлена $\mu_\vartheta(x)$. Элементы $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ составляют базис $\Bbbk(\vartheta)/\Bbbk$.*

Доказательство. Действительно, элементы $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ линейно независимы над $\Bbbk$ (иначе $\sum_{i=0}^{n-1} \lambda_i \vartheta^i = 0$ для некоторых $\lambda_i \in \Bbbk$ и мы получаем многочлен степени меньшей чем $\mu(x)$, который аннулирует ϑ). Далее любой элемент поля $\Bbbk(\vartheta)$ имеет вид $f(\vartheta)/g(\vartheta)$, где $f(x)$, $g(x)$ – многочлены над $\Bbbk$. Так как $g(\vartheta) \neq 0$, то $\mu(x)$ не делит $g(x)$. Поэтому $\mu(x)$ и $g(x)$ взаимно просты. Следовательно, существуют многочлены $u(x)$, $v(x) \in \Bbbk[x]$ такие, что $\mu(x)u(x)+g(x)v(x) = 1$. Таким образом, $f(\vartheta)g(\vartheta)v(\vartheta) = f(\vartheta)$ и $f(\vartheta)v(\vartheta) = f(\vartheta)/g(\vartheta)$, т.е. любой элемент $\beta \in \Bbbk(\vartheta)$ представляется в виде многочлена от ϑ:

$$\beta = h(\vartheta), \quad h(x) \in \Bbbk[x].$$

Более того, снова применяя деление с остатком, мы можем считать, что $\deg h(x) \leq n-1$. Но это и означает, что β является линейной комбинацией элементов $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$. □

Предложение 2.2.7 *Если $\mathbb{K}/\Bbbk$ – любое расширение полей, то элементы поля $\mathbb{K}$, алгебраические над $\Bbbk$, также образуют поле.*

Доказательство. Достаточно доказать, что для любых двух алгебраических элементов α, $\beta \in \mathbb{K}$ элементы $\alpha \pm \beta$, $\alpha\beta$ и α/β также являются алгебраическими. Согласно следствию 2.2.4, для этого достаточно доказать, что расширение $\Bbbk(\alpha, \beta)/\Bbbk$ конечно. Но $\Bbbk(\alpha, \beta) = \Bbbk(\alpha)(\beta)$. Согласно предложению 2.2.6 расширения $\Bbbk(\alpha)/\Bbbk$ и $\Bbbk(\alpha)(\beta)/\Bbbk(\alpha)$ конечны. Требуемый факт теперь легко выводится из упражнения (1). □

Определение 2.2.8 Пусть $\Bbbk$ – произвольное поле. *Полем разложения* многочлена $f(x) \in \Bbbk[x]$ называется поле $\mathbb{K} \supset \Bbbk$ такое, что $f(x)$ над $\mathbb{K}$ разлагается на линейные множители: $f(x) = c\prod(x - \alpha_i)$, где $c \in \Bbbk$, а $\alpha_i \in \mathbb{K}$ и корни α_i порождают $\mathbb{K}$ над $\Bbbk$.

Теорема 2.2.9 *Пусть* $\Bbbk$ *– поле и* $f(x)$ *– многочлен над* $\Bbbk$. *Существует поле* $\mathbb{K} \supset \Bbbk$, *являющееся полем разложения для* $f(x)$ *над* $\Bbbk$. *Любые два таких поля* $\mathbb{K}$ *изоморфны над* $\Bbbk$.

Набросок доказательства. Поле $\mathbb{K}$ получается последовательным присоединением корней неприводимых множителей многочлена $f(x)$. Доказательство единственности см., например, в [Кос01, гл. 5, §1]. □

Пусть $\Bbbk$ – произвольное поле. Обозначим через M множество всех $m \in \mathbb{N}$ таких, что $\underbrace{1 + \cdots + 1}_{m} = 0$. *Характеристикой* $\operatorname{char} \Bbbk$ поля $\Bbbk$ называется число

$$\operatorname{char} \Bbbk = \begin{cases} \min M, & \text{если } M \neq \varnothing, \\ 0, & \text{если } M = \varnothing. \end{cases} \tag{2.2.10}$$

Таким образом, $\operatorname{char} \Bbbk$ – порядок единичного элемента 1 в аддитивной группе $\Bbbk$, если этот порядок конечен. Если же порядок 1 бесконечен, то характеристика поля считается равной нулю. Ясно, что характеристика конечного поля отлична от нуля (иначе в этом поле имеется бесконечно много элементов вида $1+\cdots+1$).

Лемма 2.2.11 *Характеристика поля может быть или нулем, или простым числом.*

Доказательство. Предположим, что $\operatorname{char} \Bbbk = nm$, где n, $m > 1$. Тогда по (2.2.13) имеем $0 = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1)$. Отсюда $n \cdot 1$ или $m \cdot 1$, что противоречит определению характеристики (2.2.10). □

Для любого натурального n и любого элемента поля $a \in \Bbbk$ положим $n \cdot a := \underbrace{a + \cdots + a}_{n}$ и $(-n) \cdot a := n \cdot (-a)$. Таким образом, определено произведение $n \cdot a$ любого целого числа n на элемент поля a.

Легко проверить, что отображение

$$\phi \colon \mathbb{Z} \to \Bbbk, \qquad \phi(n) = n \cdot 1 \tag{2.2.12}$$

является гомоморфизмом колец. Действительно,

$$\phi(n+m) = (n+m)\cdot 1 = \underbrace{1+\cdots+1}_{n+m} = \underbrace{1+\cdots+1}_{n} + \\ + \underbrace{1+\cdots+1}_{m} = n\cdot 1 + m\cdot 1 = \phi(n) + \phi(m),$$

$$\phi(nm) = (nm)\cdot 1 = \underbrace{1+\cdots+1}_{nm} = (\underbrace{1+\cdots+1}_{n} \\ (\underbrace{1+\cdots+1}_{m}) = (n\cdot 1)(m\cdot 1) = \phi(n)\phi(m). \quad (2.2.13)$$

Непосредственно из определения характеристики получаем следующее

Утверждение 2.2.14 *Если* $\operatorname{char}\Bbbk = 0$, *то гомоморфизм* ϕ *инъективен. Если же* $\operatorname{char}\Bbbk = p > 0$, *то* $\operatorname{Ker}\phi = (p)$.

Определение 2.2.15 Поле, не содержащее ни одного собственного подполя, называется *простым полем*.

Каждое поле $\Bbbk$ содержит единственное простое поле – пересечение всех подполей в $\Bbbk$. Примерами простых полей являются поле рациональных чисел $\mathbb{Q}$ и поля вычетов $\mathbb{Z}_p = \mathbb{F}_p$ по простому модулю p. Верно и обратное:

Теорема 2.2.16 (см. [Лен68, гл. II]) *Любое простое поле* $\Bbbk$ *изоморфно* $\mathbb{Q}$ *или* $\mathbb{F}_p$.

Доказательство (в случае $\operatorname{char}\Bbbk = p > 0$**).** Из утверждения 2.2.14 и теоремы о гомоморфизме получаем, что $\operatorname{Im}\phi \simeq \mathbb{Z}/\operatorname{Ker}\phi = \mathbb{Z}/(p)$ является подполем. □

Упражнения. **(1)** Пусть имеются конечные расширения полей $\mathbb{K}/\mathbb{L}$ и $\mathbb{L}/\Bbbk$. Докажите, что степень $\mathbb{K}/\Bbbk$ равна произведению степеней расширений $\mathbb{K}/\mathbb{L}$ и $\mathbb{L}/\Bbbk$.

(2) Пусть $\Bbbk$ – поле. Могут ли быть изоморфны мультипликативная и аддитивная группы $\Bbbk$? *Указание.* Рассмотрите элементы порядка 2.

(3) Пусть $\Bbbk$ – поле. Докажите, что аддитивная группа $\Bbbk$ является циклической тогда и только тогда, когда она изоморфна $\mathbb{Z}_p$, где p – простое.

(4) Докажите, что аддитивная группа поля $\Bbbk$ конечно порождена тогда и только тогда, когда она имеет конечный порядок.

(5) Пусть $\mathbb{K}/\Bbbk$ конечное расширение полей степени n. Докажите, что существует не более n различных автоморфизмов поля $\mathbb{K}$, оставляющих неподвижными все элементы из $\Bbbk$. *Указание.* Разложите расширение $\mathbb{K}/\Bbbk$ в цепочку расширений $\mathbb{K} = \Bbbk(\vartheta_1, \ldots, \vartheta_m) \supset \Bbbk(\vartheta_1, \ldots, \vartheta_{m-1}) \supset \cdots$.

(6) Поле $\Bbbk$ называется *упорядоченным*, если в нем задано подмножество $\mathcal{P}$ (подмножество "положительных" элементов) такое, что

a) для любого ненулевого элемента a или $a \in \mathcal{P}$, или $-a \in \mathcal{P}$;

b) если $a \in \mathcal{P}$, то $-a \notin \mathcal{P}$;

c) если a, $b \in \mathcal{P}$, то $a + b \in \mathcal{P}$ и $ab \in \mathcal{P}$.

Если поле $\Bbbk$ упорядочено, то для любых двух элементов a, $b \in \Bbbk$ положим $a \succ b$, если $b - a \in \mathcal{P}$. Проверьте, что для отношения $\succ$ выполнены обычные правила обращения с неравенствами. Докажите, что поле характеристики $p > 0$ не может быть упорядоченным, а поле $\mathbb{Q}$ может быть упорядочено единственным (стандартным) образом.

2.3. Конечные поля

В этом параграфе мы рассмотрим конечные поля, т.е. поля состоящие из конечного числа элементов. Напомним, что характеристика конечного поля $\Bbbk$ отлична от нуля, является простым числом p и $\Bbbk$ содержит простое подполе $\Bbbk_0$ изоморфное $\mathbb{Z}_p = \mathbb{F}_p$.

Теорема 2.3.1 *Пусть $\Bbbk$ – конечное поле характеристики $p > 0$. Тогда*

(i) *$\Bbbk$ является конечномерным векторным пространством над $\Bbbk_0$,*

(ii) *число элементов $\Bbbk$ равно p^m, где $m = \dim_{\Bbbk_0} \Bbbk$,*

(iii) *каждый элемент поля $\Bbbk$ является корнем многочлена $x^{p^m} - x$.*

Доказательство. Из определения поля получаем, что $\Bbbk$ – векторное пространство над $\Bbbk_0$. Его конечномерность – следствие конечности $\Bbbk$. Утверждение о числе элементов следует из того, что каждый элемент векторного пространства однозначно задается своими координатами $(x_1, \ldots, x_m)$ (в фиксированном базисе), а в нашем случае для каждой координаты x_i имеется ровно p возможностей, так как $x_i \in \mathbb{Z}_p$. Наконец, по теореме Лагранжа порядок каждого элемента a группы $\Bbbk^*$ делит ее порядок. Поэтому $a^{p^m-1} - 1 = 0$ для любого $a \neq 0$. Очевидно, что тогда $a^{p^m} - a = 0$ для всех $a \in \Bbbk$. Теорема доказана. □

Следствие 2.3.2 *В конечном поле из $q = p^m$ элементов многочлен $x^q - x$ разлагается на линейные множители. Этот многочлен имеет только простые корни.*

Доказательство. Согласно теореме Безу многочлен $x^q - x$ имеет не более q корней (с учетом кратностей). С другой стороны, по пункту (iv) теоремы 2.3.1 имеется q различных корней. □

Таким образом, конечное поле из $q = p^m$ элементов совпадает с полем разложения многочлена $x^q - x$ над $\mathbb{F}_p$ (см. 2.2.8). Верно и обратное:

Лемма 2.3.3 *Пусть $q = p^m$, p – простое. Поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$ содержит ровно q элементов и совпадает с множеством корней $x^q - x$.*

Доказательство. Поле разложения $\mathbb{K}$ многочлена $x^q - x$ над $\mathbb{F}_p$ конечно (поскольку является конечномерным пространством над $\mathbb{F}_p$), а значит состоит из p^l элементов. Рассмотрим подмножество $M \subset \mathbb{K}$, состоящее из всех корней $x^q - x$. Докажем, что M – поле. Действительно, нетривиально проверить только, что M замкнуто относительно сложения. Пусть α, $\beta \in M$, т.е. $\alpha^q = \alpha$ и $\beta^q = \beta$. Тогда

$$(\alpha + \beta)^q = \alpha^q + q\alpha^{q-1}\beta + \cdots + \frac{q!}{(q-i)! \cdot i!}\alpha^{q-i}\beta^i + \cdots + \beta^q.$$

Так как $\frac{q!}{(q-i)!\cdot i!}$ делится на p при $i \neq 0, q$, то все члены, кроме первого и последнего, обращаются в нуль. Таким образом,

$$(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$$

и M – поле. Многочлен $x^q - x$ разлагается на линейные множители в M, поэтому M – поле разложения для $x^q - x$ и $M = \mathbb{K}$. Так как $(x^q - x)' = qx^{q-1} - 1 = -1$, то $x^q - x$ не имеет кратных множителей и в $\mathbb{K}$ имеется ровно q элементов. □

Из леммы 2.3.3 и теоремы 2.2.9 немедленно получаем следующую

Теорема 2.3.4 *Конечное поле из p^m элементов существует и единственно с точностью до изоморфизма.*

Поле из $q = p^m$ элементов будет обозначатся через $\mathbb{F}_q$.

Следствие 2.3.5 *Поле $\mathbb{F}_{p^m}$ содержит подполе из r элементов тогда и только тогда, когда $r = p^l$, где l делит m. Это подполе изоморфно $\mathbb{F}_{p^l}$.*

Доказательство. Пусть $\Bbbk \subset \mathbb{F}_{p^m}$ подполе из r элементов. Рассмотрим $\mathbb{F}_{p^m}$ как векторное пространство над $\Bbbk$. Положим $d = \dim_{\Bbbk} \mathbb{F}_{p^m}$. Как и в доказательстве пункта (iii) теоремы 2.3.1 получаем, что $p^m = r^d$. Отсюда $r = p^l$, где $ld = m$.

Наоборот, пусть $r = p^l$, где $ld = m$ для некоторого $d \in \mathbb{N}$. Пусть $\Bbbk \subset \mathbb{F}_{p^m}$ – подмножество, состоящее из всех корней многочлена $x^{p^l} - x$. По лемме 2.3.6 (ниже) многочлен $x^{p^l} - x$ делит $x^{p^m} - x$. Поэтому все эти корни – простые и их ровно p^l. С другой стороны, как и в доказательстве теоремы 2.3.4 легко показать, что $\Bbbk$ – поле. □

Лемма 2.3.6 *Многочлен $x^r - x$ делит многочлен $x^{r^d} - x$ (над любым полем).*

Доказательство. Достаточно доказать, что $x^{r-1} - 1$ делит $x^{r^d-1} - 1$. Так как $r - 1$ делит $r^d - 1$, то мы можем записать.

$r^d - 1 = (r-1)s$, $s \in \mathbb{N}$. Получим

$$x^{r^d-1} - 1 = x^{(r-1)s} - 1 = (x^{r-1} - 1)\big(x^{(r-1)(s-1)} + \cdots + x^{r-1} + 1\big).$$

□

Теорема 2.3.7 *Мультипликативная группа $\mathbb{F}_q^*$ конечного поля $\mathbb{F}_q$ является циклической.*

Доказательство. Для доказательства достаточно построить элемент $b \in \mathbb{F}_q^*$, порядок $|b|$ которого равен порядку группы $|\mathbb{F}_q^*| = q - 1$. Пусть M – наименьшее общее кратное порядков всех элементов $\mathbb{F}_q^*$. Тогда $a^M = 1$ для любого $a \in \mathbb{F}_q^*$ и по теореме Лагранжа M делит $q-1$. С другой стороны, по теореме Безу уравнение $x^M - 1 = 0$ имеет не более M корней, т.е. $q - 1 \leq M$. Отсюда $M = q-1$. Пусть $M = q-1 = p_1^{n_1} \cdots p_r^{n_r}$ – разложение на простые множители. По конструкции для каждого $i = 1, \ldots, r$ существует элемент $a_i \in \mathbb{F}_q^*$, порядок которого $|a_i|$ делится на $p_i^{n_i}$. Положим $b_i := a_i^{|a_i|/p_i^{n_i}}$. Тогда $|b_i| = p_i^{n_i}$. Теперь воспользуемся следующей леммой.

Лемма 2.3.8 *Пусть в абелевой группе A порядки элементов a и b взаимно просты. Тогда порядок их произведения равен произведению порядков: $|ab| = |a||b|$.*

Доказательство. Положим $|a| = \alpha$, $|b| = \beta$ и $|ab| = \gamma$. Ясно, что $(ab)^{\alpha\beta} = 1$. Поэтому γ делит $\alpha\beta$. Так как НОД $(\alpha, \beta) = 1$, то $\alpha u + \beta v = 1$ для некоторых α, $\beta \in \mathbb{Z}$. Отсюда

$$a = a^{\alpha u + \beta v} = a^{\beta v} = (ab)^{\beta v}, \quad b = b^{\alpha u + \beta v} = a^{\alpha u} = (ab)^{\alpha u}.$$

Следовательно, элементы a и b принадлежат циклической подгруппе, порожденной ab, и по теореме Лагранжа α и β делят γ. □

Используя эту лемму, индукцией по l доказываем, что порядок элемента $b_1 \cdots b_l$ равен $p_1^{n_1} \cdots p_l^{n_l}$. Отсюда $|b_1 \cdots b_r| = p_1^{n_1} \cdots p_r^{n_r} = q - 1$. Таким образом, мы можем положить $b = b_1 \cdots b_r$. Теорема доказана. □

Теоремы 2.3.1, 2.3.4 и 2.3.7 дают возможность описать неприводимые многочлены над конечными полями. Из теоремы 2.3.7 немедленно получаем следующее.

Следствие 2.3.9 *Для любого расширения конечных полей $\mathbb{K}/\Bbbk$ существует элемент $\vartheta \in \mathbb{K}$, который порождает $\mathbb{K}$ над $\Bbbk$ (т.е., $\mathbb{K} = \Bbbk(\vartheta)$).*

Следствие 2.3.10 *Пусть $f(x)$ – неприводимый многочлен степени d над $\mathbb{F}_q$ (где $q = p^m$). Тогда $f(x)$ является делителем $x^{q^d} - x$. Для любого d существует неприводимый многочлен степени d над $\mathbb{F}_q$.*

Доказательство. Пусть $\mathbb{K}$ – поле, полученное присоединением корня многочлена f к $\mathbb{F}_q$ (т.е. $\mathbb{K} = \mathbb{F}_q[x]/(f)$). Тогда $\mathbb{K}$ – конечное поле и размерность $\mathbb{K}$ как векторного пространства над $\mathbb{F}_q$ равна d. Как и в доказательстве пункта (iii) теоремы 2.3.1 получаем, что $\mathbb{K}$ состоит из q^d элементов и поэтому $\mathbb{K} \simeq \mathbb{F}_{q^d}$. Согласно следствию 2.3.2 многочлены $f(x)$ и $x^{q^d} - x$ имеют общий корень в $\mathbb{K}$. Следовательно, НОД $(f(x), x^{q^d} - x) \neq 1$. Но наибольший общий делитель многочленов может быть вычислен при помощи алгоритма Евклида и не зависит от основного поля. Так как многочлен $f(x)$ неприводим над $\mathbb{F}_q[x]$, то имеется единственная возможность НОД $(f(x), x^{q^d} - x) = f(x)$. Отсюда получается первое утверждение.

Для доказательства второго применим следствие 2.3.9 к $\mathbb{F}_{q^d}/\mathbb{F}_q$. Пусть ϑ – порождающий элемент поля $\mathbb{F}_{q^d}$ над $\mathbb{F}_q$. Рассмотрим минимальный многочлен $\mu_\vartheta(x)$ для ϑ. Тогда $\mu_\vartheta(x)$ и $\deg \mu_\vartheta(x) = d$ (проверьте самостоятельно). Это доказывает следствие. □

Пример 2.3.11 Построим поле $\mathbb{F}_8$ из 8 элементов. Согласно следствию 2.3.9, любой элемент из $\mathbb{F}_8$ может быть записан как линейная комбинация $\alpha_0 + \alpha_1\vartheta + \alpha_2\vartheta^2$, $\alpha_i \in \mathbb{F}_2$. Для составления таблицы умножения мы должны найти минимальный многочлен $\mu(x) = \mu_\vartheta(x)$ элемента ϑ. Воспользуемся следствием 2.3.10.

Получим, что $\mu(x)$ делит $(x^8-x)/(x^2-x) = x^6+\cdots+1$. Легко видеть, что $x^6+\cdots+1 = (x^3+x+1)(x^3+x^2+1)$. Таким образом, мы можем взять $\mu(x) = x^3+x+1$ или x^3+x^2+1. Выбрав в качестве $\mu(x)$ один из этих двух многочленов, мы можем однозначно восстановить таблицу умножения. Например, в первом случае мы имеем $\vartheta^3 = -\vartheta - 1 = \vartheta + 1$. По теореме 2.2.9 обе возможности приводят к изоморфным полям.

Конструкция алгебраического замыкания конечного поля

Поле $\mathbb{K}$ называется *алгебраически замкнутым*, если любой многочлен $f(x) \in \mathbb{K}[x]$ имеет корень в $\mathbb{K}$. Например, основная теорема алгебры утверждает, что поле комплексных чисел $\mathbb{C}$ алгебраически замкнуто. *Алгебраическим замыканием поля* $\Bbbk$ называется алгебраическое расширение $\bar{\Bbbk}/\Bbbk$ такое, что поле $\bar{\Bbbk}$ алгебраически замкнуто. Таким образом, $\mathbb{C}$ – алгебраическое замыкание поля действительных чисел $\mathbb{R}$. Однако $\mathbb{C}/\mathbb{Q}$ не является алгебраическим замыканием (поскольку $\mathbb{C}$ содержит трансцендентные над $\mathbb{Q}$ элементы). Следующая теорема является частным случаем общей конструкции, см. [Лен68].

Теорема 2.3.12 *Для любого конечного поля $\mathbb{F}_q$ существует алгебраическое расширение $\bar{\mathbb{F}}_q/\mathbb{F}_q$ такое, что $\bar{\mathbb{F}}_q$ алгебраически замкнуто.*

Доказательство. По индукции построим цепочку полей

$$\mathbb{F}_q = \mathbb{F}_{q^{1!}} \subset \mathbb{F}_{q^{2!}} \subset \mathbb{F}_{q^{3!}} \subset \cdots$$

где каждое $\mathbb{F}_{q^{k!}}$ – поле разложения многочлена $x^{q^{k!}} - x$ над $\mathbb{F}_{q^{(k-1)!}}$ (см. следствие 2.3.2). Положим $\bar{\mathbb{F}}_q := \cup_{k=1}^{\infty} \mathbb{F}_{q^{k!}}$ и определим на $\bar{\mathbb{F}}_q$ операции сложения и умножения естественным образом: если α, $\beta \in \bar{\mathbb{F}}_q$, то существует k такое, что α, $\beta \in \mathbb{F}_{q^{k!}}$ и поэтому определены элементы $\alpha+\beta$, $\alpha\beta \in \mathbb{F}_{q^{k!}} \subset \bar{\mathbb{F}}_q$. Легко показать, что $\bar{\mathbb{F}}_q$ поле. Предположим, что некоторый многочлен $f(x) \in \bar{\mathbb{F}}_q[x]$ степени $d \geq 2$ не имеет корней в $\bar{\mathbb{F}}_q$. Мы можем считать, что $f(x)$ неприводим. Снова $f(x) \in \mathbb{F}_{q^{k!}}[x]$ для некоторого k. Тогда $f(x)$ неприводим и над $\mathbb{F}_{q^{k!}}$. Согласно следствию

2.3.10 многочлен $f(x)$ является делителем $x^{q^{k!d}}-x$. Так как $(kd)!$ делится на $k!d$, то многочлен $x^{q^{l!}}-x$ делится на $x^{q^{k!d}}-x$, а поэтому и на $f(x)$. Следовательно, $f(x)$ разлагается на линейные множители в $\mathbb{F}_{q^{l!}}$ и в $\bar{\mathbb{F}}_q$. Противоречие. $\square$

Заметим, что в нашей конструкции мы можем заменить цепочку полей $\mathbb{F}_{q^{k!}}$ на $\mathbb{F}_{q^{d_k}}$, где d_1, d_2, $d_3, \ldots$ – строго возрастающая последовательность натуральных чисел таких, что a) каждое d_k делит d_{k+1} и b) для любого натурального m существует d_k, делящееся на m. Несмотря на неоднозначность конструкции, поле $\bar{\mathbb{F}}_q$ единственно с точностью до изоморфизма (см. упражнение (12), стр. 31 в конце параграфа).

В случае, когда $q = p$ – простое число $\mathbb{F}_q$ – поле вычетов по модулю p. Из изложенных выше результатов несложно получаются хорошо известные теоретико-числовые следствия.

Следствие 2.3.13 (из теоремы 2.3.7**)** *Для любого простого p существует целое число c такое, что его степени $1, c, c^2, \ldots, c^{p-2}$ исчерпывают все ненулевые вычеты по модулю p.*

Следствие 2.3.14 (теорема Вильсона) *Число p является простым тогда и только тогда, когда $(p-1)! \equiv -1 \mod p$.*

Доказательство. Пусть p – простое. Поскольку $1, \ldots, p-1$ (рассматриваемые как элементы поля $\mathbb{F}_p$) являются корнями многочлена $x^{p-1}-1$, то по теореме Виета свободный член этого многочлена совпадает с $(-1)^{p-1} \cdot 1 \cdots (p-1)$. Обратно, если p не является простым, то $(p-1)!$ делится на p. Противоречие. $\square$

Следствие 2.3.15 (малая теорема Ферма) *Если p – простое, то $a^{p-1} \equiv 1 \mod p$ для любого a, взаимно простого с p.*

Доказательство. Поскольку $1, \ldots, p-1$ (рассматриваемые как элементы $\mathbb{F}_p$) являются корнями многочлена $x^{p-1} - 1$, то по теореме Виета свободный член этого многочлена совпадает с $(-1)^{p-1} \cdot 1 \cdots (p-1)$. $\square$

Приведем еще одно следствие из теоремы 2.3.7. Напомним, что через $\mathbb{Z}_n^*$ мы обозначаем группу обратимых элементов кольца вычетов $\mathbb{Z}_n$.

Предложение 2.3.16 *Если p – нечетное простое, то группа $\mathbb{Z}_{p^k}*$ – циклическая.*

Доказательство. Ясно, что порядок $\mathbb{Z}_{p^k}^*$ равен $p^{k-1}(p-1)$. Согласно теореме 2.3.7 циклической является группа $\mathbb{Z}_p^*$. Таким образом, существует $a \in \mathbb{Z}$ такое, что его образ в $\mathbb{Z}_p^*$ имеет порядок $p-1$. В частности, $a^{p-1} = 1 + pw$ для некоторого $w \in \mathbb{Z}$. Тогда

$$(a+pt)^{p-1} = a^{p-1} + (p-1)a^{p-2}pt + p^2v = \\ = 1 + p\Big(w + (p-1)a^{p-2}t + vp\Big),$$

где $v \in \mathbb{Z}$. Выберем t таким образом, что $w + (p-1)a^{p-2}t + vp$ не делится на p и положим $b := a + pt$, $u := w + (p-1)a^{p-2}t + vp$. Имеем

$$b \equiv a \mod p, \qquad b^{p-1} = 1 + pu, \quad p \nmid u.$$

По индукции получаем

$$\begin{aligned} b^{(p-1)p} &= (1+pu)^p = 1 + p^2u_1, \quad p \nmid u_1, \\ b^{(p-1)p^2} &= (1+pu_1)^p = 1 + p^3u_2, \quad p \nmid u_2, \\ &\ldots \\ b^{(p-1)p^s} &= (1+pu_{s-1})^p = 1 + p^{s+1}u_s, \quad p \nmid u_s. \end{aligned}$$

Мы утверждаем, что образ b в $\mathbb{Z}_{p^k}^*$ является порождающим элементом. Пусть r – порядок b в $\mathbb{Z}_{p^k}^*$. Тогда $b^r \equiv 1 \mod p^k$. В частности, $a^r \equiv b^r \equiv 1 \mod p$. Поэтому r делится на $p-1$ – порядок a в $\mathbb{Z}_p^*$. По теореме Лагранжа $r = (p-1)p^l$, $l \leq k-1$. Следовательно, $b^r = b^{(p-1)p^l} = 1 + p^{l+1}u_l \equiv 1 \mod p^k$, где $p \nmid u_l$. Отсюда немедленно получаем $l + 1 \geq k$. $\square$

Вычисление квадратных корней в конечных полях

Рассмотрим вопрос о эффективном решении уравнения $x^2 = a$ в конечном поле $\mathbb{F}_q$, где $a \neq 0$ и q нечетно.

Во-первых найдем элемент $b \in \mathbb{F}_q$, не являющийся квадратом. Для этого воспользуемся вероятностным алгоритмом.

Утверждение 2.3.17 *Элемент $b \in \mathbb{F}_q^*$ является квадратом тогда и только тогда, когда $b^{(q-1)/2} = 1$.*

Доказательство. Пусть $b = c^2$. Тогда $b^{(q-1)/2} = c^{q-1} = 1$ по теореме Лагранжа. Обратно, предположим, что $b^{(q-1)/2} = 1$. Пусть θ – порождающий элемент циклической группы $\mathbb{F}_q^*$. Запишем $b = \theta^k$. Если k нечетно, то существуют такие целые числа u и v, что $1 = 2u + kv$. Но тогда $\theta = b^v\theta^{2u}$ и $\theta^{(q-1)/2} = 1$. Противоречие показывает, что k четно и мы можем положить $\sqrt{b} = \theta^{k/2}$. □

Вероятностный алгоритм для нахождения b – следующий. Выбираем случайно элемент $b \in \mathbb{F}_q^*$. Вычисляем $b^{(q-1)/2}$ методом последовательного возведения в квадрат. Если $b^{(q-1)/2} \neq 1$, то элемент b удовлетворяет условию. Если же $b^{(q-1)/2} = 1$, то мы выбираем другой $b \in \mathbb{F}_q^*$ и повторяем попытку. Вероятность неудачи на каждом шаге равна $1/2$. Следовательно, вероятность того, что за l шагов мы не найдем нужного нам элемента равна $1/2^l$. Отметим также, что в случае простого q для нахождения b можно воспользоваться символом Якоби и законом взаимности.

Таким образом, мы имеем $b \in \mathbb{F}_q$, не являющийся квадратом. Далее запишем $q-1 = 2^k m$, где m нечетно, а $k \geq 1$. Вычисляем $v := b^m$ и $w := a^{(m+1)/2}$.

Утверждение 2.3.18 *Элемент v является первообразным корнем степени 2^k из единицы.*

Доказательство. Во-первых, $v^{2^k} = b^{m2^k} = b^{q-1} = 1$. Далее предположим, что $v^{2^l} = 1$ для некоторого $0 \leq l < k$. Это означает, что $b^{2^l m} = 1$. Пусть θ – порождающий элемент циклической

группы $\mathbb{F}_q^*$. Тогда $b = \theta^r$ для некоторого $r \in \mathbb{Z}$. Отсюда $\theta^{2^l rm} = 1$ и поэтому $2^l rm$ делится на $q-1 = 2^k m$. Следовательно, r четно и $b = (\theta^{r/2})^2$. Противоречие с нашим выбором b. □

Утверждение 2.3.19 *Элемент w^2/a является корнем степени 2^{k-1} из единицы.*

Доказательство. Действительно, $(w^2/a)^{2^{k-1}} = a^{2^{k-1}m} = (x^2)^{2^{k-1}m} = x^{q-1} = 1$. □

Таким образом, мы можем записать $a = v^s w^2$, где s четно. Тогда корни уравнения $x^2 = a$ запишутся в виде $x = \pm v^h w$, где $0 \le h < 2^k$. Поскольку нас интересует только один корень, то заменяя, если необходимо, h на $h - 2^{k-1}$ мы можем считать, что $0 \le h < 2^{k-1}$. Для того, чтобы вычислить h, запишем его в двоичной записи $h = h_0 + 2h_1 + \cdots 2^{k-2}h_{k-2}$, $h_i = 0$ или 1 и будем последовательно находить h_i.

Сначала возводим w^2/a в степень 2^{k-2}. По доказанному выше $(w^2/a)^{2^{k-2}} = \pm 1$. Полагаем $h_0 = 0$ если $(w^2/a)^{2^{k-2}} = 1$ и $h_0 = 1$ в противном случае. Тогда $((v^{h_0}w)^2/a)^{2^{k-2}} = 1$.

Далее возводим $(v^{h_0}w)^2/a$ в степень 2^{k-3}. Согласно сказанному выше, $((v^{h_0}w)^2/a)^{2^{k-3}} = \pm 1$. Полагаем $h_1 = 0$ если $((v^{h_0}w)^2/a)^{2^{k-3}} = 1$ и $h_1 = 1$ в противном случае. Снова имеем $((v^{h_0+2h_1}w)^2/a)^{2^{k-3}} = 1$.

Продолжаем процесс. На некотором шаге мы найдем $h_0, \ldots, h_{i-1}$. и $(v^{h_0+2h_1+\cdots+2^{i-1}h_{i-1}}w)^2/a$ является корнем степени 2^{k-i-1} из единицы. Возводим этот корень в степень 2^{k-i-2}. Как и выше получим ± 1 и положим $h_i = 0$ или 1. Непосредственно проверяется, что

$$\left(\frac{(v^{h_0+2h_1+\cdots+2^{i-1}h_{i-1}+2^i h_i}w)^2}{a}\right)^{2^{k-i-2}} = 1.$$

На последнем шаге мы найдем h_{k-1} и получим

$$\frac{(v^{h_0+2h_1+\cdots+2^{k-2}h_{k-2}}w)^2}{a} = 1,$$

т.е. мы можем взять $x = v^{h_0+2h_1+\cdots+2^{k-2}h_{k-2}}w$.

Упражнения. **(1)** Выпишите таблицы сложения и умножения в поле из q элементов для $q = 4$, 8, 9, 16.

(2) Найдите все порождающие элементы в группе $\mathbb{F}_{37}^*$.

(3) Сколько решений имеет уравнение $x^n = 1$ в поле $\mathbb{F}_{25}$ для $n = 5$, 6, 30?

(4) При каких q существует квадратный корень из -1 в $\mathbb{F}_q$?

(5) Докажите, утверждение обратное к утверждению теоремы 2.3.7: если мультипликативная группа поля $\Bbbk$ является циклической, то $\Bbbk$ конечно.

(6) Докажите, что поле $\bar{\mathbb{F}}_q$ счетно.

(7) Пусть $\mathbb{K}/\Bbbk$ – алгебраическое расширение полей такое, что любой многочлен $f(x) \in \Bbbk[x]$ имеет корень в $\mathbb{K}$. Докажите, что $\mathbb{K}$ – алгебраическое замыкание $\Bbbk$.

(8) Найдите все неприводимые многочлены степеней 2, 3, 4 и 5 над полем $\mathbb{F}_3$.

(9) Выведите формулу для числа N_d неприводимых многочленов $f_d(x)$ степени d над полем $\mathbb{F}_q$. Сколько существует неприводимых многочленов степени 6 над $\mathbb{F}_4$? *Указание.* Воспользуйтесь тем, что $f(x)$ делит $x^{q^m} - x$ тогда и только тогда, когда d делит m. Отсюда получите формулу $x^{q^m} - x = \prod_{d|m} \prod_{f_d} f_d(x)$.

(10) Пусть $q = p^k \equiv 2 \mod 4$. Докажите, что в поле $\mathbb{F}_q$ для любого $c \neq 0$ в точности одно из уравнений $y^2 = c$ или $y^2 = -c$ имеет решение. *Указание.* Рассмотрите гомоморфизм групп $\mathbb{F}_q^* \to \mathbb{F}_q^*$, $a \to a^2$.

(11) Пусть $q = p^k \equiv 2 \mod 3$. Докажите, что в поле $\mathbb{F}_q$ для любого $c \neq 0$ уравнение $x^3 = c$ имеет в точности одно решение. *Указание.* Рассмотрите гомоморфизм $\mathbb{F}_q^* \to \mathbb{F}_q^*$, $a \to a^3$.

(12) Докажите, что алгебраическое замыкание поля $\bar{\mathbb{F}}_{p^d}$ единственно с точностью до изоморфизма и не зависит от d. *Указание.* Пусть $\bar{\mathbb{F}}_q$ – некоторое алгебраическое замыкание, а $\bar{\mathbb{F}}'_q$ – алгебраическое замыкание из доказательства теоремы 2.3.12. Последовательно постройте вложения $\mathbb{F}_{q^{k!}} \hookrightarrow \bar{\mathbb{F}}_q$ и задайте изоморфизм $\bar{\mathbb{F}}'_q \xrightarrow{\sim} \bar{\mathbb{F}}_q$.

(13) Существует ли бесконечное подполе $\mathbb{K} \subsetneq \bar{\mathbb{F}}_p$?

(14) Рассмотрим кольцо целых гауссовых чисел $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Докажите, что идеалы (3), (7), $(1 + i)$, $(2 + i)$ просты. Чему

изоморфны соответствующие факторкольца? *Указание.* Используйте то, что $\mathbb{Z}[i]$ – *евклидово кольцо* (т.е. кольцо, в котором возможно деление с остатком)

(15) Докажите, что группа $\mathbb{Z}_{2^k}$ не является циклической при $k \geq 3$.

2.4. Проверка чисел на простоту и проблема факторизации

Очень важной задачей криптографии является нахождение случайного простого числа. Для этого нужно иметь эффективные методы проверки чисел на простоту. Поскольку данная проблема выходит далеко за рамки нашего курса, мы обсудим лишь некоторые, наиболее элементарные методы. Малая теорема Ферма является основой многих *вероятностных* критериев таких проверок.

Псевдопростые числа

Согласно малой теореме Ферма, простота числа n влечет выполнение сравнения

$$a^{n-1} \equiv 1 \mod n \tag{2.4.1}$$

для всех $a \in \mathbb{Z}$ таких, что НОД $(n, a) = 1$.

Определение 2.4.2 Пусть n и a – натуральные числа такие, что НОД $(n, a) = 1$. Число n называется *псевдопростым* по основанию a, если для n и a выполнено сравнение (2.4.1).

Отметим, что из псевдопростоты числа не следует его простота: например, $n = 21$ является псевдопростым по основанию $a = 13$, но, очевидно, не является простым.

Предложение 2.4.3 *Зафиксируем $n \in \mathbb{N}$. Множество оснований, по которым n является псевдопростым, образует подгруппу в $P_n \subset \mathbb{Z}_n^*$.*

Доказательство. Очевидно и оставляется читателю. □

Следствие 2.4.4 *Если число n не проходит тест* (2.4.1) *для какого-то основания a, то оно не проходит этот тест для, по крайней мере, половины оснований $a \in \mathbb{Z}_n^*$.*

Доказательство. Следует из теоремы Лагранжа: порядок подгруппы P_n делит порядок группы $\mathbb{Z}_n^*$. □

Таким образом, вероятность того, что составное число n пройдет тест (2.4.1) для случайно выбранного a не превышает $1/2$. Мы можем рассмотреть следующий вероятностный метод проверки числа на простоту. Сначала выбираем случайное число a в интервале $1 < a < n$ и вычисляем $d := \text{НОД}\ (n, a)$ по алгоритму Евклида. Если $d > 1$, то n не является простым. В противном случае мы вычисляем $a^{n-1} \mod n$ и сравниваем результат с 1. Отметим, что вычисление a^{n-1} по модулю n существенно проще вычисления полного значения a^{n-1}. Если сравнение (2.4.1) не выполнено, то n не является простым. Если же n проходит тест (2.4.1), то мы повторяем процедуру с другим значением a. Вероятность того, что составное число n пройдет тест (2.4.1) k раз не превышает $1/2^k$ (если только n не является псевдопростым по любому основанию $a \in \mathbb{Z}_n^*$). В последнем случае наш вероятностный метод не может обнаружить, что n – составное (за исключением случая, когда для случайно выбранного a мы имеем НОД $(n, a) > 1$).

Определение 2.4.5 Если сравнение (2.4.1) выполнено для любого a такого, что НОД $(n, a) = 1$ и n – не простое, то n называется *числом Кармайкла*.

Наименьшим числом Кармайкла является $561 = 3 \cdot 11 \cdot 17$.

Проверка чисел на простоту методом Поклингтона

В отличие от изложенного выше вероятностного метода следующий метод проверки числа на простоту, предложенный Поклингтоном (H. Pocklington) дает, при выполнении некоторых условий, детерминированный ответ.

Теорема 2.4.6 *Предположим, что у* $n-1$ *имеется простой делитель* p_1*, больший* $\sqrt{n}-1$*. Предположим, также что существует* $a \in \mathbb{Z}$ *такое, что*

(i) $a^{n-1} \equiv 1 \mod n$,

(ii) НОД $(a^{(n-1)/p_1} - 1, n) = 1$.

Тогда n *– простое.*

Доказательство. Предположим, что n не является простым. Тогда у него существует простой делитель $p \leq \sqrt{n}$. Таким образом, $p - 1 < p_1$. Поэтому НОД $(p_1, p-1) = 1$ и тогда $p_1 u + (p-1)v = 1$ для некоторых $u, v \in \mathbb{Z}$. Из (i) получаем $a^{n-1} \equiv 1 \mod p$, а по малой теореме Ферма $a^{p-1} \equiv 1 \mod p$. Отсюда по модулю p имеем

$$a^{(n-1)/p_1} = a^{(p_1 u + (p-1)v)(n-1)/p_1} = a^{u(n-1)} a^{(p-1)v(n-1)/p_1} \equiv 1.$$

Это противоречит с условию (ii). □

Описанный выше критерий простоты очень хорошо работает для чисел n, у которых $n-1$ делится на простое число, большее $\sqrt{n}-1$. Более того, он дает ответ с вероятностью 100% при условии, что мы нашли число a, удовлетворяющее условию (ii) (условию (i) оно тогда должно удовлетворять, иначе n – не простое).

Пример 2.4.7 Пусть нам известно, что $p_1 = 5003$ – простое число. Докажем, что простым является также $n = 10007$. Так как $n - 1 = 2p_1$ и $p_1 > \sqrt{n} - 1$, то мы можем применить теорему 2.4.6. Возьмем $a = 2$. Ясно, что условие (ii) выполнено. Проверим (i). (Здесь все сравнения – по модулю n):

$$\begin{aligned} 2^{10006} = 4^{5003} = 4 \cdot 16^{2501} \equiv 64 \cdot 256^{1250} \equiv 64 \cdot 5494^{625} \equiv \\ \equiv 64 \cdot 5494 \cdot 2924^{312} \equiv 1371 \cdot 3798^{156} \equiv 1371 \cdot 4717^{78} \equiv \\ \equiv 1371 \cdot 4528^{39} \equiv 1371 \cdot 4528 \cdot 8448^{19} \equiv 3548 \cdot 8448 \cdot 8787^{9} \equiv \\ \equiv 2539 \cdot 8787 \cdot 7364^{4} \equiv 4590 \cdot 563^{2} \equiv 4590 \cdot 6752 \equiv 1 \end{aligned}$$

Следовательно, n – простое.

Другой важной проблемой криптографии является построение алгоритмов разложения целых чисел в произведение простых множителей. В этом параграфе мы обсудим один такой алгоритм.

$p-1$-метод Полларда разложения чисел на множители

Пусть дано натуральное число n.

Алгоритм 2.4.8 Во-первых, выбирается некоторое m, делящееся на почти все числа, меньшие некоторой константы Const (например, можно взять $m = \text{Const}!$).

Во-вторых, выбираем целое $2 \leq q \leq n-2$ и вычисляем $q^m \mod n$.

Далее, вычисляем $d := \text{НОД}\ (q^m - 1, n)$ (по алгоритму Евклида). При этом мы можем использовать лишь значение q^m по модулю n. Далее мы считаем, что $q^m \not\equiv 1 \mod n$.

Если $d \neq 1$, то мы можем продолжить алгоритм, применяя его к d и n/d. Однако может случиться, что $d = 1$. В этом случае мы должны повторить все наши вычисления с другими значениями m и q.

Таким образом, предложенный алгоритм не является однозначно определенным и даже вероятностным. Обсудим его сильные и слабые стороны.

Сильной стороной метода, конечно является его простота. Пусть p – неизвестный простой делитель n. Предположим, что в разложении $p - 1 = p_1^{l_1} \cdots p_r^{l_r}$ в произведение простых имеем $p_i^{l_i} \leq \text{Const}$ для всех i. Тогда m делится на $p-1$ и, согласно малой теореме Ферма, $q^m \equiv 1 \mod p$ (мы считаем, что q не делится на p). Но тогда p делит $d = \text{НОД}\ (q^m - 1, n)$ и поэтому $d \neq 1$.

Вывод 1 Метод хорошо работает, если для всех простых делителей p числа n все простые множители p_i в разложении $p-1$ малы: если $p-1$ не делится на $p_i^{l_i}$, то $p_i^{l_i} < \text{Const}$.

Конечно, мы можем увеличить константу Const, но при этом существенно увеличится и объем вычислений. Таким образом, метод плохо работает для чисел n с простыми делителями p такими, что $p-1$ делится на большое простое число (или большую степень простого числа).

Пример 2.4.9 Разложим на множители число $n = 2911$. Положим $\mathrm{Const} = 7$. Тогда можно взять $m = 420$. Возьмем также $q = 3$. Имеем $q^m \equiv 2131 \mod n$, НОД $(q^m - 1, n) = 71$. Получаем разложение $n = 71 \cdot 41$. Теперь ясно, что выбор константы Const был оправдан: $p - 1 = 70 = 2 \cdot 5 \cdot 7$ и $2, 5, 7 \leq \mathrm{Const} = 7$.

Метод был предложен Поллардом[1)] и носит также название $p-1$-метода.

Упражнения. **(1)** Докажите, что $561 = 3 \cdot 11 \cdot 17$ – число Кармайкла.

(2) Методом Поклинтона докажите, что $n = 907$ – простое число. *Указание.* Используйте то, что $n - 1$ имеет простой делитель 151.

(3) Методом Полларда разложите $n = 8897$ на множители. *Указание.* На первом шаге возьмите $\mathrm{Const} = 3$, $q = 2$, на втором – $\mathrm{Const} = 7$, $m = 420$, $q = 3$.

2.5. Автоморфизм Фробениуса. Совершенные поля

Лемма 2.5.1 *Пусть* $\Bbbk$ *– поле характеристики* $\mathrm{char}\,\Bbbk = p > 0$. *Тогда отображение*

$$F\colon \Bbbk \longrightarrow \Bbbk, \qquad F(\alpha) = \alpha^p$$

является изоморфизмом $\Bbbk$ *на некоторое подполе.*

Доказательство. Из соотношений

$$(\beta + \gamma)^p = \beta^p + \gamma^p, \qquad (\beta\gamma)^p = \beta^p\gamma^p.$$

[1)] Pollard J. M. Theorems of factorization and primality testing, Proc. Cambridge Phil. Soc. **76** (1974) 521–528

(см. доказательство леммы 2.3.3) следует, что F является гомоморфизмом колец, но так как $\Bbbk$ – поле, то $\operatorname{Ker} F = \{0\}$. $\square$

Замечание 2.5.2 Следует отметить, что отображение F необязательно сюръективно.

Определенное выше отображение F называется *отображением Фробениуса*. Неподвижными элементами F являются корни уравнения $x^p = x$, а это – в точности элементы простого подполя $\mathbb{F}_p \subset \Bbbk$.

Следствие 2.5.3 *Пусть $\Bbbk$ – поле характеристики $\operatorname{char}\Bbbk = p > 0$ и пусть $e \in \mathbb{N}$. Тогда множество*

$$\Bbbk^{p^e} := \{\alpha^{p^e} \mid \alpha \in \Bbbk\}$$

является подполем в $\Bbbk$ (изоморфным $\Bbbk$).

Доказательство. Очевидно, так как $\Bbbk^{p^e} = F^e(\Bbbk)$. $\square$

Определение 2.5.4 Поле $\Bbbk$ называется *совершенным* если $\operatorname{char}\Bbbk = 0$ или $\operatorname{char}\Bbbk = p > 0$ и $\Bbbk^p = \Bbbk$ (т.е. если отображение Фробениуса сюръективно).

В совершенном поле характеристики $p > 0$ отображение Фробениуса является *автоморфизмом*. Поле $\Bbbk$ характеристики $p > 0$ является совершенным тогда и только тогда, когда оно вместе с каждым своим элементом α содержит и корень p-й степени $\sqrt[p]{\alpha}$ из него. По лемме 2.5.1 этот корень должен быть единственным (т.е. он – кратный). Таким образом, в совершенном поле характеристики p уравнение $x^p - \alpha = 0$ имеет единственное решение. Ясно, что алгебраически замкнутое поле совершенно.

Предложение 2.5.5 *Любое конечное поле совершенно.*

Доказательство. Инъективное отображение $F\colon \mathbb{F}_q \to \mathbb{F}_q$ конечного множества в себя должно быть сюръективным. $\square$

Пример 2.5.6 Пусть $\Bbbk$ – любое поле характеристики $p > 0$ и пусть $\mathbb{K} = \Bbbk(t)$ – поле рациональных дробей над $\Bbbk$. Так как уравнение $x^p - t = 0$ не имеет корней в $\mathbb{K}$, то поле $\mathbb{K}$ не является совершенным.

Предложение 2.5.7 *Пусть $\Bbbk$ – совершенное поле и пусть $\mathbb{K}$ – его алгебраическое расширение. Тогда поле $\mathbb{K}$ также совершенно.*

Доказательство. Сначала предположим, что расширение $\mathbb{K}/\Bbbk$ конечно. Ясно, что мы можем считать, что $\operatorname{char}\Bbbk = p > 0$. Так как $\Bbbk^p = \Bbbk$, то мы имеем включения $\Bbbk \subset \mathbb{K}^p \subset \mathbb{K}$. Рассмотрим $\mathbb{K}$ и $\mathbb{K}^p$ как векторные пространства над $\Bbbk$. Пусть $\vartheta_1, \ldots, \vartheta_n$ – базис $\mathbb{K}$. Тогда элементы $\vartheta_1^p, \ldots, \vartheta_n^p$ – линейно независимы в $\mathbb{K}^p$ над $\Bbbk$. Действительно, предположим, что $\sum_i \lambda_i \vartheta_i^p = 0$ для $\lambda_i \in \Bbbk$. Тогда для некоторых $\beta_i \in \Bbbk$ имеем $\beta_i^p = \lambda_i$. Отсюда

$$0 = \sum_i \beta_i^p \vartheta_i^p = \Big(\sum_i \beta_i \vartheta_i\Big)^p, \qquad \sum_i \beta_i \vartheta_i = 0.$$

что дает нам $\beta_i = 0$ и $\lambda_i = 0$ для всех i. Поэтому $\dim \mathbb{K}^p \geq \dim \mathbb{K}$ и, следовательно, $\mathbb{K}^p = \mathbb{K}$.

Пусть теперь расширение $\mathbb{K}/\Bbbk$ не является конечным. Предположим, что уравнение $x^p - \vartheta = 0$ не имеет решений для некоторого $\vartheta \in \mathbb{K}$. Расширение $\mathbb{K}(\vartheta)/\Bbbk$ конечно и по доказанному выше $\sqrt[p]{\vartheta} \in \mathbb{K}(\vartheta)$. Противоречие. □

Сепарабельные расширения

Определение 2.5.8 Неприводимый многочлен $f(x) \in \Bbbk[x]$ называется *сепарабельным* над $\Bbbk$, если $f'(x) \neq 0$. Любой многочлен $f(x) \in \Bbbk[x]$ называется *сепарабельным*, если таковыми являются все его неприводимые множители. Пусть $\mathbb{K}/\Bbbk$ – расширение полей. Алгебраический элемент $\theta \in \mathbb{K}$ называется *сепарабельным* над $\Bbbk$, если таковым является его минимальный многочлен $\mu_\theta^{\Bbbk}(x)$. Расширение полей $\mathbb{K}/\Bbbk$ называется *сепарабельным*, если оно алгебраично и все элементы $\theta \in \mathbb{K}$ сепарабельны над $\Bbbk$.

Сепарабельные расширения интересны, поскольку они обладают следующим свойством:

Предложение 2.5.9 *Неприводимый многочлен $f(x) \in \Bbbk[x]$ сепарабелен, то он не имеет кратных корней в любом расширении $\mathbb{K} \supset \Bbbk$.*

Доказательство. Для того чтобы $f(x)$ обладал кратными корнями в $\mathbb{K} \supset \Bbbk$ необходимо, чтобы наибольший общий делитель НОД $(f(x), f'(x))$ многочленов $f(x)$ и $f'(x)$ был отличен от константы. С другой стороны, НОД $(f(x), f'(x))$ вычисляется при помощи алгоритма Евклида и поэтому НОД $(f(x), f'(x))$ – элемент $\Bbbk[x]$. Если многочлен $f(x)$ неприводим, то ни с каким многочленом меньшей степени: $f(x)$ не может иметь непостоянных общих множителей, следовательно, должно иметь место равенство $f'(x) = 0$. □

Следствие 2.5.10 *Пусть $\Bbbk \subset \Bbbk' \subset \mathbb{K}$ – расширения полей, причем расширение $\Bbbk \subset \Bbbk'$ конечно. Если элемент $\Theta \in \mathbb{K}$ сепарабелен над $\Bbbk$, то он сепарабелен над $\Bbbk'$.*

Доказательство. Так как $\mu_\theta^{\Bbbk}(\theta) = 0$, то $\mu_\theta^{\Bbbk'}(x)$ делит $\mu_\theta^{\Bbbk}(x)$. □

Предложение 2.5.11 *Над полем характеристики 0 любой многочлен является сепарабельным. Над полем $\Bbbk$ характеристики $p > 0$ неприводимый многочлен $f(x)$ не является сепарабельным тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого многочлена $g(y)$.*

Доказательство. Пусть $f(x) \in \Bbbk[x]$ – неприводимый несепарабельный многочлен. Тогда $f'(x) = 0$. Запишем

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \\ f'(x) &= a_1 + 2a_2 x + \cdots + n a_n x^{n-1}. \end{aligned}$$

Откуда получаем

$$a_1 = 2a_2 = \cdots = n a_n = 0.$$

В случае характеристики нуль отсюда следует, что $a_i = 0$ для всех $i = 1, \ldots, n$. Следовательно, непостоянный многочлен не может иметь кратных корней. В случае же характеристики $p > 0$ для $i = 1, \ldots, n$ мы имеем

$$a_i = 0 \quad \text{или} \quad i \equiv 0 \mod p.$$

Таким образом, чтобы многочлен $f(x)$ обладал кратными корнями, все его слагаемые должны обращаться в нуль, за исключением тех слагаемых, для которых $i \equiv 0 \mod p$, т. е, $f(x)$ должен иметь вид

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = g(x^p).$$

□

Пример 2.5.12 Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $\alpha \in \Bbbk$. Тогда любой неприводимый множитель $f(x)$ степени $l > 1$ многочлена $x^{p^e} - \alpha$ не является сепарабельным. Действительно, пусть $\mathbb{K} \supset \Bbbk$ – поле разложения для $x^{p^e} - \alpha$ и пусть $\beta \in \mathbb{K}$ – любой корень $x^{p^e} - \alpha$. Тогда $\beta^{p^e} = \alpha$ и поэтому $(x - \beta)^{p^e} = x^{p^e} - \alpha$. Таким образом, $f(x) = (x - \beta)^{p^l}$ не является сепарабельным по предложению 2.5.9.

Определение 2.5.13 Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $\mathbb{K}/\Bbbk$ – любое расширение. Элемент $\theta \in \mathbb{K}$ называется *чисто несепарабельным* над $\Bbbk$, если $\theta^{p^k} \in \Bbbk$ для некоторого k. Расширение $\mathbb{K}/\Bbbk$ называется *чисто несепарабельным* если все элементы $\theta \in \mathbb{K}$ чисто несепарабельны над $\Bbbk$.

Предложение 2.5.14 *Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $\mathbb{K}/\Bbbk$ – любое расширение. Элемент $\theta \in \mathbb{K}$ является одновременно сепарабельным и чисто несепарабельным тогда и только тогда, когда $\theta \in \Bbbk$.*

Доказательство. Действительно, θ является корнем многочлена $x^{p^e} - \alpha$ для некоторых $\alpha \in \Bbbk$ и $e \in \mathbb{N}$. Поэтому $\mu_\theta(x)$ делит $x^{p^e} - \alpha$. Согласно примеру 2.5.12 многочлен $\mu_\theta(x)$ должен быть линейным. □

Теорема 2.5.15 *Пусть* $\mathbb{K}/\Bbbk$ *– произвольное алгебраическое расширение и пусть* $\mathbb{K}_s \subset \mathbb{K}$ *– подмножество всех сепарабельных над* $\Bbbk$ *элементов. Тогда*

(i) $\mathbb{K}_s$ *– поле*;

(ii) *расширение* $\mathbb{K}/\mathbb{K}_s$ *чисто несепарабельно.*

Доказательство. Мы дожем утверждение только в случае, когда расширение $\mathbb{K}/\Bbbk$ конечно. Для рассмотрения общего случая нужны некоторые простые дополнительные соображения.

Шаг 1.

Для $e \in \mathbb{N}$ обозначим

$$\Bbbk\mathbb{K}^{p^e} := \Big\{ \sum_i \alpha_i \beta_i^{p^e} \mid \alpha_i \in \Bbbk, \quad \beta_i \in \mathbb{K} \Big\}.$$

Утверждается, что $\Bbbk\mathbb{K}^{p^e}$ – поле. Действительно, очевидно, что $\Bbbk\mathbb{K}^{p^e}$ является подкольцом в $\mathbb{K}$. Пусть $\delta \in \Bbbk\mathbb{K}^{p^e}$ – ненулевой элемент, не содержащийся в $\Bbbk$. Тогда его минимальный многочлен – неприводимый многочлен $\mu(x)$ степени > 1. В частности, $\mu(x)$ взаимно прост с x. По теореме о наибольшем общем делителе $1 = \mu(x)u(x) + xv(x)$ для некоторых многочленов $u(x), v(x) \in \Bbbk[x]$. Отсюда $1 = \mu(\delta)u(\delta) + \delta v(\delta) = \delta v(\delta)$ и, таким образом, $\delta^{-1} = v(\delta) \in \Bbbk\mathbb{K}^{p^e}$. Следовательно, $\Bbbk\mathbb{K}^{p^e}$ – поле.

Шаг 2.

Согласно шагу 1 существует цепочка вложенных полей

$$\Bbbk\mathbb{K} = \mathbb{K} \supset \Bbbk\mathbb{K}^{p} \supset \Bbbk\mathbb{K}^{p^2} \supset \cdots \supset \Bbbk\mathbb{K}^{p^l} \supset \cdots .$$

Рассматривая эти поля как векторные пространства над $\Bbbk$, мы видим, что цепочка стабилизируется: существует $e \in \mathbb{N}$ такое, что $\Bbbk\mathbb{K}^{p^e} = \Bbbk\mathbb{K}^{p^l}$ для всех $l \geq e$. Положим

$$\mathbb{L} := \bigcap_{l=0}^{\infty} \Bbbk\mathbb{K}^{p^l} = \bigcap_{l=0}^{e} \Bbbk\mathbb{K}^{p^l} = \Bbbk\mathbb{K}^{p^e}.$$

Ясно, что $\mathbb{L}$ – поле. Мы покажем, что $\mathbb{K}_s = \mathbb{L}$.

Шаг 3.

Возьмем любой элемент $\delta \in \mathbb{K}$. Тогда $\delta^{p^e} \in \mathbb{K}^{p^e} \subset \Bbbk\mathbb{K}^{p^e} = \mathbb{L}$. Поэтому $\mathbb{K}/\mathbb{L}$ – чисто несепарабельное расширение. Предположим, что δ сепарабелен над $\Bbbk$. По следствию 2.5.10 он сепарабелен над $\mathbb{L}$, а по предложению 2.5.14 δ содержится в $\mathbb{L}$. Таким образом, $\mathbb{L}$ содержит все сепарабельные над $\Bbbk$ элементов, т.е. $\mathbb{L} \supset \mathbb{K}_s$. Остается доказать, что все элементы $\mathbb{L}$ сепарабельны, т.е. $\mathbb{L} \subset \mathbb{K}_s$.

Шаг 4.

Мы утверждаем, что $\Bbbk\mathbb{L}^p = \mathbb{L}$. Действительно, включение $\Bbbk\mathbb{L}^p \subset \mathbb{L}$ очевидно. С другой стороны, пусть $\delta \in \mathbb{L}$. Тогда $\delta \in \Bbbk\mathbb{K}^{p^e}$ и поэтому δ представляется в виде

$$\delta = \sum_i \alpha_i \beta_i^{p^{e+1}} = \sum_i \alpha_i (\beta_i^{p^e})^p, \qquad \alpha_i \in \Bbbk, \quad \beta_i \in \mathbb{K}.$$

Здесь $\beta_i^{p^e} \in \Bbbk\mathbb{K}^{p^e} = \mathbb{L}$. Следовательно, $\delta \in \Bbbk\mathbb{L}^p$.

Шаг 5.

Для любых линейно независимых над $\Bbbk$ элементов $\omega_1, \ldots, \omega_r \in \mathbb{L}$ элементы $\omega_1^p, \ldots, \omega_r^p$ также линейно независимы над $\Bbbk$. Действительно, мы дополним $\omega_1, \ldots, \omega_r$ до базиса $\omega_1, \ldots, \omega_n$ пространства $\mathbb{L}$ над $\Bbbk$. Любой элемент $\beta \in \mathbb{L} = \Bbbk\mathbb{L}^p$ представляется в виде $\beta = \sum \alpha_i \beta_i^p$, где $\alpha_i \in \Bbbk$, $\beta_i \in \mathbb{L}$. Далее $\beta_i = \sum_j \gamma_{i,j}\omega_j$, где $\gamma_{i,j} \in \Bbbk$. Отсюда получаем

$$\beta = \sum_i \alpha_i \Big(\sum_j \gamma_{i,j}\omega_j\Big)^p = \sum_i \alpha_i \sum_j \gamma_{i,j}^p \omega_j^p = \sum_j \Big(\sum_i \alpha_i \gamma_{i,j}^p\Big)\omega_j^p$$

Следовательно, $\omega_1^p, \ldots, \omega_n^p$ – также базис $\mathbb{L}$ над $\Bbbk$.

Шаг 6.

Предположим, что элемент $\theta \in \mathbb{L}$ не является сепарабельным над $\Bbbk$. Тогда $\mu_\theta^{\Bbbk}(x) = g(x^p)$ для некоторого многочлена $g(y)$. Пусть $d := \deg g(y)$. Тогда $\deg \mu_\theta^{\Bbbk}(x) = pd > d$ и элементы

$1, \theta, \theta^2, \ldots, \theta^{d-1}$ линейно независимы над $\Bbbk$. Согласно предыдущему шагу элементы $1, \theta^p, \theta^{2p}, \ldots, \theta^{(d-1)p}$ также линейно независимы над $\Bbbk$. Это противоречит тому, что $\mu_\theta^{\Bbbk}(\theta) = 0$. Противоречие показывает, что $\mathbb{L} \subset \mathbb{K}_s$ и заканчивает доказательство теоремы. $\square$

Определение 2.5.16 Поле $\mathbb{K}_s$, построенное в теореме 2.5.15 называется сепарабельным замыканием поля $\Bbbk$ в $\mathbb{K}$.

Упражнения. **(1)** Пусть $q = p^k$ и $d \in \mathbb{N}$. Тогда $\mathbb{F}_q \subset \mathbb{F}_{q^d}$. Обозначим через $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ группу всех автоморфизмов поля $\mathbb{F}_{q^d}$, оставляющих неподвижными элементы $\mathbb{F}_q$. Докажите, что $F^k \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ и $(F^k)^d = 1$. Докажите, что $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ – циклическая группа порядка d, порожденная элементом F^k. *Указание.* Используйте то, что группа $\mathbb{F}_{q^d}^*$ – циклическая.

(2) Пусть $\mathbb{K}/\Bbbk$ – алгебраическое расширение полей. Докажите, что все чисто несепарабельные элементы $\mathbb{K}/\Bbbk$ образуют подполе. Образуют ли подполе все несепарабельные элементы?

(3) Пусть $\mathbb{K}/\Bbbk$ – расширение полей характеристики $p > 0$ и пусть $\vartheta \in \mathbb{K}$ алгебраический над $\Bbbk$ элемент. Докажите, что элемент ϑ^{p^e} сепарабелен над $\Bbbk$ для некоторого e.

(4) Докажите, что для чисто несепарабельного расширения $\mathbb{K}/\Bbbk$ не существует нетривиальных автоморфизмов поля $\mathbb{K}$, оставляющих неподвижными все элементы из $\Bbbk$ (ср. упражнение (5), стр. 21).

(5) Пусть $\Bbbk$ – поле характеристики p и пусть $f \in \Bbbk[x]$ – неприводимый многочлен. Докажите, что все корни f имеют одну и ту же кратность p^e для некоторого e.

(6) Если $\mathbb{K}$ – конечное чисто несепарабельное расширение поля $\Bbbk$, то степень $\mathbb{K}/\Bbbk$ является степенью числа p. Докажите.

(7) Докажите, что если $a \in \Bbbk$, $a \notin \Bbbk^p$, то многочлен $x^{p^e} - a$ неприводим в $\Bbbk[x]$ ($\mathrm{char}\,\Bbbk = p$).

(8) Докажите, что поле $\Bbbk$ характеристики $p > 0$ совершенно тогда и только тогда, когда каждый многочлен над $\Bbbk$ сепарабелен.

(9) Докажите, что следующие условия эквивалентны:

(i) ϑ сепарабелен над $\Bbbk$;

(ii) $\Bbbk(\vartheta) = \Bbbk(\vartheta^p)$;

(iii) $\Bbbk(\vartheta)$ – сепарабельное расширение поля $\Bbbk$.

2.6. Трансцендентные расширения полей

Базисы трансцендентности

Определение 2.6.1 Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Подмножество $M \subset \mathbb{K}$ называется *алгебраически независимым* над $\Bbbk$, если для любого многочлена $f(x_1, \ldots, x_m) \in \Bbbk[x_1, \ldots, x_m]$ из соотношения

$$f(\alpha_1, \ldots, \alpha_m) = 0, \qquad \alpha_i \in M, \quad \alpha_i \neq \alpha_j$$

следует, что $f(x_1, \ldots, x_m) = 0$. Подмножество $M \subset \mathbb{K}$ называется *базисом трансцендентности*, если

(i) M алгебраически независимо и

(ii) любое алгебраически независимое подмножество $M' \subset \mathbb{K}$, содержащее M, совпадает с M.

Замечание 2.6.2 Алгебраически независимое подмножество M является базисом трансцендентности $\mathbb{K}$ над $\Bbbk$ тогда и только тогда, когда поле $\mathbb{K}$ алгебраично над $\Bbbk(M)$.

Пример 2.6.3 Множество из одного элемента α алгебраически независимо тогда и только тогда, когда α трансцендентен (неалгебраичен) над $\Bbbk$.

Пример 2.6.4 Пусть $\mathbb{K} = \Bbbk(x_1, \ldots, x_n)$ – поле рациональных дробей от n переменных. Тогда элементы $x_1, \ldots, x_n$ алгебраически независимы над $\Bbbk$ и образуют базис. Верно и обратное: если $\mathbb{K} = \Bbbk(\vartheta_1, \ldots, \vartheta_n)$, где элементы $\vartheta_1, \ldots, \vartheta_n$ образуют базис трансцендентности, то $\mathbb{K}$ изоморфно полю рациональных дробей от n переменных. Такие расширения называются *чисто трансцендентными*.

Определение 2.6.5 Предположим, что расширение $\mathbb{K}/\Bbbk$ конечно порождено. Если M – алгебраически независимое подмножество в $\mathbb{K}$ и если мощность M является наибольшей среди

мощностей всех таких подмножеств, то мы будем называть эту мощность *степенью трансцендентности* расширения $\mathbb{K}$ над $\Bbbk$ и обозначать $\mathrm{degtr}_{\Bbbk}\,\mathbb{K}$ или просто $\mathrm{degtr}\,\mathbb{K}$, если это не приводит к путанице.

Лемма 2.6.6 *Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Если множество M порождает $\mathbb{K}$ над $\Bbbk$ (т. е. $\mathbb{K} = \Bbbk(M)$) и S – подмножество в M, алгебраически независимое над $\Bbbk$, то существует базис трансцендентности E поля $\mathbb{K}$ над $\Bbbk$ такой, что $S \subset E \subset M$.*

Доказательство. Мы рассмотрим только случай, когда множество M конечно. Пусть $M = \{\alpha_1, \ldots, \alpha_n\}$. После подходящей перенумерации мы можем считать, что $S = \{\alpha_1, \ldots, \alpha_r\}$, где элементы $\alpha_1, \ldots, \alpha_r$ алгебраически независимы, а каждая система $\alpha_1, \ldots, \alpha_r, \alpha_j$ для $j = r+1, \ldots, n$ алгебраически зависима. Тогда элементы $\alpha_{r+1}, \ldots, \alpha_n$ алгебраичны над $\Bbbk(\alpha_1, \ldots, \alpha_r)$, а поэтому алгебраично и расширение $\mathbb{K}/\Bbbk$. Это означает, что $\alpha_1, \ldots, \alpha_r$ – базис трансцендентности. □

Следствие 2.6.7 *Если поле $\mathbb{K}$ конечно порождено над $\Bbbk$, то в $\mathbb{K}$ существует базис трансцендентности из конечного числа элементов.*

Заметим, что понятия степени трансцендентности и алгебраической независимости очень похожи на понятия размерности и линейной независимости в линейной алгебре. Однако следует сказать, что пользоваться этой аналогией следует очень осторожно. Например, различные базисы трансцендентности в одном расширении не могут быть алгебраически выражены друг через друга.

Теорема 2.6.8 *Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Любые два базиса трансцендентности $\mathbb{K}$ над $\Bbbk$ имеют одинаковую мощность.*

Доказательство. Мы докажем утверждение только в случае, когда $\mathbb{K}$ конечно порождено над $\Bbbk$. Тогда существует по крайней мере один конечный базис трансцендентности, скажем

$\alpha_1, \ldots, \alpha_n$. По лемме 2.6.9 (ниже) любой другой базис трансцендентности также должен содержать n элементов. Это доказывает теорему. $\square$

Лемма 2.6.9 (об алгебраической зависимости) *Пусть* $\mathbb{K}$ *– расширение поля* $\Bbbk$ *и пусть* $\alpha_1, \ldots, \alpha_n$ *– базис трансцендентности для* $\mathbb{K}/\Bbbk$. *Если* $\beta_1, \ldots, \beta_m$ *– элементы из* $\mathbb{K}$, *алгебраически независимые над* $\Bbbk$, *то* $m \leq n$.

Доказательство. Мы можем считать, что $\alpha_1, \ldots, \alpha_n$ – базис трансцендентности из минимального числа элементов. По предположению существует ненулевой многочлен $f(x_1, \ldots, x_{n+1})$ с коэффициентами в $\Bbbk$, такой, что $f(\alpha_1, \ldots, \alpha_n, \beta_1) = 0$. Кроме того, по предположению x_{n+1} встречается в f и некоторое x_i, $1 \leq i \leq n$, скажем x_1, также встречается в f. Тогда элемент α_1 алгебраичен над $\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$, а, следовательно, над $\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$ алгебраичен и любой элемент из $\mathbb{K}$. По лемме 2.6.6 можно выбрать базис трансцендентности, содержащий элементы $\beta_1, \alpha_2, \ldots, \alpha_n$, а по нашему предположению этот базис совпадает с $\beta_1, \alpha_2, \ldots, \alpha_n$. Заменяя α_1 на β_1, мы можем считать, что $\beta_1 = \alpha_1$.

Далее по индукции мы сведем утверждение к случаю $\beta_1 = \alpha_1, \ldots, \beta_n = \alpha_n$. Действительно, пусть $\beta_1 = \alpha_1, \ldots, \beta_r = \alpha_r$ для некоторого $1 \leq r \leq n$. Как и выше, существует ненулевой многочлен $g(x_1, \ldots, x_{n+1})$ с коэффициентами в $\Bbbk$, для которого $g(\beta_{r+1}, \alpha_1, \ldots, \alpha_n) = 0$, причем β_{r+1} действительно встречается в g. Так как все β_i алгебраически независимы над $\Bbbk$, то некоторый элемент α_j $(j = r+1, \ldots, n)$ также встречается в g. После перенумерации мы можем считать, что $j = r+1$. Тогда α_{r+1} алгебраичен над

$$\Bbbk(\beta_{r+1}, \alpha_1, \ldots, \widehat{\alpha_{r+1}}, \ldots, \alpha_n).$$

Следовательно, над этим полем алгебраичен и любой элемент из $\mathbb{K}$. По нашему предположению $\beta_{r+1}, \alpha_1, \ldots, \widehat{\alpha_{r+1}}, \ldots, \alpha_n$ – базис трансцендентности. Заменяя α_{r+1} на β_{r+1}, мы можем считать, что $\beta_{r+1} = \alpha_{r+1}$. Таким образом, мы можем считать, что

$\beta_1 = \alpha_1, \ldots, \beta_n = \alpha_n$. Если $m > n$, то элемент β_{n+1} должен быть алгебраическим над $\Bbbk(\alpha_1, \ldots, \alpha_n) = \Bbbk(\beta_1, \ldots, \beta_n)$, что невозможно. $\square$

Мы, таким образом, доказали следующее: либо степень трансцендентности конечна и равна мощности любого другого базиса трансцендентности, либо она бесконечна, и тогда всякий базис трансцендентности бесконечен.

Упражнения. **(1)** Докажите, что мультипликативная группа поля $\Bbbk$ конечно порождена тогда и только тогда, когда $\Bbbk$ конечно. *Указание.* Если $\operatorname{char}\Bbbk = 0$, то $\Bbbk^* \supset \mathbb{Q}^*$. Если же $\operatorname{char}\Bbbk = p > 0$, то или $\Bbbk$ является чисто трансцендентным расширением некоторого поля $\Bbbk_0$ или для любого r поле $\Bbbk$ содержит конечное подполе из $p^l > r$ элементов.

(2) Докажите, что поле действительных чисел $\mathbb{R}$ имеет бесконечную степень трансцендентности над $\mathbb{Q}$.

(3) Пусть $\mathbb{K} = \Bbbk(t)/\Bbbk$ – чисто трансцендентное расширение степени трансцендентности 1. Докажите, что дробно-линейное отображение $\Bbbk(t) \to \Bbbk(t)$, заданное формулой $t \longmapsto (at+b)/(ct+d)$, $\quad a, b, c, d \in \Bbbk$, является автоморфизмом тогда и только тогда, когда $ad - bc \neq 0$.

(4) Пусть $\mathbb{K}/\Bbbk$ – расширение полей такое, что *каждый* элемент $\mathbb{K}$ трансцендентен над $\Bbbk$. Верно ли, что расширение чисто трансцендентно?

(5) Пусть $\mathbb{K}/\Bbbk$ – конечно порожденное расширение полей. Докажите, что любое промежуточное подполе $\mathbb{L}$ конечно порождено над $\Bbbk$.

Глава 3.

Алгебраические многообразия

Цель этой главы – дать *очень краткое* ведение в алгебраическую геометрию. Мы определим основные объекты изучения – алгебраические многообразия, а также рассмотрим некоторые важные, связанные с ними понятия, такие, как размерность, неособость, регулярные и рациональные функции. Следует отметить, что наше изложение часто является упрощенным: некоторые доказательства опускаются или приводятся лишь в частных случаях. За более подробными изложениями введения в предмет мы отсылаем читателя к книгам [Шаф88], [Рид91].

Всюду на протяжении этой главы, если не оговаривается противное, основное поле $\Bbbk$ предполагается алгебраически замкнутым произвольной характеристики.

3.1. Аффинные алгебраические многообразия

Определение алгебраических многообразий

Пусть $\Bbbk$ – фиксированное алгебраически замкнутое поле. Определим n-мерное аффинное пространство над $\Bbbk$, которое будем обозначать через $\mathbb{A}^m$, как множество всех наборов из n элементов поля $\Bbbk$. Упорядоченный набор $P = (a_1, \ldots, a_n)$, $a_i \in \Bbbk$, будем называть точкой P пространства $\mathbb{A}^m$, а его компоненты a_i – координатами точки P.

Элементы кольца многочленов $\Bbbk[x_1, \ldots, x_n]$ будем интерпретировать как функции на n-мерном аффинном пространстве со значениями в $\Bbbk$, полагая $f(P) = f(a_1 \ldots, a_n)$, где $f \in \Bbbk[x_1, \ldots, x_n]$ и $P \in \mathbb{A}^n$. Имеет смысл, следовательно, говорить о *множестве нулей* $Z(f) = \{P \in \mathbb{A}^n \mid f(P) = 0\}$ любого многочлена $f \in \Bbbk[x_1, \ldots, x_n]$. Более общим образом можно говорить

о множестве нулей

$$Z(T) = \{P \in \mathbb{A}^n \mid f(P) = 0, \quad \forall\, f \in T\}$$

произвольного подмножества T многочленов из $\Bbbk[x_1, \ldots, x_n]$. Если $\mathfrak{a}$ – идеал в $\Bbbk[x_1, \ldots, x_n]$, порожденный подмножеством T, то, очевидно, $Z(T) = Z(\mathfrak{a})$.

Определение 3.1.1 Подмножество X в $\mathbb{A}^n$ называется (*аффинным*) *алгебраическим множеством*, если существует такое подмножество $T \subset \Bbbk[x_1, \ldots, x_n]$, что $X = Z(T)$. Непустое алгебраическое множество называется также *аффинным алгебраическим многообразием* или просто *аффинным многообразием*.

Отметим, что каждое подмножество $T \subset \Bbbk[x_1, \ldots, x_n]$ однозначно определяет подмножество $Z(T)$. Однако, T не может быть однозначно восстановлено по $Z(T)$. Например, многочлены f и f^k определяют одно и то же подмножество: $Z(f) = Z(f^k)$.

Определение 3.1.2 Для любого алгебраического множества $X \subset \mathbb{A}^m$ определим *его идеал* $\mathfrak{I}(X)$ в $\Bbbk[x_1, \ldots, x_n]$, полагая

$$\mathfrak{I}(X) = \{f \in \Bbbk[x_1, \ldots, x_n] \mid f(P) = 0, \quad \forall P \in X\}. \qquad (3.1.3)$$

Будем говорить, что алгебраическое многообразие $X \subset \mathbb{A}^m$ является *гиперповерхностью* заданной многочленом f, если f порождает идеал $\mathfrak{I}(X)$, т.е. $\mathfrak{I}(X) = (f)$.

Предложение 3.1.4 *Пересечение любого семейства алгебраических множеств также будет алгебраическим множеством. Объединение двух (и любого конечного числа) алгебраических множеств является алгебраическим множеством. Пустое множество и все пространство являются алгебраическими множествами.*

Доказательство. Пусть $X_\alpha = Z(T_\alpha)$ – произвольное семейство алгебраических множеств, тогда $\cap X_\alpha = Z(\cup T_\alpha)$. Если $X_1 = Z(T_1)$ и $X_2 = Z(T_2)$, то $X_1 \cup X_2 = Z(T_1 T_2)$, где $T_1 T_2$

обозначает множество всех попарных произведений элементов из T_1 на элементы из T_2. Наконец, пустое множество представляется в виде $\varnothing = Z(1)$, а все пространство – в виде $\mathbb{A}^n = Z(0)$. $\square$

Топология Зарисского

Напомним, что *топологическим пространством* называется непустое множество X, на котором определена система подмножеств $\mathscr{T}$ таких, что

(i) пустое множество и все пространство X содержатся в $\mathscr{T}$;

(ii) пересечение любых двух (а, значит, и любого конечного числа) множеств из $\mathscr{T}$ принадлежит $\mathscr{T}$;

(iii) объединение любого (необязательно конечного) числа множеств из $\mathscr{T}$ принадлежит $\mathscr{T}$.

Подмножества из $\mathscr{T}$ называются *открытыми*. Дополнения к открытым множествам называются *замкнутыми* подмножествами. На самом деле, правильнее говорить, что топологическое пространство – это пара $(X, \mathscr{T})$, удовлетворяющая условиям выше, поскольку на данном множестве X можно задать различные системы подмножеств $\mathscr{T}$. Если $Y \subset X$ – непустое подмножество, то Y также имеет естественную структуру топологического пространства: положим $\mathscr{T}_Y := \{U \cap Y \mid U \in \mathscr{T}\}$.

Топологическое пространство X называется *хаусдорфовым* (или *отделимым*), если оно дополнительно удовлетворяет следующей *аксиоме отделимости*:

(iv) для любых различных точек $P, Q \in X$ существуют открытые множества U_P, U_Q такие, что $P \in U_P$, $Q \in U_Q$ и $U_P \cap U_Q = \varnothing$.

Пример 3.1.5 Пусть $X = \mathbb{R}^n$ – евклидово пространство. Определим систему открытых множеств следующим образом: $U \in \mathscr{T}$ тогда и только тогда, когда вместе с каждой точкой $P \in U$ множество U содержит и достаточно малый шар $\text{Ш}_{P,\epsilon}$ с центром в P. Очевидно, что такая топология хаусдорфова, она часто называется *классической* топологией.

Определение 3.1.6 Зададим на $\mathbb{A}^n$ *топологию Зарисского*, выбрав в качестве замкнутых множеств алгебраические подмножества, а в качестве открытых – дополнения к замкнутым. Это действительно топология, согласно предложению 3.1.4.

Задание топологии на алгебраических многообразиях позволяет определить и непрерывные отображения между ними: говорят, что отображение $f\colon X \to Y$ непрерывно, если прообраз открытого множества открыт. В случае $\Bbbk = \mathbb{C}$ на пространстве $\mathbb{A}^n$ имеется также классическая топология, которая *сильнее* топологии Зарисского. Это означает, что открытое в топологии Зарисского множество является также открытым и в классической топологии.

Топология Зарисского нехаусдорфова: любые два открытые подмножества пересекаются (докажите!). Поэтому некоторые традиционные понятия теряют в ней смысл. Например, предел последовательности точек не является единственным.

Пример 3.1.7 Выясним, как устроены алгебраические множества на аффинной прямой $\mathbb{A}^1$. Каждый идеал в кольце $\Bbbk[x]$ является главным, поэтому каждое алгебраическое множество – это множество нулей одного многочлена. Так как поле $\Bbbk$ алгебраически замкнуто, то всякий ненулевой многочлен может быть записан в виде $f(x) = c(x-a_1)^{k_1}(x_2-a_2)^{k_2}\cdots(x_m-a_m)^{k_m}$, где $c, a_1, \ldots, a_m \in \Bbbk$. В таком случае $Z(f) = \{a_1, \ldots, a_m\}$. Таким. образом, алгебраические множества в $\mathbb{A}^1$ – это пустое множество, всевозможные конечные подмножества и вся прямая.

Неприводимые аффинные многообразия

Определение 3.1.8 Аффинное алгебраическое многообразие $X \subset \mathbb{A}^n$ называется *неприводимым*, если его нельзя представить в виде объединения $X = X_1 \cup X_2$ двух собственных алгебраических подмножеств X_1 и X_2.

Отметим, что в некоторых курсах аффинное многообразие автоматически предполагается неприводимым.

Пример 3.1.9 (i) Аффинная прямая $\mathbb{A}^1$ неприводима, потому что ее собственные алгебраические подмножества конечны, а

$\mathbb{A}^1$ – бесконечное множество (поскольку поле $\Bbbk$ алгебраически замкнуто и, следовательно, бесконечно).

(ii) Любое аффинное многообразие $X \subset \mathbb{A}^n$ содержит неприводимое подмногообразие – точку.

Предложение 3.1.10 *Аффинное многообразие $X \subset \mathbb{A}^m$ неприводимо тогда и только тогда, когда его идеал $\mathfrak{I}(X)$ прост.*

Доказательство. Пусть X неприводимо. Предположим, что $fg \in \mathfrak{I}(X)$, но $f, g \notin \mathfrak{I}(X)$. Тогда $X = Z(\mathfrak{I}(X), f) \cup Z(\mathfrak{I}(X), g)$. Если, например, $X = Z(\mathfrak{I}(X), f)$, то из определения (3.1.3) имеем $f \in \mathfrak{I}(X)$. Противоречие.

Обратно, пусть идеал $\mathfrak{I}(X)$ прост. Предположим, что $X = X_1 \cup X_2$, где X_i – алгебраические подмножества и $X_i \neq X$. Существуют многочлены $f_i \in \mathfrak{I}(X_i)$ такие, что $f_i \notin \mathfrak{I}(X)$. Но тогда $f_1 f_2 \in \mathfrak{I}(X)$. Из простоты идеала $\mathfrak{I}(X)$ получаем, что f_1 или f_2 содержится в $\mathfrak{I}(X)$. Противоречие. □

Следствие 3.1.11 *Гиперповерхность $X \subset \mathbb{A}^m$, заданная многочленом f, неприводима тогда и только тогда, когда многочлен f неприводим.*

Теорема 3.1.12 *Рассмотрим два многочлена $f, g \in \Bbbk[x, y]$. Если f неприводим, а система уравнений*

$$f(x, y) = g(x, y) = 0$$

имеет бесконечное множество решений, то f делит g.

В этой теореме мы можем считать, что $\Bbbk$ – произвольное поле.

Доказательство. Мы можем считать, что f зависит от y. Рассмотрим f и g как многочлены над полем рациональных функций $\Bbbk(x)$. Тогда f неприводим как элемент кольца $\Bbbk(x)[y]$. Действительно, предположим, что существует нетривиальное разложение $f = f_1 f_2$, где f_1, $f_2 \in \Bbbk(x)[y]$. Пусть $a(x)$ – общее кратное знаменателей коэффициентов f_1 и f_2. Имеем $a(x)^2 f(x, y) = \bar{f}_1(x, y)\bar{f}_2(x, y)$, где $\bar{f}_i(x, y) = a(x) f_i(x, y)$ – многочлены из $\Bbbk[x, y]$.

Так как $\Bbbk[x,y]$ – кольцо с однозначным разложением на множители, то или $\bar{f}_1$, или $\bar{f}_2$ делится на f. Пусть, например, $\bar{f}_1 = fh$, $h \in \Bbbk[x,y]$. Тогда $a(x)^2 = h(x,y)\bar{f}_2(x,y)$. Отсюда f_2 зависит только от x, что противоречит нашему выбору f_1 и f_2.

Таким образом, f неприводим как элемент кольца $\Bbbk(x)[y]$. Предположим, что f не делит g. Легко видеть, что тогда f также не делит g в кольце $\Bbbk(x)[y]$. Поэтому многочлены f и g взаимно просты в $\Bbbk(x)[y]$. Существуют u, $v \in \Bbbk(x)[y]$ такие, что $fu + gv = 1$. Как и выше умножим это равенство на общее кратное $b(x)$ знаменателей коэффициентов u и v. Получим $f(x,y)\bar{u}(x,y) + g(x,y)\bar{v}(x,y) = b(x)$, где $\bar{u} = ub$, $\bar{v} = vb$. Пусть теперь (x_n, y_n) – бесконечная последовательность решений системы $f = g = 0$. Тогда x_n – последовательность решений уравнения $b(x) = 0$, которое имеет лишь конечное множество решений. Переходя к подпоследовательности, мы можем считать, что последовательность x_n постоянна: $x_n = x_0$. Теперь видно, что все y_n являются корнями уравнения $f(x_0, y) = 0$. Так как $f(x,y)$ не делится на $x - x_0$, то многочлен $f(x_0, y)$ отличен от нуля и поэтому для его корней y_n имеется лишь конечное множество значений. Противоречие. □

Теорема 3.1.13 *Пусть $\mathfrak{p} \subset \Bbbk[x,y]$ – простой идеал. Имеет место одно из следующих:*

(i) $\mathfrak{p} = (0)$;

(ii) $\mathfrak{p} = (f)$, *где $f = f(x,y)$ – неприводимый многочлен;*

(iii) $\mathfrak{p} = (x - a, y - b)$ *для некоторых $a, b \in \Bbbk$.*

Доказательство. Предположим, что идеал $\mathfrak{p}$ не является главным. Существуют непропорциональные неприводимые многочлены f, $g \in \Bbbk[x,y]$. Как и в доказательстве предыдущей теоремы, рассмотрим их как многочлены из $\Bbbk(x)[y]$. Тогда f и g снова неприводимы. Следовательно они взаимно просты в $\Bbbk(x)[y]$ и поэтому существуют элементы $u, v \in \Bbbk(x)[y]$ такие, что $fu + gv = 1$. Домножая на знаменатели получим $f\bar{u} + g\bar{v} = w$, где $\bar{u}, \bar{v} \in \Bbbk[x,y]$ и $w = \in \bar{\Bbbk}[x]$. Таким образом, $w = w(x) \in \mathfrak{p}$. Поскольку наше поле алгебраически замкнуто, то $w = c(x - a_1) \cdots (x - a_m)$.

Из простоты идеала $\mathfrak{p}$ получаем, что $x - a \in \mathfrak{p}$ для некоторого $a = a_i$. Аналогично, рассуждая в кольце $\Bbbk(y)[x]$ получим, что $y - b \in \mathfrak{p}$ для некоторого $b \in \Bbbk$. $\square$

Следствие 3.1.14 *Пусть $X \subset \mathbb{A}^2$ – неприводимое аффинное многообразие отличное от точки и всей плоскости $\mathbb{A}^2$. Тогда X – гиперповерхность, т.е. $\mathfrak{I}(X) = (f)$, где $f \in \Bbbk[x, y]$ – неприводимый многочлен.*

Теорема 3.1.15 *Пусть $X \subset \mathbb{A}^2$ – аффинное многообразие. Тогда существует разложение*

$$X = X_1 \cup \cdots \cup X_m \tag{3.1.16}$$

в объединение конечного числа различных, не содержащихся друг в друге неприводимых аффинных многообразий. Это разложение единственно с точностью до порядка.

Доказательство. Мы можем считать, что X состоит из бесконечного числа точек и $X \neq \mathbb{A}^2$. Пусть $h \in \Bbbk[x, y]$ – любой ненулевой многочлен, обращающийся в нуль на X. Разложим его на множители: $h = h_1^{k_1} \cdots h_s^{k_s}$. Тогда $X = \cup(X \cap Z(h_i))$. Пусть $X \cap Z(h_i)$ является бесконечным множеством при $i = 1, \ldots, r$ и конечным при $i = r + 1, \ldots, s$. Для каждого $i = 1, \ldots, r$ по теореме 3.1.12 имеем $Z(h_i) \subset X$. Таким образом,

$$X = \left(\bigcup_{i=1}^{r} Z(h_i) \right) \cup \left(\bigcup_{i=r+1}^{s} (X \cap Z(h_i)) \right),$$

где второй член – конечное множество точек. Это доказывает существование (3.1.16).

Далее, если существует два разложения

$$X = X_1 \cup \cdots \cup X_m = X_1' \cup \cdots \cup X_l',$$

то $X_i' \subset X_1 \cup \cdots \cup X_m$. Поэтому $X_i' = (X_1 \cap X_i') \cup \cdots \cup (X_m \cap X_i')$, где $X_i \cap X_i'$ – алгебраические множества. Отсюда $X_i' = X_j \cap X_i'$ для некоторого j и $X_i' \subset X_j$. Аналогично имеются обратные включения $X_i' \supset X_j$. $\square$

Компоненты X_i разложения (3.1.16) называются *неприводимыми компонентами* многообразия X, а само это разложение называется *разложением на неприводимые компоненты*.

Упражнения. **(1)** Докажите, что $\mathbb{A}^n$ – неприводимое многообразие.

(2) Пусть $X \subset \mathbb{A}^n$ – гиперповерхность, заданная многочленом f. Докажите, что f не имеет кратных множителей.

(3) Покажите на примерах, что следствие 3.1.14 перестает быть верным в аффинных пространствах размерности > 2.

(4) Докажите, что в топологии Зарисского любое аффинное многообразие *компактно* (т.е. из любого открытого покрытия можно выбрать конечное подпокрытие).

(5) Докажите, что любое непустое открытое подмножество аффинного многообразия всюду плотно.

3.2. Регулярные и рациональные функции. Размерность

Определение 3.2.1 Пусть $X \subset \mathbb{A}^n$ – аффинное многообразие и $\mathfrak{I}(X)$ – соответствующий ему идеал. Факторкольцо $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/\mathfrak{I}(X)$ будем называть *кольцом регулярных функций* многообразия X.

Ясно, что $\Bbbk[X]$ является конечно порожденной алгеброй над $\Bbbk$. Элементы $\Bbbk[X]$ могут рассматриваться как *алгебраические* (или *регулярные*) функции на X.

В случае, когда X – неприводимое аффинное многообразие, из предложения 3.1.10 следует, что кольцо $\Bbbk[X]$ не имеет делителей нуля. Поэтому существует его поле частных, которое мы обозначим через $\Bbbk(X)$ и будем называть *полем рациональных функций* многообразия X. Таким образом, для каждого элемента $f \in \Bbbk(X)$ имеет место представление $f = g/h$, где $g, h \in \Bbbk[X]$ и $g \neq 0$. Элементы $\Bbbk(X)$ называются *рациональными функциями на* X. Функция $f \in \Bbbk(X)$ называется *регулярной* в точке $P \in X$, если существует представление $f = g/h$ такое, что $g(P) \neq 0$. Множество

$$\mathscr{O}_{P,X} = \{f \in \Bbbk(X) \mid f \text{ регулярна в } P\}$$

называется *локальным кольцом* точки.

Рассмотрим пример.

Пример 3.2.2 Пусть $X = \mathbb{A}^n$. Тогда $\mathfrak{I}(X) = (0)$, $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]$, а поле $\Bbbk(X)$ является полем рациональных дробей от n переменных. Для точки $P \in X$ ее локальное кольцо $\mathscr{O}_{P,X}$ состоит из дробей $g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$ таких, что $g(P) \neq 0$.

Определение 3.2.3 Пусть $X \subset \mathbb{A}^n$ – неприводимое аффинное многообразие. Его *размерностью* $\dim X$ называется степень трансцендентности поля рациональных функций над $\Bbbk$:

$$\dim X := \operatorname{degtr}_{\Bbbk} \Bbbk(X).$$

Говорят, что необязательно неприводимое) аффинное многообразие имеет *чистую размерность* d, если размерности всех его неприводимых компонент равны d.

Пример 3.2.4 Пусть $X = (a_1, \ldots, a_n) \in \mathbb{A}^n$ – точка. Легко видеть, что $\mathfrak{I}(X) = (x_1 - a_1, \ldots, x_n - a_n)$. Поэтому $\Bbbk[X] = \Bbbk(X) = \Bbbk$ и $\dim X = 0$. Если же $X = \mathbb{A}^n$, то $\Bbbk(X) = \Bbbk(x_1, \ldots, x_n)$ и поэтому $\dim X = n$.

Пример 3.2.5 Из следствия 3.1.14 (ниже) вытекает, что $\dim \mathbb{A}^2 = 2$, а одномерные неприводимые подмногообразия в $\mathbb{A}^2$ – подмножества, заданные одним неприводимым многочленом. Они называются *плоскими кривыми*. В общем случае *кривой* называется алгебраическое многообразие чистой размерности 1.

Предложение 3.2.6 *Если $X \subset Y$ – вложенные неприводимые аффинные многообразия, то*

$$\dim X \leq \dim Y.$$

Если, кроме того, $\dim X = \dim Y$, *то* $X = Y$.

Доказательство. Пусть $X \subset Y \subset \mathbb{A}^n$. Так как $\mathfrak{I}(X) \supset \mathfrak{I}(Y)$, то по теореме о гомоморфизме колец имеются канонические сюръективные отображения

$$\Bbbk[X] \xleftarrow{\phi} \Bbbk[Y] \longleftarrow \Bbbk[x_1, \ldots, x_n].$$

Координаты x_i мы будем отождествлять с образами при этих отображениях, т.е. рассматривать их как порождающие элементы колец $\Bbbk[x_1, \ldots, x_n]$, $\Bbbk[X]$ и $\Bbbk[Y]$. Пусть $\operatorname{degtr} \Bbbk(Y) = d$. Тогда среди координат $x_1, \ldots, x_n$ любые $d+1$ алгебраически зависимы как элементы $\Bbbk(Y)$, т. е. связаны соотношением $f(x_{i_1}, \ldots, x_{i_{d+1}}) = 0$ на Y. Тем более оно выполняется на X. Это и значит, что степень трансцендентности поля $\Bbbk(X)$ не больше d.

Пусть теперь $\operatorname{degtr} \Bbbk(X) = \operatorname{degtr} \Bbbk(Y) = d$. Для доказательства совпадения X и Y достаточно показать, что гомоморфизм ϕ имеет тривиальное ядро. Предположим противное. Возьмем любой элемент $g \in \operatorname{Ker} \phi$, $g \neq 0$ на Y. Некоторые d из координат $x_1, \ldots, x_n$ независимы на X (т.е. в $\Bbbk[X]$). Пусть это $x_1, \ldots, x_d$. Тем более они независимы на Y. Тогда g алгебраически зависим от $x_1, \ldots, x_d$ на Y, т. е. выполнено соотношение

$$a_m(x_1, \ldots, x_d) g^m + \cdots + a_1(x_1, \ldots, x_d) g + a_0(x_1, \ldots, x_d) = 0 \tag{3.2.7}$$

на Y.

Мы можем выбрать многочлен в левой части неприводимым, и тогда $a_0(x_1, \ldots, x_d) \neq 0$ на Y. Тем более соотношение (3.2.7) верно на X. По нашему условию $g = 0$ на X. Тогда из (3.2.7) следует, что $a_0(x_1, \ldots, x_d) = 0$ на X, а так как $x_1, \ldots, x_d$ по условию независимы на X, то $a_0(x_1, \ldots, x_d) = 0$ на всем $\mathbb{A}^n$. Это противоречит тому, что $a_0(x_1, \ldots, x_d) \neq 0$ на Y. Таким образом, если $g = 0$ на X, то $g = 0$ на Y, а это и значит, что $X = Y$. Предложение доказано. □

Следствие 3.2.8 *Пусть X – неприводимое аффинное многообразие. Предположим, что существует цепочка*

$$X = X_d \supsetneq X_{d-1} \supsetneq \cdots \supsetneq X_0 \neq \varnothing, \tag{3.2.9}$$

где все X_i – различные неприводимые аффинные многообразия. Тогда $\dim X \geq d$.

Следствие 3.2.10 *Пусть $X \subset \mathbb{A}^n$ – неприводимое аффинное многообразие. Тогда* $\dim X \leq n$ *и равенство достигается только если $X = \mathbb{A}^n$.*

Следствие 3.2.11 *Пусть $X \subset \mathbb{A}^n$ – неприводимое аффинное многообразие. Следующие условия эквивалентны:*

(i) $\dim X = n - 1$;

(ii) *X – гиперповерхность, т.е. $\mathfrak{I}(X) = (f)$ для некоторого неприводимого многочлена $f \in \Bbbk[x_1, \ldots, x_n]$.*

Доказательство. Пусть $\mathfrak{I}(X) = (f)$, где многочлен f неприводим. Кольцо $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/(f)$ порождается координатными функциями $x_1, \ldots, x_n$. Без ограничения общности мы можем считать, что f нетривиально зависит от x_n. Мы утверждаем, что тогда элементы $x_1, \ldots, x_{n-1}$ алгебраически независимы в $\Bbbk[X]$. Действительно, предположим, что $g(x_1, \ldots, x_{n-1}) = 0$ в $\Bbbk[X]$. Это означает, что многочлен g содержится в $\mathfrak{I}(X) = (f)$, т.е. g делится на f в $\Bbbk[x_1, \ldots, x_n]$. Но это невозможно, поскольку g не зависит от x_n. Таким образом, в $\Bbbk[X]$ имеются $n-1$ алгебраически независимых элементов и поэтому $\operatorname{degtr} \Bbbk(X) = n - 1$.

Пусть $\dim X = n - 1$. Рассмотрим любой ненулевой многочлен h, обращающийся в нуль на X. Разложим его на множители: $h = h_1^{k_1} \cdots h_m^{k_m}$. Тогда $X \subset Z(h) = \cup Z(h_i)$ и $X = \cup(X \cap Z(h_i))$. Так как X – неприводимое многообразие, то $X = X \cap Z(h_i)$ для некоторого i и $X \subset Z(h_i)$. Но тогда $n - 1 = \dim X \leq \dim Z(h_i) < \dim \mathbb{A}^n = n$. Отсюда получаем $\dim X = \dim Z(h_i)$ и $X = Z(h_i)$. □

Замечание 3.2.12 Можно доказать, что если $X \subset \mathbb{A}^n$ – неприводимое аффинное многообразие размерности d, то его идеал $\mathfrak{I}(X)$ не может быть порожден менее чем $n - d$ элементами. Геометрическая интуиция подсказывает, что тогда должна существовать система порождающих из ровно $n - d$ элементов. Однако это не всегда так (см., например, упражнение (1), стр. 59).

Упражнения. **(1)** Рассмотрим подмножество $X \subset \mathbb{A}^3$, заданное параметрически:

$$x_1 = t^3, \quad x_2 = t^4, \quad x_4 = t^5.$$

Докажите, что X – неприводимая аффинная кривая (т.е. неприводимое аффинное многообразие размерности 1). Докажите, что $\mathfrak{I}(X)$ не может порождаться двумя элементами.

(2) Докажите, что любая конечно порожденная алгебра над $\Bbbk$ изоморфна алгебре регулярных функций $\Bbbk[X]$ некоторого аффинного многообразия X.

(3) Докажите, что любое конечно порожденное над $\Bbbk$ поле $\mathbb{K}$ изоморфно полю рациональных функций $\Bbbk(X)$ некоторого аффинного многообразия X. Существенно ли здесь условие конечной порожденности?

3.3. Особые и неособые точки

Определение 3.3.1 Пусть $X \subset \mathbb{A}^n$ – некоторое аффинное многообразие и пусть $P = (\alpha_1, \ldots, \alpha_n) \in X$. *Касательным пространством Зарисского* к X в точке P называется аффинное подпространство в $\mathbb{A}^n$, определенное уравнениями

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)(x_i - \alpha_i) = 0 \qquad \text{для всех } f \in \mathfrak{I}(X). \tag{3.3.2}$$

Обозначим это пространство следующим образом: $T_{P,X}$. Пусть теперь X – аффинное многообразие. Будем говорить, что X *неособо* в точке $P \in X$, если $\dim T_{P,X} = \dim X$. В противном случае мы будем говорить, что X особо в этой точке или что $P \in X$ – особая точка. Многообразие называется *неособым*, если оно неособо в каждой своей точке.

Примеры 3.3.3 (i) Аффинное пространство $\mathbb{A}^n$ неособо в каждой своей точке.

(ii) Гиперповерхность $X \subset \mathbb{A}^n$, заданная многочленом f, неособа в точке P тогда и только тогда, когда градиент $(\partial f/\partial x_1, \ldots, \partial f/\partial x_n)$ в точке P отличен от нуля.

(iii) Кривая $X \subset \mathbb{A}^2$, заданная уравнением $x^2 - y^3 = 0$ особа в точке $(0,0)$. Касательное пространство в этой точке совпадает с $\mathbb{A}^2$.

Поясним вышеприведенное определение на примере гиперповерхности X, заданной многочленом f. Рассмотрим прямую L в $\mathbb{A}^n$, проходящую через точку P. Она может быть задана параметрически:

$$x_1 = \alpha_1 + \beta_1 t, \ \ldots, x_n = \alpha_n + \beta_n t, \qquad t \in \Bbbk.$$

Подставив эти выражения в $f(x_1, \ldots, x_n)$, мы получим многочлен от t:

$$g(t) = f(\alpha_1 + \beta_1 t, \ldots, \alpha_n + \beta_n t),$$

который обращается в нуль при $t = 0$. Кратность этого корня называется *кратностью пересечения* L и X. Говорят, что прямая L *касается* гиперповерхности X, если кратность пересечения ≥ 2.

Поместим теперь начало координат в точку $P \in X$, т.е. пусть $P = (0, \ldots, 0)$. Тогда $\alpha_i = 0$ для всех i и для многочлена f имеется разложение

$$f = f_1 + \cdots + f_d,$$

где f_k – сумма всех одночленов степени k. Несложно видеть, что

(i) точка $(0, \ldots, 0)$ неособа тогда и только тогда, когда $f_1 \neq 0$;

(ii) касательное пространство Зарисского $T_{P,X}$ задается уравнением $f_1(x_1, \ldots, x_n) = 0$.

Параметрическая прямая $x_1 = \beta_1 t, \ \ldots, x_n = \beta_n t$ касается гиперповерхности X в точке P тогда и только тогда, когда кратность многочлена

$$f = f_1(\beta_1, \ldots, \beta_n)t + f_2(\beta_1, \ldots, \beta_n)t^2 + \cdots + f_d(\beta_1, \ldots, \beta_n)t^d$$

в нуле строго больше 1. Последнее эквивалентно тому, что $f_1(\beta_1, \ldots, \beta_n) = 0$, т.е. прямая лежит в $T_{P,X}$. Следовательно,

касательное пространство Зарисского $T_{P,X}$ совпадает с объединением всех касательных в точке P прямых.

Следует однако предостеречь читателя, что выбирая f_j в системе (3.3.2), нельзя ограничиться только уравнениями, задающими многообразие X (т.е. такими многочленами, что $X = Z(f_1, \ldots, f_m)$):

Пример 3.3.4 Пусть $X = Z(x_1)$ в $\mathbb{A}^2$. Тогда $T_{0,X}$ – координатная ось $x_1 = 0$. С другой стороны, $X = Z(f)$, где $f = x_1^r$, $r \geq 2$. Для многочлена f система (3.3.2) состоит из одного уравнения, которое тривиально.

Теорема 3.3.5 *Пусть X – аффинное многообразие.*

(i) *Множество всех его особых точек* $\operatorname{Sing} X$ *является алгебраическим подмножеством, отличным от X.*

(ii) *Для любой точки $P \in X$ имеем* $\dim T_{P,X} \geq \dim X$.

Доказательство. Мы рассмотрим только случай гиперповерхности X, заданной многочленом f в $\mathbb{A}^n$, т.е. мы предполагаем, что $\mathfrak{I}(X) = (f)$. Положим $g_i := \partial f/\partial x_i$. Тогда касательное пространство Зарисского $T_{P,X}$ в точке $P = (a_1, \ldots, a_n)$ задается одним уравнением

$$\sum g_i(P)(x_i - a_i) = 0.$$

Таким образом,

$$\dim T_{P,X} = \begin{cases} \dim X \quad\; = n-1 & \text{если } \exists\ i \text{ такое, что } g_i(P) \neq 0, \\ \dim X + 1 = n & \text{если } g_i(P) = 0 \ \ \forall\ i. \end{cases}$$

Отсюда немедленно получается (ii). Отсюда же получается, что $\operatorname{Sing}(X)$ алгебраично и задается уравнениями $f = g_1 = \cdots = g_n = 0$. Предположим, что $\operatorname{Sing}(X) = X$. Тогда $g_1, \ldots, g_n \in \mathfrak{I}(X) = (f)$, т.е. все g_i делятся на f. Так как степень $g_i = \partial f/\partial x_i$ меньше степени f, то это возможно только если $g_i = 0$. В нулевой характеристике это дает противоречие. Если же $\operatorname{char} \Bbbk = p > 0$, то как и в доказательстве предложения 2.5.11 получаем,

что f представляется в виде многочлена от x_i^p (для всех i). Таким образом, $f(x_1,\dots,x_n) = h(x_1^p,\dots,x_n^p)$. Поле $\Bbbk$ алгебраически замкнуто. Поэтому $f(x_1,\dots,x_n) = (h(x_1,\dots,x_n))^p$. Противоречие с тем, что $\mathfrak{I}(X) = (f)$. $\square$

Инвариантное определение касательного пространства Зарисского

Напомним, что произведение $\mathfrak{ab}$ идеалов $\mathfrak{a}$ и $\mathfrak{b}$ – это идеал, порожденный всевозможными произведениями ab, где $a \in \mathfrak{a}$ и $b \in \mathfrak{b}$. Степень $\mathfrak{a}^n$ идеала $\mathfrak{a}$ – это идеал $\underbrace{\mathfrak{a}\cdots\mathfrak{a}}_{n}$.

Теорема 3.3.6 *Пусть $X \subset \mathbb{A}^n$ – аффинное многообразие и $P \in X$ – некоторая точка. Существует канонический изоморфизм*

$$T_{P,X} \simeq P + (\mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2)^*.$$

Здесь через V^* обозначается двойственное к векторному пространству V. Отметим, что $\mathfrak{m}_{P,X}$ и $\mathfrak{m}_{P,X}^2$ являются бесконечномерными векторными пространствами над полем $\Bbbk$. Несмотря на это, размерность факторпространства $\mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2$ конечна.

Доказательство. Для наглядности, мы докажем теорему только в случае, когда $X \subset \mathbb{A}^n$ – гиперповерхность, заданная уравнением $f(x_1,\dots,x_n) = 0$. Пусть $P = (a_1,\dots,a_n)$. Тогда $T_{P,X}$ задается уравнением

$$\sum_{i=1}^{n} c_i(x_i - a_i) = 0, \quad \text{где} \quad c_i := \left.\frac{\partial f}{\partial x_i}\right|_P.$$

Таким образом, вектор $v = (v_1,\dots,v_n)$ лежит в $T_{P,X} - P$ тогда и только тогда, когда $\sum c_i v_i = 0$. Для каждого $v \in T_{P,X} - P$ рассмотрим линейную функцию

$$\ell_v \colon \mathfrak{m}_{P,X} \to \Bbbk, \qquad \ell_v(\varphi) = \sum_{i=0}^{n} v_i \left.\frac{\partial \varphi}{\partial x_i}\right|_P.$$

(Здесь идеал $\mathfrak{m}_{P,X}$ рассматривается как векторное пространство над $\Bbbk$). Предположим, что $\varphi \in \mathfrak{m}_{P,X}^2$. Тогда $\varphi = \sum_j \varphi_j \psi_j$, где φ_j, $\psi_j \in \mathfrak{m}_{P,X}$. Отсюда

$$\ell_v(\varphi) = \sum_{i=0}^{n} v_i \sum_j \left(\varphi_j(P) \frac{\partial \psi_j}{\partial x_i}\bigg|_P + \psi_j(P) \frac{\partial \varphi_j}{\partial x_i}\bigg|_P \right) = 0.$$

Следовательно, $\operatorname{Ker} \ell_v \supset \mathfrak{m}_{P,X}^2$ и поэтому ℓ_v является также линейной функцией на $\mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2$. Получаем отображение

$$\Phi\colon T_{P,X} - P \longrightarrow (\mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2)^*, \qquad v \longmapsto \ell_v,$$

которое, очевидно, является линейным. Докажем, что Φ – изоморфизм. Действительно, если $\Phi(v) = 0$, то $\ell_v(\varphi) = 0$ для всех $\varphi \in \mathfrak{m}_{P,X}$. В частности, $v_i = \ell_v(x_i - a_i) = 0$ для всех i. Это дает нам $v = 0$, т.е., инъективность отображения Φ. Для доказательства сюръективности рассмотрим линейную функцию $\ell\colon \mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2 \to \Bbbk$. Ясно, что мы можем ее рассматривать как функцию на $\mathfrak{m}_{P,X}$, которая зануляется на $\mathfrak{m}_{P,X}^2$. Положим $v_i := \ell(x_i - a_i)$ и $v := (v_1, \ldots, v_n)$. Любую функцию $\varphi \in \mathfrak{m}_{P,X}$ можно записать в виде

$$\varphi = \sum_{i=1}^{n} b_i(x_i - a_i) + \varphi_2, \quad \text{где} \quad b_i = \frac{\partial \varphi}{\partial x_i}\bigg|_P, \quad \varphi_2 \in \mathfrak{m}_{P,X}^2.$$

Отсюда

$$\ell(\varphi) = \sum_{i=1}^{n} b_i \ell(x_i - a_i) = \sum_{i=1}^{n} v_i \left.\frac{\partial \varphi}{\partial x_i}\right|_P = \ell_v(\varphi).$$

Таким образом, $\ell = \ell_v$. Это доказывает сюръективность Φ. $\square$

Пусть $P \in X$ – неособая точка. Множество элементов $y_1, \ldots, y_d \in \mathfrak{m}_{P,X}$ называется *системой локальных параметров* в точке P, если их образы в $\mathfrak{m}_{P,X}/\mathfrak{m}_{P,X}^2$ образуют базис.

Упражнения. **(1)** Может ли *гиперповерхность Ферма* $\sum_i x_i^d + 1 = 0$ быть особой?

(2) Найдите все особые точки кривой, заданной уравнением $y^4 - x - 4xy - 2xy^2 + x^2 = 0$ в $\mathbb{A}^2$.

(3) Докажите, что для любого $d \in \mathbb{N}$ существует неособая гиперповерхность степени d в $\mathbb{A}^n$. Рассмотрите случай произвольной характеристики.

(4) Пусть $X_1 \subset \mathbb{A}^n$ и $X_2 \subset \mathbb{A}^n$ – алгебраические множества такие, что $X_1 \cap X_2 \neq \varnothing$ и пусть $X = X_1 \cup X_2$. Докажите, что X особо в каждой точке $P \in X_1 \cap X_2$.

(5) Докажите, что кривая $y^2 = f(x)$ является особой тогда и только тогда, когда многочлен $f(x)$ имеет кратные корни.

3.4. Проективные многообразия

Как и всюду в этой главе основное поле $\Bbbk$ алгебраически замкнуто. Напомним, что n-мерное *проективное пространство* над $\Bbbk$ – это множество классов эквивалентных наборов $(a_0, \ldots, a_n)$, $a_i \in \Bbbk$, $(a_0, \ldots, a_n) \neq (0, \ldots, 0)$, относительно эквивалентности $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$, $\lambda \in \Bbbk^*$, т. е. относительно умножения на любой отличный от нуля элемент поля. Проективное пространство обозначается через $\mathbb{P}^n$. Элементы из $\mathbb{P}^n$ называются точками. Любой набор элементов $(a_0, \ldots, a_n)$ из класса эквивалентности, определяющего некоторую точку $P \in \mathbb{P}^n$, называется *однородными координатами* точки P. Чтобы акцентировать внимание на том, что координаты a_i определены с точностью до умножения на ненулевой элемент поля, мы будем их записывать также в виде $(a_0 : \cdots : a_n)$.

Кольцо многочленов $\Bbbk[x_0, \ldots, x_n]$ мы будем рассматривать как градуированное кольцо: кольцо R называется *градуированным*, если оно обладает разложением в прямую сумму $R = \bigoplus_{i=0}^{\infty} R_d$ абелевых групп R_d, таких, что $R_d R_e \subset R_{d+e}$ для любых d, e. Элементы из R_d называются *однородными степени* d. Таким образом, любой элемент из R можно *однозначно* записать в виде (конечной) суммы однородных элементов. Ясно, что кольцо многочленов $R = \Bbbk[x_0, \ldots, x_n]$ является градуированным: R_d порождается одночленами степени d и состоит из многочленов f таких, что $f(tx_0, \ldots, tx_n) = t^d f(x_0, \ldots, x_n)$.

Идеал $\mathfrak{a}$ в градуированном кольце R называется *однородным*, если он представляется в виде $\mathfrak{a} = \bigoplus_{i=0}^{\infty} (\mathfrak{a} \cap R_d)$, где в правой части стоит прямая сумма абелевых групп. Иначе говоря, идеал $\mathfrak{a}$ однороден, если каждый его элемент f представляется в виде суммы однородных элементов из $\mathfrak{a}$.

Замечание 3.4.1 Для однородного идеала $\mathfrak{a} \subset R$ имеется естественный сюръективный гомоморфизм

$$R = \bigoplus R_d \to \bigoplus R_d/(R_d \cap \mathfrak{a}),$$

ядром которого является наш идеал $\mathfrak{a}$. По теореме о гомоморфизме имеем разложение $R/\mathfrak{a} = \bigoplus_{d=0}^{\infty} R_d/(R_d \cap \mathfrak{a})$. Оно определяет градуировку на факторкольце $R/\mathfrak{a}$, т.е. факторкольцо $R/\mathfrak{a}$ также градуировано. Если $\pi\colon R \to R/\mathfrak{a}$ – гомоморфизм факторизации, то градуировка определяется следующим образом: $(R/\mathfrak{a})_d = \pi(R_d)$.

Пример 3.4.2 Идеал $\mathfrak{a}$, порожденный однородными элементами $f_\alpha \in R_\alpha$, $\alpha \in I$ однороден. Действительно, любой элемент $f \in \mathfrak{a}$ имеет вид $f = \sum_\alpha f_\alpha g_\alpha$ для некоторых $g_\alpha \in R$. Так как кольцо R градуировано, то $g_\alpha = \sum_k h_{\alpha,k}$, $h_{\alpha,k} \in R_k$. Поэтому $f = \sum_{\alpha,k} f_\alpha g_k \in \bigoplus(\mathfrak{a} \cap R_{\alpha+k})$. Очевидно, что верно и обратное: каждый однородный идеал порождается однородными элементами.

Многочлены из $\Bbbk[x_0, \ldots, x_n]$ мы уже не можем рассматривать как функции на $\mathbb{P}^n$ ввиду неоднозначности координатных представлений точек в $\mathbb{P}^n$. Однако если f – однородный многочлен степени d, то $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d df(a_0, \ldots, a_n)$, так что свойство f обращаться или не обращаться в нуль зависит только от класса эквивалентности $(a_0 : \cdots : a_n)$. Таким образом, имеет смысл говорить о множестве $Z(f) = \{P \in \mathbb{P}^n \mid f(P) = 0\}$ нулей в $\mathbb{P}^n$ однородного многочлена $f \in \Bbbk[x_0, \ldots, x_n]$. Для любого множества T однородных элементов из $\Bbbk[x_0, \ldots, x_n]$ также можно определить его множество нулей $Z(T)$, полагая $Z(T) = \{P \in \mathbb{P}^n \mid f(P) = 0 \quad \forall f \in T\}$. Если $\mathfrak{a}$ – однородный идеал в $\Bbbk[x_0, \ldots, x_n]$, то определим его множество нулей $Z(\mathfrak{a})$, полагая $Z(\mathfrak{a}) = Z(T)$, где T – множество всех однородных элементов из $\mathfrak{a}$.

Определение 3.4.3 Подмножество $X \subset \mathbb{P}^n$ называется *проективным алгебраическим множеством*, если существует множество T однородных элементов из $\Bbbk[x_0, \ldots, x_n]$, такое, что

$X = Z(T)$. Непустое алгебраическое множество $X \subset \mathbb{P}^n$ называется *проективным алгебраическим многообразием* или просто *проективным многообразием*.

Аналогично предложению 3.1.4 доказывается следующее

Предложение 3.4.4 *Объединение двух проективных алгебраических множеств является алгебраическим множеством. Пересечение любого семейства проективных алгебраических множеств тоже будет алгебраическим множеством. Пустое множество и все пространство $\mathbb{P}^n$ являются алгебраическими множествами.*

Таким образом, как и в определении 3.1.6, мы можем определить *топологию Зарисского* на $\mathbb{P}^n$ и на произвольном проективном алгебраическом множестве $X \subset \mathbb{P}^n$, назвав замкнутыми подмножествами алгебраические множества.

Для любого подмножества $X \subset \mathbb{P}^n$ определим его *однородный идеал* в $\Bbbk[x_0, \ldots, x_n]$, обозначаемый через $\mathfrak{I}(X)$, как идеал, порожденный множеством однородных элементов $f \in \Bbbk[x_0, \ldots, x_n]$, таких, что $f(P) = 0$ для всех $P \in X$. Факторкольцо $R(X) = \Bbbk[x_0, \ldots, x_n]/\mathfrak{I}(X)$ назовем *однородным координатным кольцом* $R(X)$ проективного многообразия X. Кольцо $R(X)$ также градуировано (см. замечание 3.4.1). Проективное многообразие $X \subset \mathbb{P}^n$ называется *гиперповерхностью*, если его однородный идеал $\mathfrak{I}(X)$ является главным, т.е. $\mathfrak{I}(X) = (f)$. В этом случае говорят, что гиперповерхность X *задается* многочленом f (ср. 3.1.2).

Определение 3.4.5 Проективное многообразие $X \subset \mathbb{P}^n$ называется *неприводимым*, если оно не допускает представления $X = X_1 \cup X_2$ в виде объединения проективных алгебраических множеств $X_1, X_2 \neq X$.

Так же как и в аффинном случае доказывается, что проективное многообразие $X \subset \mathbb{P}^n$ неприводимо тогда и только тогда, когда его однородный идеал $\mathfrak{I}(X)$ прост.

Пример 3.4.6 Гиперповерхность, заданная многочленом f, неприводима, если и только если многочлен f неприводим.

Отметим, что в отличие от аффинного случая, элементы кольца $R(X)$ не могут рассматриваться как функции на X.

Определение 3.4.7 Пусть $X \subset \mathbb{P}^n$ – неприводимое проективное многообразие. Определим *поле рациональных функций* $\Bbbk(X)$ многообразия X как следующее подполе поля рациональных дробей кольца $R(X)$:

$$\Bbbk(X) := \left\{ \frac{f}{g} \;\middle|\; \begin{array}{l} f, g \in R(X) - \text{однородные} \\ \text{одинаковой степени и } g \neq 0 \end{array} \right\},$$

Здесь степени $\deg f$ и $\deg g$ определяются градуировкой из замечания 3.4.1. Ясно, что каждый элемент поля $\Bbbk(X)$ является $\Bbbk$-значной функцией, определенной на открытом по Зарисскому множестве в X.

Аффинное покрытие

Рассмотрим *координатную гиперплоскость* H_i – подмногообразие в $\mathbb{P}^n$, заданное уравнением $x_i = 0$ и пусть $U_i := \mathbb{P}^n \setminus H_i$. Тогда $\mathbb{P}^n$, очевидно, покрывается открытыми множествами U_i. Определим отображение

$$\phi_i \colon U_i \to \mathbb{A}^n, \qquad \phi_i(a_0, ..., a_n) = (a_0/a_i, \ldots, \widehat{a_i/a_i}, \ldots, a_n/a_i)$$

(здесь пропущено a_i/a_i). Отметим, что отображение ϕ_i определено корректно. Множества U_i называются *аффинными картами*.

Предложение 3.4.8 *Отображение ϕ_i биективно и переводит алгебраические множества в алгебраические. Более точно: если $X \subset \mathbb{P}^n$ – алгебраическое множество, то и $\phi_i(X \cap U_i)$ является алгебраическим множеством. Если $X \subset \mathbb{P}^n$ – неприводимое алгебраическое множество, то неприводимым является и $\phi_i(X \cap U_i)$.*

Доказательство. Будем считать, что $i = 0$. Во-первых, отображение ϕ_0, очевидно, биективно. Действительно, обратным к нему отображением является $\psi \colon \mathbb{A}^n \to U_0$, $\psi(a_1, ..., a_n) =$

$(1, a_1, ..., a_n)$. Поэтому достаточно показать, что замкнутые множества в U_i соответствуют замкнутым множествам в $\mathbb{A}^n$. Пусть $X \subset \mathbb{P}^n$ – алгебраическое множество, пусть $\mathfrak{I}(X) \subset \Bbbk[x_0, x_1, \ldots, x_n]$ – его однородный идеал и пусть $T \subset \mathfrak{I}(X)$ – множество всех однородных элементов. Для любого $f \in T$ определим $\tilde{f} \in \Bbbk[y_1, \ldots, y_n]$ следующим образом:

$$\tilde{f}(y_1, \ldots, y_n) = f(1, x_1, \ldots, x_n).$$

Ясно, что отображение $\Bbbk[x_0, x_1, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n], \;\; f \mapsto \tilde{f}$ является гомоморфизмом колец. Положим

$$\tilde{T} = \{\tilde{f} \mid f \in T\} \subset \Bbbk[y_1, \ldots, y_n].$$

Имеем

$$P = (a_0 : \cdots : a_n) \in U_0 \cap X \iff a_0 \neq 0 \text{ и } f(P) = 0, \; \forall f \in T.$$

Поэтому $Q = (b_1, \ldots, b_n) \in \phi_0(X \cap U_0) \iff (1 : b_1 : \cdots : b_n) \in X \cap U_0 \iff f(1, b_1, \ldots, b_n) = 0 \iff \tilde{f}(b_1, \ldots, b_n)$. Таким образом, $\phi_i(X \cap U_i) = Z(\tilde{T})$. Доказательство последнего утверждения мы оставляем читателю. □

Таким образом, каждое проективное многообразие X покрывается аффинными многообразиями $X \cap U_i$. Обратно, по каждому аффинному многообразию $Y \subset \mathbb{A}^n$ мы можем построить проективное многообразие $X \subset \mathbb{P}^n$ такое, что $X \cap U_i \simeq Y$. Этот процесс называется *проективным замыканием*.

Пример 3.4.9 Пусть $Y \subset \mathbb{A}^n$ – гиперповерхность, заданная многочленом $f(y_1, \ldots, y_n)$ степени d. Тогда ее проективное замыкание $X \subset \mathbb{P}^n$ задается однородным многочленом $x_0^d f(x_1/x_0, \ldots, x_n/x_0)$.

Предложение 3.4.10 *Пусть $X \subset \mathbb{P}^n$ – неприводимое проективное многообразие. Если $X \cap U_i \neq \varnothing$, то существует естественный изоморфизм полей функций $\phi_i^* \colon \Bbbk(\phi_i(U_i \cap X)) \longrightarrow \Bbbk(X)$.*

Доказательство. Пусть, например, $i = 0$. Положим, $Y_0 := \phi_0(X \cap U_0) \subset \mathbb{A}^n$. Рассмотрим элемент $f \in \Bbbk(X)$. По определению мы можем (неоднозначно) представить его в виде $f = g/h$,

где $g, h \in R(X)$ – однородные элементы и $h \neq 0$. Мы можем рассматривать g и h как однородные многочлены одинаковой степени от $x_0, \ldots, x_n$, причем $h \notin \mathfrak{I}(X)$. Положим $\phi_0^*(f) := \tilde{g}/\tilde{h}$. Докажем корректность этой формулы. Во-первых $\phi_0^*(f)$ не зависит от выбора представителей g и h по модулю $\mathfrak{I}(X)$. Действительно, пусть $g' = g + \sum t_i r_i$, $h' = h + s_i q_i$, где $t_i, s_i \in \mathfrak{I}(X)$ – однородные элементы, а $r_i, q_i \in \Bbbk[x_0, \ldots, x_n]$. Тогда

$$\phi_0^*\left(\frac{g'}{h'}\right) = \frac{\tilde{g}'}{\tilde{h}'} = \frac{\tilde{g} + \sum \tilde{t}_i \tilde{r}_i}{\tilde{h} + \sum \tilde{s}_i \tilde{q}_i} = \phi_0^*\left(\frac{g}{h}\right).$$

Последнее выполнено поскольку $\tilde{t}_i, \tilde{s}_i$ – элементы (неоднородного) идеала $\mathfrak{I}(Y_0)$ аффинного многообразия Y_0.

Далее, если $g/h = g'/h'$, то в кольце $R(X)$ имеет место равенство $gh' = g'h$. Отсюда в кольце $\Bbbk[Y_0]$ имеем $\tilde{g}\tilde{h}' = \tilde{g}'\tilde{h}$ и поэтому $\phi_0^*(g'/h') = \phi_0^*(g/h)$. Из определения отображения $g \mapsto \tilde{g}$ получаем, что ϕ_0^* – гомоморфизм (а, следовательно, вложение) полей. Наконец, сюръективность ϕ_0^* следует из сюръективности отображения $g \mapsto \tilde{g}$. □

Замечание 3.4.11 Рассматривая элементы $\Bbbk(\phi_i(U_i \cap X))$ и $\Bbbk(X)$ как (не всюду определенные) функции на $\phi_i(U_i \cap X)$ и X соответственно, мы можем отображение ϕ_i записать в виде $\phi_i^*(f) = f \circ \phi_i$.

Определим *размерность* $\dim X$ проективного многообразия X как степень трансцендентности его поля рациональных функций $\Bbbk(X)$. Последнее предложение показывает, что размерность X совпадает с размерностью пересечения $X \cap U_i$ (если это пересечение непусто). Как и в аффинном случае, будем говорить, что необязательно неприводимое) проективное многообразие имеет *чистую размерность* d, если размерности всех его неприводимых компонент равны d. *Проективной кривой* называется проективное многообразие чистой размерности 1. Плоской проективной кривой называется кривая $X \subset \mathbb{P}^2$.

Будем говорить, что функция $f \in \Bbbk(X)$ *регулярна* в точке $P \in X$, если функция $f \circ \phi_i$ регулярна в точке $\phi_i(P)$ на $\phi_i(U_i \cap X)$.

Предложение 3.4.12 *Пусть $X \subset \mathbb{P}^n$ – неприводимое проективное многообразие. Если функция $f \in \Bbbk(X)$ регулярна в каждой точке X, то она – константа.*

Доказательство. Положим $R := R(X)$ Пусть $f \in \Bbbk(X)$ – непостоянная регулярная функция. Рассмотрим аффинную карту $U_i = \{x_i \neq 0\}$. В обозначениях доказательства предложения 3.4.10 имеем $\phi_i^*(f) = \tilde{g}/\tilde{h}$ – регулярная функция на аффинном многообразии $Y_i := \phi_i(U_i \cap X) \subset \mathbb{A}^n$. Поэтому имеет место представление $\tilde{g}/\tilde{h} = \tilde{g}_i/\tilde{h}_i$, где $f_i, g_i \in R(X)$ – однородные элементы одинаковой степени и $\tilde{h}_i = 1$ в кольце $\Bbbk(Y_i)$. Это возможно только если $h_i = x_i^{d_i}$, $d_i = \deg g_i = \deg h_i$.

Таким образом, для каждого $i = 0, \ldots, n$ мы можем записать $f = g_i/x_i^{d_i}$. Отсюда $f \cdot R_{d_i} \subset R_{d_i}$. Положим $d := \sum d_i$. Тогда $f \cdot R_d \subset R_d$. Заметим, что R_d является конечномерным векторным пространством над $\Bbbk$. Более того, $R_d \neq 0$. Действительно, иначе идеал $\mathfrak{I}(X)$ содержит все однородные многочлены степени d. Из простоты $\mathfrak{I}(X)$ тогда немедленно получаем $x_i \in \mathfrak{I}(X)$. Поэтому $\mathfrak{I}(X) = (x_0, \ldots, x_n)$, $R = \Bbbk$ и $\Bbbk(X) = \Bbbk \ni f$, что противоречит нашему предположению.

Рассмотрим в R_d оператор умножения на f, т.е. оператор $\mathscr{A}\colon R_d \to R_d$, $s \mapsto f \cdot s$. Пусть $\mu(t)$ – минимальный многочлен этого оператора и пусть $s \in R_d$ – любой ненулевой элемент. Тогда $0 = \mu(\mathscr{A})s = \mu(f)s$. С другой стороны, поле $\Bbbk$ алгебраически замкнуто. Следовательно, $\mu(t)$ разлагается на линейные множители: $\mu(t) = \prod(t - \alpha_i)$ и $s\prod(f - \alpha_i) = 0$. Так как в кольце R нет делителей нуля и $s \neq 0$, то $f = \alpha_i$ для некоторого i. Предложение доказано. □

Определение 3.4.13 Проективное многообразие $X \subset \mathbb{P}^n$ называется *неособым* в точке $P \in X$, если для некоторой аффинной карты U_i аффинное многообразие $X \cap U_i$ неособо в P.

Несложно проверить, что это определение не зависит от выбора аффинной карты: если P принадлежит двум аффинным картам U_i и U_j, то неособость $X \cap U_i$ и $X \cap U_j$ эквивалентна. Покажем это на примере гиперповерхности.

Предложение 3.4.14 *Пусть $X \subset \mathbb{P}^n$ – гиперповерхность, заданная многочленом $f(x_0, \ldots, x_n)$. Тогда X особа в точке $P \in X$ если и только если*

$$\partial f/\partial x_i(P) = 0 \quad \textit{для всех } i.$$

Доказательство. Пусть точка P лежит в карте U_0. Мы можем считать, что $P = (1 : a_1 : \cdots : a_n)$. Уравнение $X \cap U_0 \subset \mathbb{A}^n$ имеет вид $f(1, x_1, \ldots, x_n)$.

Точка $P \in X \cap U_0$ особа тогда и только тогда, когда $\partial f/\partial x_i(P) = 0, \;\; i = 1, \ldots, n$. Напомним формулу Эйлера: если $f(x_0, \ldots, x_n)$ – неприводимый однородный многочлен степени m, то

$$\sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i} = mf.$$

Подставляя сюда $(x_0, \ldots, x_n) = (1 : a_1 : \cdots : a_n)$, получим $\partial f/\partial x_0(P) = 0$. □

В дальнейшем нас будут интересовать лишь одномерные проективные многообразия – проективные алгебраические кривые. Большая часть теории плоских алгебраических кривых опирается на изучение их пересечений и здесь основную роль играет *теорема Безу*. Мы докажем ее сейчас в несколько ослабленной форме:

Теорема 3.4.15 (теорема Безу) *Пусть $X, Y \subset \mathbb{P}^2$ – различные кривые степеней n и m, соответственно. Тогда $X \cap Y \neq \varnothing$. Если X и Y не имеют общих компонент, то X и Y имеют не более nm общих точек.*

Доказательство. Пусть $\mathfrak{I}(X) = (f)$ и $\mathfrak{I}(Y) = (g)$, где f и g – многочлены без кратных множителей. Мы можем считать также, что f и g не имеют общих множителей. Отметим, что $X \cap Y$ – или пусто, или нульмерное алгебраическое множество, являющееся объединением конечного числа точек $P_1, \ldots, P_r$. Во втором случае мы соединим точки P_i попарно прямыми $L_{i,j}$. Так как таких прямых конечное число, то найдется точка P, не лежащая ни на этих прямых, ни на данных кривых X или Y. Если

$X \cap Y = \varnothing$, то мы возьмем в качестве P произвольную точку. Выберем координатную систему $x : y : z$ так, чтобы точка P имела координаты $(1 : 0 : 0)$. Тогда в случае $X \cap Y \neq \varnothing$ прямая, проходящая через P и P_i, не содержит точек P_j при $j \neq i$. Это означает, что каждая точка $P_i = (\alpha_i : \beta_i : \gamma_i)$ однозначно определяется двумя последними координатами $(\beta_i : \gamma_i)$.

Запишем

$$f(x, y, z) = a_0 x^n + \cdots + a_{n-1} x + a_n,$$
$$g(x, y, z) = b_0 x^m + \cdots + b_{m-1} x + b_m.$$

где a_i, b_j – однородные многочлены от y, z степеней i и j, соответственно. *Результант*

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & & & & \\ & a_0 & a_1 & \ldots & a_n & & & \\ & & \ldots\ldots\ldots\ldots & & & & & \\ & & & & a_0 & a_1 & \ldots\ldots & a_n \\ b_0 & b_1 & \ldots\ldots\ldots\ldots & & b_m & & & \\ & b_0 & b_1 & \ldots\ldots\ldots\ldots & & b_m & & \\ & & & \ldots\ldots\ldots\ldots & & & & \\ & & & & b_0 & b_1 & \ldots\ldots & b_m \end{vmatrix} \tag{3.4.16}$$

многочленов f и g относительно x является однородным многочленом степени nm от неизвестных y, z (возможно нулевым). Действительно, для проверки последнего утверждения достаточно доказать тождество

$$R(f(x, ty, tz), g(x, ty, tz)) = t^{n+m} R(f(x, y, z), g(x, y, z)).$$

Так как $a_i(ty, tz) = t^i a_i(y, z)$ и $b_j(ty, tz) = t^j b_j(y, z)$, то левая часть последнего равенства равна

$$\begin{vmatrix} a_0 & ta_1 & t^2 a_2 & \ldots & t^n a_n & & & \\ & a_0 & ta_1 & \ldots\ldots\ldots & t^n a_n & & & \\ & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\ & & & & a_0 & ta_1 & \ldots\ldots & t^n a_n \\ b_0 & tb_1 & \ldots\ldots\ldots\ldots\ldots\ldots & & t^m b_m & & & \\ & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\ & & b_0 & tb_1 & \ldots\ldots\ldots\ldots\ldots\ldots & & & t^m b_m \end{vmatrix}$$

Умножим каждую i-ую строку на t^{i-1} при $1 \le i \le m$ и на t^{i-m-1} при $m+1 \le i \le n+m$. Получим

$$\begin{vmatrix} a_0 & ta_1 & t^2a_2 & \dots & t^na_n & & & \\ & ta_0 & t^2a_1 & \dots\dots & t^{n+1}a_n & & & \\ & & \dots\dots\dots\dots\dots\dots\dots\dots & & & & & \\ & & & t^{m-1}a_0 & t^ma_1 & \dots & t^{n+m-1}a_n \\ b_0 & tb_1 & \dots\dots\dots\dots\dots & & t^mb_m & & & \\ & \dots\dots\dots\dots\dots\dots\dots\dots & & & & & & \\ & & t^{n-1}b_0 & t^nb_1 & \dots\dots\dots\dots & & t^{n+m-1}b_m \end{vmatrix}$$

Сравнивая последний определитель с (3.4.16), делаем вывод, что

$$t^{m(m-1)/2}t^{n(n-1)/2}R(f(x,ty,tz),g(x,ty,tz)) = \\ = t^{(n+m)(n+m-1)/2}R(f,g).$$

Отсюда получаем требуемое равенство. Таким образом, $R(f,g)$ является однородным многочленом степени nm.

Далее по основному свойству результанта $R(f,g)$ обращается в нуль в точке $y=\beta$, $z=\gamma$ тогда и только тогда, когда существует такое значение $x=\alpha$, что $f(\alpha,\beta,\gamma)=g(\alpha,\beta,\gamma)=0$, т. е. когда β, γ будут второй и третьей координатами некоторой точки пересечения кривых X и Y. Так как основное поле алгебраически замкнуто, то это доказывает непустоту $X\cap Y$. Далее если $X\cap Y=\{P_1,\dots,P_r\}$ и $r>nm$, то, согласно нашему выбору точки P, все P_i дают различные значения отношения $\beta_i:\gamma_i$. Поэтому однородный многочлен $R(f,g)$ степени nm обращается в нуль в $r>nm$ непропорциональных точках $\beta_i:\gamma_i$. Это возможно только если $R(f,g)$ – нулевой многочлен. Последнее противоречит конечности множества $X\cap Y$. □

Замечание 3.4.17 Теорема Безу в общей форме утверждает, что если кривые X, $Y\subset\mathbb{P}^2$ не имеют общих компонент, то

$$\sum_{P\in X\cap Y}\operatorname{mult}_P(X\cap Y)=nm,$$

где $\operatorname{mult}_P(X\cap Y)$ – так называемая *кратность пересечения* кривых X и Y в точке P.

Упражнения. **(1)** Докажите, что единица в любом градуированном кольце является однородным элементом степени 0.

(2) Рассмотрим отображение

$$\phi\colon \mathbb{P}^1 \longrightarrow \mathbb{P}^n, \qquad (u:v) \longmapsto (u^n : u^{n-1}v : \cdots : uv^{n-1} : v^n).$$

Докажите, что образом ϕ является неособая алгебраическая кривая, а ее однородный идеал порождается элементами степени 2.

(3) При каком a кривая, заданная уравнением $x^3+y^3+z^3+axyz=0$ в $\mathbb{P}^2$, приводима?

(4) При каком a кривая, заданная уравнением $x^3+y^3+z^3+axyz=0$ в $\mathbb{P}^2$, особа?

(5) Найдите все особые точки кривой, заданной уравнением $y^4 - xz^3 - 4xyz^2 - 2xy^2z + x^2z^2 = 0$ в $\mathbb{P}^2$.

(6) Докажите, что в градуированном кольце

(i) идеал $\mathfrak{a}$ однороден тогда и только тогда, когда он может быть порожден однородными элементами;

(ii) сумма, произведение и пересечение однородных идеалов, а также радикал однородного идеала однородны;

(iii) для установления простоты однородного идеала $\mathfrak{a}$ достаточно проверить, что для любых двух однородных элементов f и g из условия $fg \in \mathfrak{a}$ следует, что либо $f \in \mathfrak{a}$, либо $g \in \mathfrak{a}$.

(7) Покажите, что проективное многообразие $X \subset \mathbb{P}^n$ тогда и только тогда имеет размерность $n-1$, когда оно является множеством нулей одного неприводимого однородного многочлена f положительной степени *Указание.* Воспользуйтесь 3.2.11.

(8) Докажите теорему Безу в форме 3.4.17 для случая, когда X – прямая. *Указание.* Воспользуйтесь определением кратности пересечения кривой и прямой, данным в §3.3

(9) Докажите, что неприводимая плоская кубическая кривая может иметь не более одной особой точки. *Указание.* Воспользуйтесь теоремой Безу и упражнением выше.

3.5. Дискретные нормирования полей степени трансцендентности 1

3.5.1 Напомним, что как и всюду в этой главе, если не оговаривается противное, то мы считаем, что основное поле $\Bbbk$ ал-

гебраически замкнуто. Пусть X – (аффинная или проективная) алгебраическая кривая над $\Bbbk$ и пусть $\mathbb{K} = \Bbbk(X)$ – поле функций на X. Тогда $\mathbb{K}$ удовлетворяет следующим двум условиям:

(i) $\mathbb{K}$ конечно порождено (как поле) над $\Bbbk$;

(ii) степень трансцендентности $\mathbb{K}$ над $\Bbbk$ равна 1.

Эти два условия эквивалентны следующему:

(iii) $\mathbb{K}$ является конечным алгебраическим расширением чисто трансцендентного расширения $\Bbbk(t)/\Bbbk$.

Определение 3.5.2 Пусть K – любое поле. *Дискретным нормированием* K называется гомоморфизм $v\colon K^* = K \setminus \{0\} \to \mathbb{Z}$ такой, что

$$v(a+b) \geq \min(v(a), v(b)) \tag{3.5.3}$$

для всех $a, b \in K^*$. Обычно v доопределяют на всем K, полагая $v(0) = +\infty$. Кольцо $\{a \in K \mid v(a) \geq 0\}$ называется *кольцом нормирования поля* K. В этом кольце имеется идеал $\mathfrak{m} := \{a \in K \mid v(a) > 0\}$ и каждый элемент $\mathscr{O} \setminus \mathfrak{m}$ является обратимым. Поэтому $\mathfrak{m}$ – единственный максимальный идеал в $\mathscr{O}$, т.е. кольцо $\mathscr{O}$ *локально*.

Простейшим примером является *тривиальное* дискретное нормирование $v(K^*) = 0$.

Замечание 3.5.4 Пусть $v(\cdot)$ – дискретное нормирование поля K. Положим $\|a\| = e^{-v(a)} \in \mathbb{R}$. Тогда

(i) $\|a\| \geq 0$ и $\|a\| = 0$ тогда и только тогда, когда $a = 0$;

(ii) $\|ab\| = \|a\|\|b\|$;

(iii) $\|a+b\| \leq \max\{\|a\|, \|b\|\} \leq \|a\| + \|b\|$.

Следовательно, $\rho(a,b) := \|a-b\|$ является *метрикой* и задает на K *топологию*.

Замечание 3.5.5 Если $v(a) \neq v(b)$, то в (3.5.3) имеет место равенство. Действительно, предположим, что $v(a) < v(b)$. Тогда

$$v(a+b) \geq v(a) = v(a+b-b) \geq \min(v(a+b), v(b))$$

Если $\min(v(a+b), v(b)) = v(a+b)$, то всюду выше мы имеем равенства. Если же $\min(v(a+b), v(b)) = v(b)$, то $v(a) \geq v(b)$. Противоречие. По индукции это правило распространяется на любое количество слагаемых: если $v(a_i) \neq v(a_j)$ при $i \neq j$, то

$$v\Big(\sum_{i=1}^{n} a_i\Big) = \min\big(v(a_1), \ldots, v(a_n)\big).$$

Действительно, предположим, что это равенство верно для $n-1$. Тогда $v\left(\sum_{i=1}^{n-1} a_i\right) = \min(v(a_1), \ldots, v(a_{n-1}))$. Отсюда $v\left(\sum_{i=1}^{n-1} a_i\right) \neq v(a_n)$ и тогда

$$v\Big(\sum_{i=1}^{n} a_i\Big) = \min\big(v(a_n), \min\left(v(a_1), \ldots, v(a_{n-1})\right)\big) = \\ = \min\big(v(a_1), \ldots, v(a_n)\big).$$

Примеры 3.5.6 (i) Пусть $K = \mathbb{Q}$. Зафиксируем простое число p. Тогда каждый элемент $r \in \mathbb{Q}$ можно записать в виде $r = p^s \frac{n}{m}$, где $p \nmid nm$. Положим $v_p(r) := s$. Тогда v_p – дискретное нормирование поля $\mathbb{Q}$ (так называемое *p-адическое нормирование*).

(ii) Пусть $K = \Bbbk(x)$ – поле рациональных дробей над произвольным полем $\Bbbk$. Зафиксируем неприводимый многочлен $p(x) \in \Bbbk[x]$. Как выше каждую дробь представим в виде $\frac{f(x)}{g(x)} p(x)^s$, $p(x) \nmid f(x)g(x)$ и определим дискретное нормирование $v_{p(x)}(\frac{f(x)}{g(x)} p(x)^s) = s$. Если поле $\Bbbk$ алгебраически замкнуто, то $p(x)$ имеет вид $x - \alpha$ и, следовательно, такие нормирования $v_{p(x)}$ взаимно однозначно соответствуют элементам $\alpha \in \Bbbk$.

(iii) Пусть снова $K = \Bbbk(x)$, где $\Bbbk$ – произвольное поле. Для каждой дроби $f(x)/g(x) \in \Bbbk(x)$ положим $v_\infty(f/g) = -\deg f + \deg g$ (и $v_\infty(\alpha) = 0$ для $\alpha \in \Bbbk$). Получим еще одно дискретное нормирование $v_\infty \colon \Bbbk(x)^* \to \mathbb{Z}$.

(iv) Рассмотрим поле $\mathscr{M}$ мероморфных функций на $U \subset \mathbb{C}$ (или на произвольной римановой поверхности X). Зафиксируем точку $x_0 \in \mathbb{C}$ и разложим $f \in \mathscr{M}$ в ряд Лорана в окрестности x_0

$$f(x) = \sum_{k=s}^{\infty} a_k (x - x_0)^k, \qquad a_k \neq 0.$$

Тогда $v_{x_0}(f) = s$ является дискретным нормированием поля $\mathscr{M}$. Ограничение v_{x_0} на подполе $\mathbb{C}(x) \subset \mathscr{M}$ совпадает с нормированием, определенным в (ii).

(v) Если имеется одно дискретное нормирование v поля K, то для любого $n \in \mathbb{N}$ отображение $nv\colon K^* \to \mathbb{Z}$ также является дискретным нормированием. Нормирования v и nv мы обычно не различаем.

Теорема 3.5.7 *Пусть X – неприводимая алгебраическая кривая над полем $\Bbbk = \bar{\Bbbk}$, пусть $\mathbb{K} := \Bbbk(X)$ – ее поле рациональных функций и пусть $P \in X$ – неособая точка. Тогда существует дискретное нормирование $v = v_p$ поля $\mathbb{K}$ тривиальное на $\Bbbk$ и такое, что локальное кольцо $\mathscr{O}_{P,X}$ является кольцом нормирования для v. Такое нормирование v единственно с точностью до пропорциональности.*

Доказательство. Теорема будет доказана только для случая плоской алгебраической кривой. Общий случай отличается лишь незначительным усложнением обозначений. Он также может быть сведен к плоскому при помощи подходящих проекций окрестности точки P. Мы также можем считать, что X – аффинная кривая.

Итак пусть $X \subset \mathbb{A}^2$ – неприводимая плоская аффинная кривая и пусть $P \in X$ – неособая точка. Для удобства выберем координаты в $\mathbb{A}^2$ так, что P – начало координат. Положим $\mathscr{O} := \mathscr{O}_{P,X}$ и $\mathfrak{m} := \mathfrak{m}_{P,X}$. Доказательство будет проведено в несколько шагов.

Шаг 1.

Поле $\mathscr{O}/\mathfrak{m}$ совпадает с $\Bbbk$.

Доказательство. Действительно, отображение $\pi\colon \mathscr{O} \to \Bbbk$, $\varphi \mapsto \varphi(P)$ является сюръективным гомоморфизмом колец и $\operatorname{Ker}\pi = \mathfrak{m}$. По теореме о гомоморфизме $\mathscr{O}/\mathfrak{m} = \Bbbk$. □

Шаг 2.

Каждый ненулевой простой идеал в $\mathscr{O}$ совпадает с $\mathfrak{m}$.

Доказательство. Предположим, что $\mathfrak{p}$ – простой идеал такой, что $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$. Возьмем элементы $a \in \mathfrak{p} \setminus (0)$ и $b \in \mathfrak{m} \setminus \mathfrak{p}$. Поскольку степень трансцендентности $\mathbb{K}$ над $\Bbbk$ равна 1, то элементы a и b алгебраически зависимы над $\Bbbk$. Поэтому существует неприводимый многочлен $f(x,y) \in \Bbbk[x,y]$ такой, что $f(a,b) = 0$. Запишем его в виде $f(x,y) = xg(x,y)+h(y)$, где $h(y) = \prod(y-\alpha_i)$, $\alpha_i \in \Bbbk$. Тогда

$$h(b) = \prod(b-\alpha_i) = -ag(a,b) \in \mathfrak{p}.$$

Отсюда $b-\alpha_i \in \mathfrak{p} \subset \mathfrak{m}$ для некоторого i. Так как $b \in \mathfrak{m}$, а $1 \notin \mathfrak{m}$, то $\alpha_i = 0$ и $b \in \mathfrak{p}$. Противоречие. □

Шаг 3.

Для любого ненулевого идеала $\mathfrak{a} \subset \mathscr{O}$ и любого $a \in \mathfrak{m}$ существует $n \in \mathbb{N}$ такое, что $a^n \in \mathfrak{a}$.

Доказательство. Предположим, что $a^n \notin \mathfrak{a}$ для всех $n \in \mathbb{N}$. Рассмотрим множество M всех идеалов $\mathfrak{b} \supset \mathfrak{a}$ таких, что $a^n \notin \mathfrak{b}$ для всех $n \in \mathbb{N}$. Так как $\mathfrak{a} \in M$, то M непусто. Существует максимальный по включению элемент $\mathfrak{p} \in M$. Докажем, что $\mathfrak{p}$ – простой идеал. Пусть $bc \in \mathfrak{p}$, а $b, c \notin \mathfrak{p}$. Тогда идеалы $(b)+\mathfrak{p}$ и $(c)+\mathfrak{p}$ не принадлежат M. Поэтому $a^n \in (b)+\mathfrak{p}$ и $a^m \in (c)+\mathfrak{p}$ для некоторых $n, m \in \mathbb{N}$. Следовательно, $a^{n+m} \in (bc)+\mathfrak{p} = \mathfrak{p}$. Противоречие показывает, что $\mathfrak{p}$ – простой идеал. Но тогда $\mathfrak{p} = \mathfrak{m}$ и $a \in \mathfrak{p}$. □

Шаг 4.

Для любого ненулевого идеала $\mathfrak{a} \subset \mathscr{O}$ имеем $\mathfrak{m}^n \subset \mathfrak{a}$ для некоторого $n \in \mathbb{N}$. В частности, $\cap_n \mathfrak{m}^n = (0)$.

Доказательство. Имеются вложения $\Bbbk[X] \subset \mathscr{O} \subset \Bbbk(X)$, где, как обычно, $\Bbbk[X] = \Bbbk[x_1, x_2]/\mathfrak{I}(X)$ – кольцо регулярных функций на X. Пересечение $\mathfrak{m} \cap \Bbbk[X]$ является идеалом в $\Bbbk[X]$, порожденным координатными функциями $\bar{x}_1, \bar{x}_2$ (т.е. образами элементов $x_1, x_2 \in \Bbbk[x_1, x_2]$). По построению кольца $\mathscr{O} = \mathscr{O}_{P,X}$ любая функция из $\mathfrak{m}$ получается делением некоторого элемента из $\mathfrak{m} \cap \Bbbk[X]$ на ненулевую в начале координат функцию. Поэтому идеал $\mathfrak{m}$ порождается элементами $\bar{x}_1, \bar{x}_2$. Из предыдущего шага имеем $\bar{x}_i^{n_i} \in \mathfrak{a}$ для некоторых $n_1, n_2 \in \mathbb{N}$. Положим $n = n_1 + n_2$. Тогда $\mathfrak{m}^n$ порождается элементами $\bar{x}_1^{d_1} \bar{x}_2^{d_2}$, где $d_2 + d_2 = n$. Следовательно, $\mathfrak{m}^n \subset \mathfrak{a}$. □

Шаг 5.

Докажем, что $\mathfrak{m}$ – главный идеал (т.е. порождается одним элементом).

Доказательство. Возьмем элемент $t \in \mathfrak{m}$ такой, что его образ в $\mathfrak{m}/\mathfrak{m}^2$ – ненулевой. Напомним, что из неособости точки $P \in X$ следует одномерность пространства $\mathfrak{m}/\mathfrak{m}^2$ как векторного пространства над $\Bbbk = \mathscr{O}/\mathfrak{m}$. Тогда $\mathfrak{m} = (t) + \mathfrak{m}^2$. По индукции легко показать, что $\mathfrak{m} = (t) + \mathfrak{m}^n$ для любого $n \in \mathbb{N}$. С другой стороны, согласно предыдущему утверждению, для некоторого n имеем $(t) \supset \mathfrak{m}^n$. Отсюда $\mathfrak{m} = \mathfrak{m}^n$ и $\mathfrak{m} = (t)$. □

Таким образом, $\mathfrak{m} = (t)$ и $\mathfrak{m}^m = (t^m)$.

Шаг 6.

Докажем, что любой ненулевой элемент $a \in \mathfrak{m}$ однозначно представляется в виде $a = t^n u$, где u – обратимый элемент.

Доказательство. Согласно сказанному выше, имеем $a \in \mathfrak{m}^n$, $a \notin \mathfrak{m}^{n+1}$ для некоторого n. С другой стороны, $a \in \mathfrak{m}^n$ тогда и только тогда, когда $a = t^a u$, где u – обратимый элемент. □

Шаг 7.

Пусть теперь v – дискретное нормирование поля $\Bbbk(X)$, неотрицательное на $\mathscr{O}$. Положим $v_0 := v(t)$. Тогда для любого элемента $a = t^n u$ имеем

$$v(a) = v(t^n u) = v(t^n) = nv(t) = nv_0. \tag{3.5.8}$$

С точностью до пропорциональности мы можем считать, что $v_0 = 1$ и тогда нормирование v задается однозначно. Обратно, для любого $v_0 \in \mathbb{N}$ формула (3.5.8) определяет дискретное нормирование. Это доказывает теорему. □

Следствие 3.5.9 *Пусть X – неособая неприводимая проективная алгебраическая кривая над $\Bbbk$. Существует взаимно однозначное соответствие между точками X и дискретными нормированиями поля рациональных функций $\Bbbk(X)$, тривиальными на $\Bbbk$. При этом функция $f \in \mathbb{K}$ регулярна в точке P тогда и только тогда, когда $v_P(f) \geq 0$.*

Рассмотрим теперь простейший пример $X = \mathbb{P}^1$:

Теорема 3.5.10 *Любое нетривиальное нормирование поля рациональных дробей $\Bbbk(x)$, тривиальное на $\Bbbk$, пропорционально нормированию вида* (ii) *или* (iii) *из примера* 3.5.6.

Эта теорема верна для любого поля $\Bbbk$ (необязательно алгебраически замкнутого).

Доказательство. Рассмотрим произвольное нетривиальное нормирование $v\colon \Bbbk(x)^* \to \mathbb{Z}$. Сначала предположим, что v неотрицательно на $\Bbbk[x]$. Тогда существует неприводимый многочлен $p(x)$ такой, что $v(p) > 0$. Любой другой многочлен $f(x)$ запишем в виде $f(x) = g(x)p(x)^s$, где НОД $(p(x), g(x)) = 1$. Тогда существуют многочлены $u_1(x)$ и $u_2(x)$ такие, что $1 = p(x)u_1(x) + g(x)u_2(x)$. Отсюда $0 = v(1) \geq \min(v(p) + v(u_1), v(g) + v(u_2))$. Так как $v(p) > 0$, то согласно нашему предположению $v(g) = v(u_2) = 0$. Отсюда $v(f) = sv(p)$. Ясно, что такое нормирование пропорционально нормированию (ii) из примера 3.5.6.

Теперь предположим, что $v(f) < 0$ для некоторого многочлена $f(x)$. Выберем такой многочлен минимальной степени и пусть $v(f) = -v_0$. Пусть $g(x)$ – любой непостоянный многочлен меньшей степени. Разделим f на g с остатком: $f(x) = g(x)h(x) + r(x)$. Если $r(x) = 0$, то $v(f) = v(g) + v(h) \geq 0$. Противоречие. Поэтому $r(x) \neq 0$ и $v(f) \geq \min(v(g) + v(h), v(r)) \geq 0$. Снова противоречие. Это показывает, что $\deg f(x) = 1$, т.е. $f(x) = x - \alpha$. Но тогда $v(x - \beta) = v(x - \alpha + \alpha - \beta) = v(x - \alpha)$ (см. замечание 3.5.5). Таким образом, $v(x) = -v_0$ и $v(a_k x^k) = -kv_0$ для $a_k \in \Bbbk^*$. Снова согласно замечанию 3.5.5 имеем $v(\sum_{k=0}^{n} a_k x^k) = -nv_0$. С точностью до пропорциональности мы можем положить $v_0 = 1$. Получаем нормирование (iii) из примера 3.5.6. □

Теорема 3.5.11 *Пусть X – неприводимая алгебраическая кривая над полем $\Bbbk = \bar{\Bbbk}$, пусть $\mathbb{K} := \Bbbk(X)$ – ее поле рациональных функций (иначе говоря, $\mathbb{K}/\Bbbk$ – конечно порожденное расширение степени трансцендентности 1). Пусть $f \in \mathbb{K}$, $f \notin \Bbbk$. Тогда*

(i) *существует лишь конечное число нормирований v поля $\mathbb{K}$ тривиальных на $\Bbbk$ и таких, что $v(f) \neq 0$;*

(ii)
$$\sum_v v(f) = 0,$$
где суммирование производится по всем нормированиям поля $\mathbb{K}$, тривиальным на $\Bbbk$.

Мы докажем теорему только для случая $\mathbb{K} = \Bbbk(t)$.

Доказательство. Пусть $\mathbb{K} = \Bbbk(t)$ и пусть $f(t) \in \Bbbk(t)$ – ненулевой элемент. Разложим f в произведение неприводимых множителей: $f(t) = \prod (t - \alpha_i)^{k_i}$, где $k_i \in \mathbb{Z}$. По теореме 3.5.10 любое нормирование v поля $\mathbb{K}$ тривиальное на $\Bbbk$ имеет вид v_∞ или $v = v_{t-\alpha}$ для некоторого $\alpha \in \Bbbk$. По определению

$$v_{t-\alpha}(f) = \begin{cases} k_i & \text{если } \alpha = \alpha_i, \\ 0 & \text{если } \alpha \neq \alpha_i. \end{cases}$$

Ясно, что $v(f)$ отлично от нуля лишь для конечного множества v. Это доказывает (i) Для доказательства (ii) запишем

$$\sum_v v(f) = \sum_\alpha v_{t-\alpha}(f) + v_\infty(f) = \sum k_i - \deg f = 0.$$

□

Упражнения. **(1)** В обозначениях 3.5.1 докажите, что любое промежуточное поле $\Bbbk \subsetneq \mathbb{K}' \subset \mathbb{K}$ также удовлетворяет условиям (i) и (ii).

(2) Докажите аналог предложения 3.5.10 для поля рациональных чисел: любое нетривиальное дискретное нормирование поля $\mathbb{Q}$ пропорционально p-адическому нормированию (теорема Островского).

(3) Докажите, что конечное поле не имеет нетривиальных дискретных нормирований.

(4) Докажите, что алгебраически замкнутое поле не имеет нетривиальных дискретных нормирований.

(5) Пусть $\Bbbk$ – алгебраически замкнутое поле и пусть $\mathbb{K}/\Bbbk$ – конечно порожденное расширение степени трансцендентности 1. Пусть v и v' – два дискретных нормирования поля $\mathbb{K}$, тривиальные на $\Bbbk$. Тогда следующие условия эквивалентны:

(i) v и v' пропорциональны;

(ii) для любого элемента $a \in \mathbb{K}$ из того, что $v(a) \geq 0$ следует, что $v'(a) \geq 0$.

Глава 4.

Эллиптические кривые

Естественным и наиболее важным инвариантом плоской кривой является ее степень. Кривые степени 1 называются *прямыми*. Все они переводятся друг в друга проективными преобразованиями. Кривые степени 2 называются *ониками*. Их свойства подробно изучались в курсе аналитической геометрии. Неособые коники над алгебраически замкнутым полем также могут быть переведены друг в друга проективным преобразованием.

Мы изучим следующий по сложности класс кривых – неособые кубические кривые. Оказывается, что этот случай нетривиален и дает возможность построить очень красивую алгебро-геометрическую и арифметическую теории.

Плоские неособые кубические кривые называются также *эллиптическими кривыми* (на самом деле, этот термин чаще употребляется, когда кривая рассматривается абстрактно, независимо от вложения). Мы постараемся показать, что теория эллиптических кривых доставляет пример глубокой взаимосвязи абстрактной алгебраической геометрии, комплексного анализа и теории чисел. Более полными изложениями данного предмета являются, например, книги [BSS00], [Sil86].

4.1. Гессиан и точки перегиба плоских кривых

Кратности пересечений с прямыми

Пусть $X \subset \mathbb{P}^2$ – проективная кривая, а $L \subset \mathbb{P}^2$ – прямая. Обозначим через $\mathrm{mult}_P(X \cap L)$ кратность пересечения X и L в точке P (см. §3.3). Доказательство следующей леммы оставляется читателю.

Лемма 4.1.1 *Кратность* $\mathrm{mult}_P(X \cap L)$ *не зависит от выбора*

координат и параметризации L.

Определение 4.1.2 Пусть $X \subset \mathbb{P}^2$ – проективная кривая. Неособая точка $P \in X$ называется *точкой перегиба*, если существует прямая L такая, что кратность пересечения $X \cap L$ в точке P строго больше 2.

Гессиан

Пусть $f = f_d(x_0, \ldots, x_n)$ – однородный многочлен степени d. Определим *матрицу Гессе* многочлена f (относительно координат $(x_0, \ldots, x_n)$) формулой

$$H(f) = H(f, \mathbf{x}) = (\partial^2 f / \partial x_i \partial x_j)_{0 \le i,j \le n}$$

и *гессиан* $h(f) = h(f, \mathbf{x})$ как детерминант $h(f) = \det H(f)$.

Лемма 4.1.3 *Пусть $\mathbf{x} = (x_0, \ldots, x_n) \longmapsto \mathbf{x}' = (x'_0, \ldots, x'_n)$ – проективная замена координат с невырожденной матрицей $A = (a_i^j)$. Тогда матрица Гессе преобразуется следующим образом:*

$$H(f, \mathbf{x}') = (A^t) H(f, \mathbf{x}) A.$$

В частности, $h(f, \mathbf{x}') = (\det A)^2 h(f, \mathbf{x})$.

Доказательство. Используя тензорные обозначения, мы можем написать

$$x_i = \sum_{j'} a_i^{j'} x'_{j'}.$$

Отсюда

$$\frac{\partial^2 f}{\partial x'_{i'} \partial x'_{j'}} = \sum_{i,j} \frac{\partial x_i}{\partial x'_{i'}} \frac{\partial^2 f}{\partial x_i \partial x_j} \frac{\partial x_j}{\partial x'_{j'}} = \sum_{i,j} a^i_{i'} \frac{\partial^2 f}{\partial x_i \partial x_j} a^j_{j'},$$

что и доказывает требуемое равенство. □

Гессиан является многочленом степени $(n+1)(d-2)$ от $x_0, \ldots, x_n$. Однако он может обращаться в нуль:

Пример 4.1.4 Для многочлена $f = x^4 + yz^3 + xy^3$ над полем характеристики 2 гессиан равен нулю (см. также упражнение (1), стр. 87).

Предложение 4.1.5 *Пусть $X \subset \mathbb{P}^2$ – кривая степени d над полем $\Bbbk$, характеристика которого не равна 2 и не делит $d-1$. Неособая точка $P \in X$ является точкой перегиба, если и только если гессиан h в точке P обращается в нуль.*

Доказательство. Пусть $P \in X$ – неособая точка и пусть $L := T_{P,X}$. Поместим начало координат в точку P и сделаем прямую L осью Ox. Тогда в аффинной системе координат уравнение X имеет вид

$$y + g(x, y) = 0, \tag{4.1.6}$$

где $g(x, y)$ содержит только члены степени ≥ 2. Рассмотрим разложение Тейлора для g в $(0, 0)$:

$$g = g_2 + g_3 + \cdots .$$

Тогда проективное уравнение X имеет вид

$$f(x_0, x_1, x_2) = x_0^{d-1}x_2 + x_0^{d-2}g_2(x_1, x_2) + x_0^{d-3}g_3(x_1, x_2) + \cdots = 0.$$

Отсюда матрица Гессе в точке $P = (1 : 0 : 0)$ имеет вид

$$H = \begin{pmatrix} 0 & 0 & d-1 \\ 0 & \partial^2 g_2/\partial x_1^2 & \partial^2 g_2/\partial x_1 \partial x_2 \\ d-1 & \partial^2 g_2/\partial x_1 \partial x_2 & \partial^2 g_2/\partial x_2^2 \end{pmatrix}$$

Поскольку $\operatorname{char}\Bbbk$ не делит $d-1$, то $\det H = 0$ тогда и только тогда когда $\partial^2 g_2/\partial x_1^2 = 0$ в точке P. Последнее означает, что в $g_2(x, y)$ отсутствует член x^2, т.е. $g_2(x, y)$ делится на y. (Здесь используется то, что $\operatorname{char}\Bbbk \neq 2$.) Наконец, условие делимости g_3 на y в точности эквивалентно тому, что кратность пересечения прямой L, заданной уравнением $y = 0$, и кривой X, заданной уравнением (4.1.6), больше 2. □

Следствие 4.1.7 *Пусть $X \subset \mathbb{P}^2$ – неособая кривая степени d над полем $\Bbbk$, характеристика которого не равна 2 и не делит $d-1$. Тогда X имеет по крайней мере одну точку перегиба.*

Доказательство. Уравнение $h = 0$ задает на $\mathbb{P}^2$ *кривую Гессе* H степени $3(d-2)$ или $h = 0$ всюду. По теореме Безу пересечение $X \cap H$ непусто. $\square$

Следствие 4.1.8 *Неособая кубическая кривая $E \subset \mathbb{P}^2$ над полем $\Bbbk$, характеристики $\neq 2$ имеет по крайней мере одну точку перегиба.*

Этот факт верен также и для полей характеристики 2, однако доказательство в этом случае использует другие методы (см., например, упражнения (11), стр. 99 и (13), стр. 99). Рассмотрим примеры.

Пример 4.1.9 Пусть характеристика основного поля равна $p > 0$. Гессианом кривой $x_0^{d-1}x_2 + x_0^{d-2}x_1^2 + x_1^d = 0$ будет многочлен $h = -2(d-1)^2 x_0^{3d-6}$. Он тождественно обращается в нуль, если $p = 2$ и если p делит $d-1$. Однако, точка $(1:0:0)$ не является точкой перегиба (проверьте!). Это показывает, что условия $\operatorname{char}\Bbbk \neq 2$ и $\nmid d-1$ в предложении 4.1.5 необходимы.

Пример 4.1.10 Рассмотрим следующую неособую кривую

$$x_0^p x_1 + x_1^p x_2 + x_2^p x_0 = 0 \tag{4.1.11}$$

над полем характеристики $p \geq 3$. Найдем точки перегиба. Для этого перейдем в аффинную карту $x_0 = 1$. Уравнение кривой примет вид $x_1 + x_1^p x_2 + x_2^p = 0$, а уравнение касательной в точке (a, b) – вид $x_1 - a + a^p(x_2 - b) = 0$. Таким образом, точки пересечения находятся из уравнений

$$\begin{cases} x_1 + x_1^p x_2 + x_2^p = 0, \\ x_1 - a + a^p(x_2 - b) = 0. \end{cases}$$

Сделаем замену $x_1 \to x_1 + a$, $x_2 \to x_2 + b$:

$$\begin{cases} x_1 + a + (x_1^p + a^p)(x_2 + b) + x_2^p + b^p = 0, \\ x_1 + a^p x_2 = 0. \end{cases}$$

Учитывая равенство $a + a^p b + b^p = 0$, получим

$$\begin{cases} x_1 + x_1^p x_2 + b x_1^p + a^p x_2 + x_2^p = 0, \\ x_1 + a^p x_2 = 0. \end{cases}$$

Исключим теперь x_1:

$$0 = ((-1)^p a^{p^2} x_2 + (-1)^p b a^{p^2} + 1) x_2^p$$

Поскольку кратность корня $x_2 = 0$ не меньше p, то *каждая точка кривой* (4.1.11) *является точкой перегиба.*

Пример 4.1.12 Пусть $\operatorname{char} \Bbbk$ не делит $d(d-1)$. Гессиан кривой Ферма $x_0^d + x_1^d + x_2^d = 0$ имеет вид $d^3(d-1)^3 x_0^{d-2} x_1^{d-2} x_2^{d-2}$, а точки перегиба находятся из уравнений

$$\begin{cases} x_0 = 0 \\ x_1^d + x_2^d = 0 \end{cases} \qquad \begin{cases} x_1 = 0 \\ x_0^d + x_2^d = 0 \end{cases} \qquad \begin{cases} x_2 = 0 \\ x_0^d + x_1^d = 0 \end{cases}$$

В частности, кривая Гессе может быть приводимой.

Упражнения. **(1)** Докажите, что если характеристика основного поля делит $d-1$, то гессиан обращается в нуль. *Указание.* Воспользуйтесь формулой Эйлера для $\partial f / \partial x_i$.

(2) Найдите все точки перегиба кривой $x_0^2 x_1 + x_1^2 x_2 + x_2^2 x_0 = 0$ над полем характеристики 2.

(3) Найдите координаты всех точек перегиба кубической кривой $x^3 + y^3 + z^3 + axyz = 0$.

(4) Пусть $X \subset \mathbb{P}^3$ – неособая кубическая поверхность. Используя гессиан, докажите, что существует точка $P \in X$, касательная плоскость $T_{P,X}$ которой пересекается с X по кривой, которая или приводима, или имеет в P каспидальную особенность (см. упражнение (4), стр. 92).

4.2. Нормальная форма Вейерштрасса

Напомним, что эллиптической кривой мы называем неприводимую неособую проективную кривую $E \subset \mathbb{P}^2$ степени 3.

Лемма 4.2.1 *Предположим, что неприводимая кубическая кривая $E \subset \mathbb{P}^2$ имеет точку перегиба P. Выберем систему координат $x : y : z$ так, чтобы точкой перегиба была $(0 : 1 : 0)$, а уравнение касательной в этой точке имело вид $z = 0$. Тогда уравнение кривой E в аффинной системе координат x, y будет*

$$x^3 + f(x, y) = 0, \tag{4.2.2}$$

где многочлен f имеет степень 2.

Доказательство. В аффинной системе координат x, z точка P – начало координат. Так как она же является и точкой перегиба, то уравнение E имеет вид $x^3 + zg(x, z) = 0$, где $\deg g \leq 2$. В однородной системе координат это уравнение примет вид $x^3 + zy^2 g(x/y, z/y) = 0$. Отсюда $f(x, y) = y^2 g(x/y, 1/y)$. □

Теорема 4.2.3 *Пусть $E \subset \mathbb{P}^2$ – неприводимая кубическая кривая над (алгебраически замкнутым) полем $\Bbbk$ характеристики $\neq 2$. Предположим, что существует точка перегиба $P \in E$ (согласно следствию 4.1.8 это выполнено, если кривая E неособа). Тогда существует система координат в $\mathbb{P}^2$ такая, что координаты точки P равны $(0 : 1 : 0)$, касательная в этой точке совпадает с бесконечной прямой, а уравнение кривой E имеет вид*

$$y^2 = g(x), \tag{4.2.4}$$

где $g(x)$ – многочлен степени 3. Если $\operatorname{char} \Bbbk \neq 2, 3$, то это уравнение приводится у виду

$$y^2 = x^3 + ax + b. \tag{4.2.5}$$

Доказательство. По лемме 4.2.1 уравнение E приводится к виду (4.2.2). Многочлен $f(x, y)$ должен содержать ay^2, $a \neq 0$, так как в противном случае точка $(0 : 1 : 0)$ была бы особой. Таким образом, $f(x, y) = ay^2 + l(x)y + q(x)$, где $\deg l(x) \leq 1$ и $\deg q(x) \leq 2$. Преобразованием $y \mapsto y - \alpha x - \beta$ уравнение (4.2.2) приводится к виду

$$x^3 + ay^2 + (l(x) - 2a\alpha x - 2a\beta)y + a(\alpha x + \beta)^2 - l(x)(\alpha x + \beta) + q(x) = 0,$$

Так как $\operatorname{char}\Bbbk \neq 2$, то можно найти α и β такие, что

$$l(x) - 2a\alpha x - 2a\beta = 0.$$

Получим уравнение вида $x^3 + ay^2 + q(x) = 0$, которое приводится к виду (4.2.4) (или (4.2.5) если $\operatorname{char}\Bbbk \neq 3$). Если бы при этом многочлен $g(x)$ имел кратный корень α, то дальнейшим преобразованием $x \mapsto x - \alpha$ уравнение приводилось бы к виду $y^2 = x^2(x - \beta)$ и кривая E имела бы в начале координат особую точку. □

Определение 4.2.6 Уравнение (4.2.5) называется (*краткой*) *формой Вейерштрасса* кубической кривой. Числа

$$\Delta := -16(4a^3 + 27b^2), \qquad j(E) := -1728(4a)^3/\Delta$$

называются ее *дискриминантом* и *j-инвариантом* (заметим: $1728 = 2^6 \cdot 3^3$).

Таким образом,

$$j(E) = 4^4 \cdot 27a^3/(4a^3 + 27b^2).$$

Позже, в §4.4 будет показано, что j-инвариант кубической кривой действительно является ее инвариантом, т.е., он не зависит от способа приведения к форме Вейерштрасса.

Пусть $\Bbbk \subsetneq \bar{\Bbbk}$. Говорят, что кривая $E \subset \mathbb{P}^2$ *определена* над $\Bbbk$, если она может быть задана многочленом с коэффициентами из $\Bbbk$. Если кривая вида (4.2.5) определена над $\Bbbk$, то, очевидно, ее j-инвариант принадлежит $\Bbbk$. Обратно, для любого $j \in \Bbbk$ существует неособая кривая E вида (4.2.5) определенная над $\Bbbk$ с $j(E) = j$. Действительно, при $j \neq 0$ можно положить $a = b$. Тогда $j(4a + 27) = 6912a$ и

$$a = b = \frac{729}{16}\frac{j^2}{(1728 - j)^2}.$$

Нарисуем вещественную (определенную над $\mathbb{R}$) кривую, заданную уравнением $y^2 = x^3 - x$:

Однако, этот вид "не совсем правильный", поскольку изображены только вещественные точки. Мы изучаем кривые над алгебраически замкнутыми полями и нам следовало бы рисовать кривую над $\mathbb{C}$, что довольно затруднительно. Комплексные же точки любой кривой образуют связное множество, что не соответствует нашему рисунку. Знак дискриминанта вещественной (т.е. определенной над $\mathbb{R}$) кривой E, заданной уравнением (4.2.5), совпадает со знаком дискриминанта многочлена $x^3 + ax + b$. Это показывает, что пересечение E с осью x состоит из трех (действительных) точек если $\Delta > 0$ и из одной точки если $\Delta < 0$. Отсюда можно вывести, что число компонент связности множества вещественных точек E определяется ее дискриминантом: их две если $\Delta > 0$ и ровно одна если $\Delta < 0$.

Теорема 4.2.3 не верна в характеристике 2: кривая (4.2.4) всегда особа, в то время как существуют неособые кубические кривые. Согласно лемме 4.2.1, над любым алгебраически замкнутым полем уравнение неособой кубической кривой может быть записано в *обобщенной форме Вейерштрасса*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.2.7}$$

Определим числа

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \tag{4.2.8}$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Тогда дискриминант и j-инвариант определяются следующим образом:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j(E) = c_4^3/\Delta. \tag{4.2.9}$$

Заметим однако, что формулы (4.2.9) имеет смысл писать только если $\operatorname{char}\Bbbk = 2$ и 3. В этом случае они допускают упрощение, см. упражнения (1) и (2), стр. 102. Отметим также, что при $\operatorname{char}\Bbbk \neq 2\,3$ мы имеем

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

Кривые вида (4.2.7) могут быть особыми, однако это случается "довольно редко":

Предложение 4.2.10 *Кривая* (4.2.7) *особа тогда и только тогда, когда* $\Delta = 0$.

Доказательство. Докажем это в случае, когда $\operatorname{char}\Bbbk \neq 2, 3$ и кривая может быть записана в краткой форме Вейерштрасса (4.2.5) (общий случай отличается лишь сложностью вычислений). Эта кривая всегда неособа на бесконечности и особа в конечной аффинной карте тогда и только тогда, когда многочлен x^3+ax+b имеет кратный корень (см. упражнение (5), стр. 64). Последнее эквивалентно тому, что система

$$\begin{aligned} x^3 + ax + b &= 0, \\ 3x^2 + a &= 0. \end{aligned}$$

имеет решение. Если $a = 0$, то кривая будет особа тогда и только тогда, когда $b = 0$, что эквивалентно $\Delta = 0$. Пусть $a \neq 0$. Единственным решением системы может быть $x = -3b/(2a)$.

Подставляя это во второе уравнение, получим $-1/4(27b^2 + 4a^3)/a^2 = 0$, что опять эквивалентно $\Delta = 0$. $\square$

Упражнения. **(1)** Найдите нормальную форму Вейерштрасса кубической кривой Ферма $x^3+y^3+z^3 = 0$. Вычислите ее j-инвариант.

(2) Постройте эллиптическую кривую с j-инвариантом $j = 7$.

(3) ($\operatorname{char}\Bbbk \neq 2, 3$) Особая точка $P = (a, b)$ плоской кривой X, заданной уравнением $f(x, y) = 0$, называется *обыкновенной*, если в разложении Тейлора

$$f(x, y) = f_1(x - a, y - b) + f_2(x - a, y - b) + \cdots$$

квадратичная форма $f_2(\xi_1, \xi_2)$ невырождена. Докажите, что неприводимая кубическая кривая, имеющая обыкновенную особую точку, имеет три точки перегиба, лежащие на одной прямой. Ее уравнение может быть приведено к виду $y^2 = x^2(x+1)$ (*декартов лист*, см. рис 4.1).

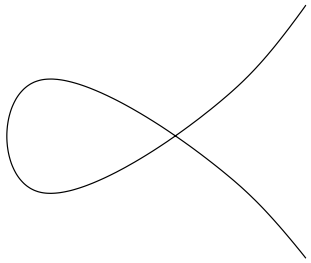


Рис. 4.1 Декартов лист

(4) ($\operatorname{char}\Bbbk \neq 2, 3$) Говорят, что кубическая кривая имеет *каспидальную особую точку* (точку возврата), если в разложении Тейлора ранг квадратичной формы $f_2(\xi_1, \xi_2)$ равен 1. (Для кривых произвольной степени это определение следует формулировать иначе.) Докажите, что неприводимая кубическая кривая с каспидальной особой точкой имеет одну точку перегиба. Ее уравнение можно привести к виду $y^2 = x^3$ (*полукубическая парабола*, см. рис 4.2).

(5) Пусть $E \subset \mathbb{P}^2$ – неособая кубическая кривая. Докажите, что через каждую точку $P \in \mathbb{P}^2$ проходит лишь конечное число касательных к E.

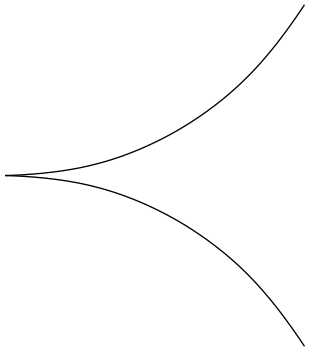


Рис. 4.2 Полукубическая парабола

4.3. Точки перегиба кубических кривых

Кривая Гессе H плоской кубической кривой E имеет степень 9. По теореме Безу пересечение $H \cap E$ состоит из не более чем девяти точек (если $H \neq E$). Мы докажем, что это пересечение состоит ровно из девяти точек (если $\operatorname{char}\Bbbk \neq 3$). Более того, конфигурация этих точек обладает интересными свойствами:

Теорема 4.3.1 *Неособая кубическая кривая над полем $\Bbbk$ характеристики $\neq 2, 3$ имеет ровно девять точек перегиба. Любая прямая, соединяющая две из этих точек, обязательно проходит через третью.*

Замечание 4.3.2 В случаях $\operatorname{char}\Bbbk = 2$ и 3 точки перегиба описаны в упражнениях (11), стр. 99 и (4), стр. 98.

Доказательство. Запишем уравнение (4.2.5) в виде

$$f = y^2 - x^3 - ax - b = 0,$$

где $4a^3+27b^2 \neq 0$, так как многочлен x^3+ax+b имеет лишь простые корни. Непосредственным вычислением получим гессиан кривой

$$h = 8(3ax^2 + 9bx + 3xy^2 - a^2).$$

Исключив y^2 из f и h, получим

$$g(x) := 3x^4 + 6ax^2 + 12bx - a^2 = 0. \qquad (4.3.3)$$

Производная последнего многочлена равна $g'(x) = 12(x^3 + ax + b)$. Применим алгоритм Евклида к g и g':

$$g(x) = 3x(x^3 + ax + b) + 3ax^2 + 9bx - a^2,$$

$$3a^2(x^3 + ax + b) = (ax - 3b)(3ax^2 + 9bx - a^2) + (4a^3 + 27b^2)x$$

Отсюда немедленно получаем, что многочлены g, g' взаимно просты. Следовательно, уравнение $g(x) = 0$ имеет четыре различных корня. Для каждого из указанных корней найдутся два различных значения y, так как ни одно из полученных значений x не удовлетворяет уравнению $x^3 + ax + b = g'(x)/12 = 0$. Так как мы имели с самого начала одну точку перегиба в бесконечности, то всего получается девять точек перегиба. Второе утверждение теоремы теперь получается непосредственно, так как из любых двух таких точек одна может быть принята за $(0 : 1 : 0)$, другая – за $(\alpha : \beta : 1)$. Но в таком случае точка $(\alpha : -\beta : 1)$ также является точкой перегиба и эти точки лежат на одной прямой. □

Пусть $P_1, \ldots, P_9$ – точки перегиба кубической кривой $E \subset \mathbb{P}^2$. Из доказательства теоремы 4.3.1 следует, что диагональное проективное преобразование $\mathrm{Diag}(1, -1, 1)$ переводит кривую E в себя, оставляет на месте бесконечную точку перегиба и попарно переставляет остальные. Поскольку за бесконечную точку перегиба мы можем принять любую из $P_1, \ldots, P_9$, то мы получаем девять таких инволюций (элементов второго порядка) $\tau_1, \ldots, \tau_9$. Обозначим через $\mathrm{Aut}_{\mathbb{P}}(E)$ группу проективных преобразований (т.е. подгруппу $PGL(3, \Bbbk)$), переводящую кривую E в себя, а через $\mathrm{Aut}'_{\mathbb{P}}(E)$ – подгруппу в $\mathrm{Aut}_{\mathbb{P}}(E)$, порожденную инволюциями τ_i. Поскольку $\mathrm{Aut}_{\mathbb{P}}(E)$ переводит точки перегиба в точки перегиба, то она действует на множестве $\{P_1, \ldots, P_9\}$. Это действие эффективно (т.е. соответствующий гомоморфизм $\mathrm{Aut}_{\mathbb{P}}(E) \to S_9$) инъективен. Действительно, любое проективное преобразование $\mathbb{P}^2$ однозначно задается образами четырех точек, никакие три из которых не лежат на одной прямой. Ясно,

что среди точек $P_1, \ldots, P_9$ можно выбрать такую конфигурацию. Поэтому элемент $\phi \in \mathrm{Aut}_{\mathbb{P}}(E)$, оставляющий на месте все точки P_i, должен быть тривиален. Группа $\mathrm{Aut}_{\mathbb{P}}(E)$ зависит от кривой E (от ее j-инварианта). Она будет изучена позже. Сейчас мы опишем лишь подгруппу $\mathrm{Aut}'_{\mathbb{P}}(E)$.

Предложение 4.3.4 *Группа $\mathrm{Aut}'_{\mathbb{P}}(E)$ транзитивно действует на множестве точек перегиба $\{P_1, \ldots, P_9\}$ и имеет порядок 18. Более того, $\mathrm{Aut}'_{\mathbb{P}}(E)$ является полупрямым произведением инволюции и подгруппы, изоморфной $(\mathbb{F}_3)^2$.*

Доказательство. Пусть $O \subset \{P_1, \ldots, P_9\}$ – орбита некоторой точки и предположим, что $O \neq \{P_1, \ldots, P_9\}$. Если $P_i \notin O$, то O разбивается на пары, попарно переставляемых инволюцией τ_i точек. Поэтому в O – четное число элементов. Аналогично, если $P_i \in O$, то $O \setminus \{P_i\}$ разбивается на пары, попарно переставляемых точек. Поэтому в O – нечетное число элементов. Противоречие показывает, что $O = \{P_1, \ldots, P_9\}$. Далее, так как стабилизатор каждой точки P_i содержит инволюцию τ_i, то по формуле для числа элементов в орбите имеем $|\mathrm{Aut}'_{\mathbb{P}}(E)| \geq 2 \cdot 9 = 18$.

Для того, чтобы оценить сверху порядок группы $\mathrm{Aut}'_{\mathbb{P}}(E)$ и описать ее структуру мы воспользуемся терминологией конечных аффинных геометрий.

Определение 4.3.5 *Абстрактной аффинной плоскостью Λ_q* порядка q называется множество, элементы которого называются точками и на котором задана система подмножеств называемых прямыми, такое, что выполнена следующая система аксиом:

A1. Через любые две различные точки проходит ровно одна прямая.

A2. Для каждой прямой L и точки $P \notin L$ существует одна и только одна прямая, проходящая через P и параллельная L (т.е. не пересекающая L).

A3. Существует треугольник (три точки, не лежащие на одной прямой).

A4. Существует прямая, состоящая из q ($q > 1$) точек.

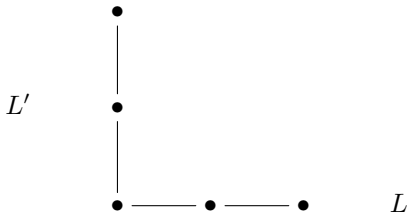
Примером такой плоскости является аффинное пространство $\mathbb{A}^2_{\mathbb{F}_q}$ над конечным полем $\mathbb{F}_q$. Из аксиом A1-A4 непосредственно выводится следующая.

Лемма 4.3.6 *Пусть Λ_q – абстрактная аффинная плоскость порядка q. Тогда Λ_q содержит ровно q^2 точек и q^2+q прямых. На каждой прямой лежит ровно q точек и через каждую точку проходит ровно $q+1$ прямая.*

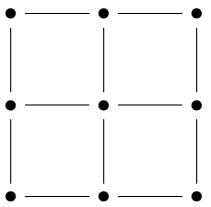
Нас интересует только одна абстрактная аффинная плоскость – плоскость порядка 3.

Лемма 4.3.7 *Абстрактная аффинная плоскость Λ_3 порядка 3 единственна с точностью до изоморфизма и поэтому изоморфна $\mathbb{A}^2_{\mathbb{F}_3}$.*

Идея доказательства. Из аксиомы A4 и леммы 4.3.6 получаем, что Λ_3 содержит следующую конфигурацию точек и прямых:



Проведем прямые параллельные L и L'. Получим



Каждая из оставшихся шести прямых проходит через точки, лежащие в разных строках и разных столбцах. Через каждую

пару таких точек проходит ровно одна прямая и третья ее точка определяется парой однозначно. Таким образом, мы полностью восстановим разбиение на тройки коллинеарных точек. Это доказывает лемму. □

Вернемся к доказательству предложения 4.3.4. Пусть $P_1, \dots, P_9$ – точки перегиба неособой кубической кривой $E \subset \mathbb{P}^2$. Рассмотрим абстрактную аффинную плоскость Λ_3, точками которой являются $P_1, \dots, P_9$, а прямыми – тройки точек, лежащих на одной прямой в $\mathbb{P}^2$. Утверждения аксиом A1-A4 немедленно следуют из теоремы 4.3.1. Поскольку $\mathrm{Aut}_{\mathbb{P}}(E)$ переводит точки перегиба в точки перегиба и сохраняет коллинеарность, то существует естественный гомоморфизм $\Phi\colon \mathrm{Aut}_{\mathbb{P}}(E) \to GA(\Lambda_3)$ в группу аффинных преобразований плоскости Λ_3. При этом образ каждой инволюции τ_i является отражением: $\Phi(\tau_i)(P_j) = P_i - \overrightarrow{P_iP_j}$.

Напомним, как устроена группа аффинных преобразований $GA(\Lambda_3)$. Если мы зафиксируем точку $P = P_i$ (начало координат), то любое преобразование $\phi \in GA(\Lambda_3)$ раскладывается в композицию $\phi = \phi_P \circ \psi$ параллельного переноса ψ и аффинного преобразования ϕ_P, оставляющего точку P на месте. Подгруппа всех параллельных переносов $\mathrm{Tran}(\Lambda_3)$ нормальна в $GA(\Lambda_3)$ и изоморфна $(\mathbb{F}_3)^3$, а подгруппа аффинных преобразований с неподвижной точкой изоморфна группе $GL(2, \mathbb{F}_3)$ невырожденных матриц. Таким образом, имеется гомоморфизм $\Psi\colon GA(\Lambda_3) \to GL(2, \mathbb{F}_3)$ с ядром $\mathrm{Tran}(\Lambda_3) \simeq (\mathbb{F}_3)^3$. В частности, порядок группы $GA(\Lambda_3)$ равен $9 \cdot (9-1) \cdot (9-3) = 432$. Теперь заметим, что для каждой инволюции τ_i ее образ $\Psi \circ \Phi(\tau_i)$ – скалярная матрица $-\mathcal{E}$. Поэтому $\Psi \circ \Phi(\mathrm{Aut}'_{\mathbb{P}}(E)) = \{\pm\mathcal{E}\}$ и

$$|\mathrm{Aut}'_{\mathbb{P}}(E)| = 2 \cdot |\mathrm{Ker}(\Psi \circ \Phi) \cap \mathrm{Aut}'_{\mathbb{P}}(E)| = 2 \cdot |\mathrm{Tran}(\Lambda_3) \cap \Phi(\mathrm{Aut}'_{\mathbb{P}}(E))|.$$

Отсюда немедленно получаем, что $|\mathrm{Aut}'_{\mathbb{P}}(E)| \leq 2|\mathrm{Tran}(\Lambda_3)| = 18$. Последнее утверждение предложения теперь очевидно и оставляется читателю для самостоятельного разбора. □

Упражнения. **(1)** Найдите координаты точек перегиба кривой Ферма $x^3 + y^3 = z^3$.

(2) Докажите, что неособая кубическая кривая $E \subset \mathbb{P}^2$, определенная над $\mathbb{R}$, имеет действительную точку перегиба. Выведите отсюда,

что в некоторой системе координат E может быть задана уравнением Вейерштрасса (4.2.5) с действительными a и b.

(3) Вычислите дискриминант уравнения (4.3.3) и сравните его с дискриминантом соответствующей кубической кривой. Выведите отсюда, что кубическая кривая, определенная над $\mathbb{R}$, не может иметь девять точек перегиба. Приведите примеры вещественных кривых с пятью точками перегиба.

(4) Докажите, что кривая $y^2 = x^3 + cx^2 + ax + b$ над полем характеристики 3 имеет ровно три точки перегиба при $c \neq 0$ и единственную точку перегиба (на бесконечности) при $c = 0$.

(5) Пусть $E \subset \mathbb{P}^2$ – неособая кубическая кривая над полем характеристики $\neq 2, 3$. Докажите, что ее кривая Гессе H неособа при $j(E) \neq 0$ и приводима при $j(E) = 0$. Как связаны j-инварианты E и H?

(6) ($\operatorname{char}\Bbbk \neq 2, 3$) Покажите, что точки перегиба неособой кубической кривой, после надлежащего выбора координат, можно записать в виде

$$\begin{array}{lll} (0:1:-1) & (-1:0:1) & (1:-1:0) \\ (0:1:\alpha_1) & (\alpha_1:0:1) & (1:\alpha_1:0) \\ (0:1:\alpha_2) & (\alpha_2:0:1) & (1:\alpha_2:0) \end{array} \tag{4.3.8}$$

где α_1 и α_2 – корни уравнения $x^2 - x + 1 = 0$.

(7) ($\operatorname{char}\Bbbk \neq 2, 3$) Любая кубическая кривая, проходящая через точки (4.3.8), определяется уравнением

$$x^3 + y^3 + z^3 + 3axyz = 0.$$

Докажите, что эта кривая имеет особую точку только тогда, когда a принимает одно из значений ∞, -1, α_1, α_2 и когда кривая распадается на три прямые. Если кривая неприводима, то она имеет девять точек (4.3.8) своими точками перегиба. Найдите зависимость j-инварианта от параметра a.

(8) ($\operatorname{char}\Bbbk \neq 2, 3$) Пусть Γ – подгруппа $PGL(3, \Bbbk)$, переводящая в себя множество точек перегиба неособой кубической кривой (но необязательно саму кривую). Докажите, что $\Psi \circ \Phi(\Gamma) = SL(2, \mathbb{F}_3)$. Поэтому порядок Γ равен 216. Группа Γ называется *группой Гессе*, а конфигурация точек (4.3.8) – *конфигурацией Гессе*.

(9) Если F – неособая кубическая кривая и H – ее кривая Гессе, то каждая кубическая кривая вида $aF + bH$, кроме четырех исключительных, является также неособой и имеющей те же точки перегиба, что и F.

В следующих двух задачах мы предполагаем, что основное поле $\Bbbk$ имеет характеристику 2.

(10) Докажите, что кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.3.9}$$

(см. (4.2.7)), является особой тогда и только тогда, когда

$$a_1^6a_6 + a_1^5a_4a_3 + a_1^4a_4^2 + a_1^4a_3^2a_2 + a_1^3a_3^3 + a_3^4 = 0, \tag{4.3.10}$$

что эквивалентно $\Delta = 0$.

(11) Докажите, что неособая кривая вида (4.3.9) имеет ровно 9 точек перегиба.

(12) Докажите, что неособая кубическая кривая над полем *любой* характеристики не может иметь бесконечного числа точек перегиба.

Следующая задача дает другое, верное в произвольной характеристике, доказательство следствия 4.1.8. Однако для этого потребуются дополнительные знания из алгебраической геометрии. Неподготовленный читатель может пропустить это упражнение.

(13) Отождествим множество всех неособых кубик в $\mathbb{P}^2$ с открытым по Зарисскому подмножеством $U \subset \mathbb{P}^9$, а множество всех прямых на $\mathbb{P}^2$ – с двойственной проективной плоскостью $\mathbb{P}^{2^*}$. Покажите, что множества

$$Y := \left\{(L, P) \in \mathbb{P}^{2^*} \times \mathbb{P}^2 \mid P \in L\right\},$$
$$Z := \left\{(E, L, P) \in U \times \mathbb{P}^{2^*} \times \mathbb{P}^2 \mid \operatorname{mult}_P E \cap L \geq 3\right\}$$

замкнуты по Зарисскому в $\mathbb{P}^{2^*} \times \mathbb{P}^2$ и $U \times \mathbb{P}^{2^*} \times \mathbb{P}^2$, соответственно и $\dim Y = 3$. Далее покажите, что прообраз точки $(L, P) \in Y$ при проекции $Z \to Y$ также замкнут и имеет размерность 6. Выведите отсюда, что $\dim Z = 9$. Воспользуйтесь результатом предыдущей задачи и докажите, что неособая кубическая кривая над полем любой характеристики имеет точку перегиба, а если характеристика основного поля не равна 3, этих точек – ровно девять. (В этом рассуждении существенно то, что проекция $Z \to U$ – *собственный* морфизм.)

4.4. j-инвариант

Запись кубической кривой в форме Вейерштрасса не является единственной. Естественным образом возникает вопрос о нахождении всех значений параметров a и b в (4.2.5), при которых соответствующие кривые могут быть переведены друг в друга проективным преобразованием плоскости. Напомним, что j-инвариант кривой вида

$$y^2 = x^3 + ax + b \tag{4.4.1}$$

вычисляется по формуле

$$j = \frac{4^4 \cdot 27a^3}{4a^3 + 27b^2}.$$

Теорема 4.4.2 *Две кривые, заданные уравнениями вида* (4.2.7)*, переводятся друг в друга проективным преобразованием тогда и только тогда, когда их j-инварианты совпадают.*

Таким образом, j-инвариант является инвариантом кривой и не зависит от способа приведения кривой к вейерштрассовой форме.

Доказательство. Докажем теорему для случая $\mathrm{char} \neq 2, 3$. Тогда в некоторой системе координат уравнение кривых имеет вид (4.4.1). Диагональное преобразование

$$x \to \alpha x, \quad y \to \beta y, \quad \text{где} \quad \alpha^3 = \beta^2 \neq 0 \tag{4.4.3}$$

переводит кривую $y^2 = x^3 + ax + b$ в кривую $y^2 = x^3 + a'x + b'$, где $a' = a\alpha/\beta^2$, $b' = b/\beta^2$.

Пусть кривые E и E' заданы уравнениями

$$y^2 = x^3 + ax + b, \qquad y^2 = x^3 + a'x + b'$$

и предположим, что $j(E) = j(E')$. Если $a = 0$, то $a' = 0$ и мы можем воспользоваться преобразованием (4.4.3) с $\beta^2 = b/b'$. Пусть $a \neq 0$. Тогда $a' \neq 0$ и

$$4 + 27b^2/a^3 = (4a^3 + 27b^2)/a^3 = (4a'^3 + 27b'^2)/a'^3 = 4 + 27b'^2/a'^3.$$

Отсюда $b^2/a^3 = b'^2/a'^3$. Преобразование (4.4.3) с $\beta^2 = b/b'$, $\alpha = a'\beta^2/a$ переводит E в E'.

Наоборот, предположим, что кривая E переводится в E' некоторым проективным преобразованием, которое в аффинных координатах записывается в виде

$$\Phi\colon x \to \frac{p_1x + q_1y + r_1}{p_0x + q_0y + r_0}, \quad y \to \frac{p_2x + q_2y + r_2}{p_0x + q_0y + r_0}.$$

Точка перегиба $P_0 = (0:1:0)$ кривой E переходит в точку перегиба P_0' кривой E'. Рассматривая композицию Φ с проективным автоморфизмом, переставляющим точки перегиба кривой E', мы можем считать, что $\Phi(P_0) = P_0$. Так как касательные кривые в точке P_0 к E и к E' совпадают с бесконечно удаленной прямой, то Φ переводит бесконечно удаленную прямую в себя и поэтому является аффинным преобразованием:

$$\Phi\colon x \to p_1x + q_1y + r_1, \quad y \to p_2x + q_2y + r_2.$$

Так как $\Phi(P_0) = P_0$, то $q_1 = 0$. Теперь видно, что $\Phi(E)$ задается уравнением

$$(p_2x + q_2y + r_2)^2 = (p_1x + r_1)^3 + a(p_1x + r_1) + b,$$

которое должно иметь вейерштрассову форму. Отсюда $p_2 = r_2 = r_1 = 0$, т.е. Φ имеет диагональный вид

$$\Phi\colon x \to p_1x, \quad y \to q_2y,$$

а $\Phi(E)$ – вид

$$(q_2y)^2 = (p_1x)^3 + ap_1x + b,$$

Заменяя y на $q_2/\sqrt{p_1^3}y$ получим

$$y^2 = x^3 + a'x + b', \quad \text{где} \quad a' = a/p_1^2,\ b' = b/p_1^3.$$

Таким образом, j-инвариант новой кривой будет

$$j' = 4^4 \cdot 27a'^3/(4a'^3 + 27b'^2) = 4^4 \cdot 27a^3/(4a^3 + 27b^2) = j.$$

□

Пример 4.4.4 Кривая $y^2 = x^3 - x$ является неособой над произвольным полем $\Bbbk$, $\operatorname{char}\Bbbk \neq 2$. Для нее $a = -1$, $b = 0$, и, следовательно, $\Delta = 64$, $j(E) = 1728$.

Пример 4.4.5 Кривая Ферма $x^3 + y^3 = z^3$ неособа над любым полем $\Bbbk$, $\operatorname{char}\Bbbk \neq 3$. Сделав замену $z := z' + y$ и положив $z' = -1/3$. получаем

$$y^2 - \frac{1}{3}y + x^3 + \frac{1}{27} = 0$$

Далее заменой $y = y' + 1/6$ добиваемся того, что уравнение принимает вид $y^2 + x^3 + 1/108 = 0$. Для него $a = 0$, $b = 1/108$ Следовательно, $\Delta = -1/27$ и $j(E) = 0$.

Упражнения. **(1)** Докажите, что в случае $\operatorname{char}\Bbbk = 2$ уравнение (4.2.7) можно линейной заменой координат привести к одной из следующих форм

$$y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{или} \quad y^2 + a_1 xy = x^3 + a_2 x^2 + a_6.$$

Найдите выражение j-инварианта через a_i в этих случаях (см. (4.2.9)).

(2) Пусть неособая кубическая кривая над полем характеристики 3 задана уравнением $y^2 = g(x)$ (см. (4.2.4)). Найдите выражение j-инварианта через коэффициенты многочлена $g(x)$.

(3) Уравнение Вейерштрасса (4.2.4) (в случае $\operatorname{char}\Bbbk \neq 2$) может быть переписано в следующем виде

$$y^2 = x(x-1)(x-\lambda),$$

который называется *формой Лежандра*. Найдите выражение j-инварианта через λ.

(4) Пусть $E \subset \mathbb{P}^2$ – неособая кубическая кривая над полем характеристики $\neq 2, 3$. Возьмем точку $P \in E$ и рассмотрим проекцию из P на некоторую прямую $L \not\ni P$. Докажите, что существует ровно четыре различные точки $P_1, \ldots, P_4 \in E$, для которых прямые PP_i касаются E (будем считать, что P не является точкой перегиба). Образы $\pi(P_i)$ этих точек из P на $L = \mathbb{P}^1$ называются *точками ветвления* проекции π. Пусть δ – двойное отношение $(\pi(P_1), \pi(P_2); \pi(P_3), \pi(P_4))$ точек ветвления на $\mathbb{P}^1$. Докажите, что число

$$\gamma := \frac{(\delta^2 - \delta + 1)^3}{\delta^2(\delta - 1)^2}.$$

не зависит от выбора P и отличается от j-инварианта E постоянным, не зависящим от E и P, множителем.

4.5. Групповой закон на эллиптической кривой

Определение 4.5.1 Групповой закон на эллиптической кривой. Пусть $E \subset \mathbb{P}^2$ – неособая кубическая кривая. Зафиксируем точку $O \in E$. Определим сложение точек на E следующим образом. Прямую, проходящую через (различные) точки $P_1, \ldots, P_r \in \mathbb{P}^2$, $r \geq 2$ мы будем обозначать через $L_{P_1,\ldots,P_r}$ (если такая прямая существует). Для любой точки $R \in E$ обозначим через $\bar{R}$ третью точку пересечения прямой $L_{O,R}$ и E. Мы учитываем точки пересечения с кратностями, поэтому для $R = O$ мы положим $L_{O,O} = T_{O,E}$. Пусть $R \in E$ – третья точка пересечения прямой PQ и E. Положим $P + Q := \bar{R}$ (см. рис. 4.3).

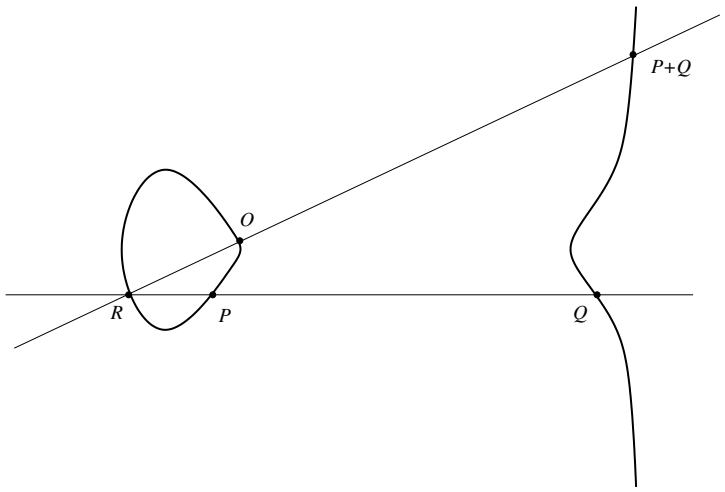


Рис. 4.3 Сложение точек на эллиптической кривой

Отметим, что наша конструкция сложения зависит от выбора начальной точки O. Чтобы выделить эту точку, неособая кубическая (= эллиптическая) кривая с фиксированным групповым законом часто обозначается (E, O).

Теорема 4.5.2 *Описанная конструкция задает на E структуру абелевой группы, где нулем является O, а противоположным элементом к точке $P \in E$ – третья точка пересечения прямой $P\bar{O}$ с E.*

Прежде чем приступать с доказательству теоремы мы приведем некоторые вспомогательные утверждения.

Предложение 4.5.3 (Упрощенный групповой закон) *Если O – точка перегиба, то $\bar{O} = O$ и поэтому*

(i) *для любой точки $P \in E$ точка $-P$ – это третья точка пересечения прямой OP с E;*

(ii) *для любых трех точек $P, Q, R \in E$ равенство $P+Q+R = 0$ имеет место тогда и только тогда, когда эти точки лежат на одной прямой.*

Доказательство. Очевидная переформулировка определения 4.5.1. □

Лемма 4.5.4 *Пусть O – точка перегиба. Предположим, что (E, O) – группа. Тогда для любой точки $O_1 \in E$ (E, O_1) также будет группой, изоморфной (E, O_1). Изоморфизм $(E, O) \simeq (E, O_1)$ задается по правилу $\phi(P) = P + O_1$, где знак "+" понимается как сложение в группе (E, O).*

Доказательство. Обозначим через $\dot{+}$ сложение в смысле группового закона (E, O_1). Достаточно доказать, что $\phi(P + Q) = \phi(P) \dot{+} \phi(Q)$, т.е. $(P+Q)+O_1 = (P+O_1) \dot{+} (Q+O_1)$. Пусть R – третья точка пересечения прямой $L_{P+O_1, Q+O_1}$ с E. Тогда требуемое равенство эквивалентно тому, что точки $(P+Q)+O_1$, R и O_1 лежат на одной прямой, а согласно упрощенному групповому закону оно эквивалентно равенству $(P+Q)+O_1+R+O_1 = 0$ в

(E, O). Если (E, O) – группа, то это выполнено по конструкции точки R. $\square$

Обозначим через $\mathcal{R}_d$ множество однородных многочленов степени d от трех переменных. Легко видеть, что $\mathcal{R}_d$ является векторным пространством размерности $\frac{1}{2}(d+1)(d+2)$. Для различных точек $P_1, \ldots, P_m$ обозначим

$$\mathcal{R}_d(P_1, \ldots, P_m) := \{f \in \mathcal{R}_d \mid f(P_i) = 0, \quad \forall i = 1, \ldots, m\}.$$

Каждое условие $f(P_i) = 0$ задает одно линейное соотношение на коэффициенты f. Следовательно, $\mathcal{R}_d(P_1, \ldots, P_m)$ – также векторное пространство размерности $\geq \frac{1}{2}(d+1)(d+2) - m$. В частности,

$$\dim \mathcal{R}_2(P_1, \ldots, P_5) \geq 1, \quad \dim \mathcal{R}_3(P_1, \ldots, P_9) \geq 1 \qquad (4.5.5)$$

для любых различных P_i.

Лемма 4.5.6 (лемма о кубических кривых) *Пусть X и Y – две (необязательно неприводимые) кубические кривые такие, что $X \cap Y = \{P_1, \ldots, P_9\}$, где все P_i различны. Тогда любая кубическая кривая Z, проходящая через $P_1, \ldots, P_8$, проходит также и через P_9.*

Доказательство. Пусть кривые X, Y и Z задаются кубическими многочленами f, g и h, соответственно. Предположим, что $P_9 \notin Z$. Тогда многочлены f, g и h линейно независимы. Тогда для любых двух различных точек $P', P'' \in \mathbb{P}^2$ можно взять $\alpha, \beta, \gamma \in \Bbbk$ так, чтобы кривая, заданная многочленом $\alpha f + \beta g + \gamma h$, проходила через P' и P''. Действительно, линейная оболочка f, g и h в $\mathcal{R}_3$ – трехмерное подпространство, которое должно нетривиально пересекаться с подпространством $\mathcal{R}_3(P', P'')$ размерности ≥ 8.

Заметим, что никакие четыре из девяти точек P_i не могут лежать на одной прямой, так как эта прямая была бы общей компонентой X и Y. По аналогичной причине никакие семь из точек P_i не могут лежать на кривой второй степени (конике).

Рассмотрим случаи.

1. Точки P_1, P_2, P_3 лежат на прямой L. Из (4.5.5) следует, что существует кривая Q степени 2, проходящая через пять точек $P_4, \ldots, P_8$. Но эти пять точек расположены на однозначно определенной конике. Действительно, если две различные коники имеют пять общих точек, то они имеют общую компоненту. Другие их компоненты являются прямыми и могут иметь лишь одну точку пересечения, не лежащую на общей прямой. Отсюда следует, что остальные четыре точки лежат на прямой, а это невозможно. Пусть теперь P' – точка прямой L, отличная от P_1, P_2, P_3 и P'' – точка, не лежащая ни на L, ни на Q. Если α, β, γ выбраны так, что кривая заданная многочленом $\alpha f + \beta g + \gamma h$, всегда проходящая через $P_1, \ldots, P_8$, проходит также через P' и P'', то эта кривая должна иметь прямую L своей компонентой. Другой компонентой должна быть кривая Q. Но это невозможно, так как L и Q не содержат точки P''.

2. Точки $P_1, \ldots, P_6$ лежат на конике Q. Пусть $L = L_{P_7 P_8}$ – прямая, проходящая через точки P_7 и P_8. Беря в качестве точки P' любую из других точек кривой Q, а в качестве P'' – точку, не лежащую ни на Q, ни на L, приходим к противоречию тем же путем, что и выше.

3. Никакие три из точек $P_1, \ldots, P_8$ не лежат на прямой и никакие шесть – на конике. Возьмем в качестве L прямую L_{P_1,P_2}, а в качестве Q – конику, проходящую через точки $P_3, \ldots, P_7$. Беря точки P' и P'' на прямой L и поступая как в случае 1, снова приходим к противоречию, так как точка P_8 не лежит ни на Q, ни на L.

Этим исчерпаны все возможности и лемма доказана. □

Доказательство теоремы 4.5.2**.** Проверка коммутативности и того, что O является нулем очевидны. Докажем ассоциативность сложения для "достаточно общих" точек. Пусть даны точки $P, Q, R \in E$. Рассмотрим приводимые кубические кривые

$$\begin{aligned} X_1 &:= L_{P,Q,\overline{P+Q}} \cup L_{\overline{Q+R},O,Q+R} \cup L_{P+Q,R,\overline{(P+Q)+R}}, \\ X_2 &:= L_{Q,R,\overline{Q+R}} \cup L_{\overline{P+Q},O,P+Q)} \cup L_{Q+R,P,\overline{P+(Q+R)}}. \end{aligned}$$

Каждая из трех кривых E, X_1 и X_2 содержит восемь точек

$$O,\ P,\ Q,\ P+Q,\ \overline{P+Q},\ R,\ Q+R,\ \overline{Q+R}$$

и, кроме того,

$$E \cap X_1 \ni \overline{(P+Q)+R}, \qquad E \cap X_2 \ni \overline{P+(Q+R)}.$$

Если все точки в $E \cap X_1$ попарно различны, то по лемме 4.5.6, примененной к $X = E$, $Y = X_1$, $Z = X_2$ имеем $\overline{(P+Q)+R} = \overline{P+(Q+R)}$, а следовательно, и $(P+Q)+R = P+(Q+R)$.

Мы наметим полное доказательство только для случая $\Bbbk = \mathbb{C}$. Используются следующие два утверждения:

1) отображение $E \times E \to E$, $(P,Q) \to P+Q$ является непрерывной функцией (координат),

2) для любых трех точек $P, Q, R \in E$ существуют достаточно близкие точки $P_\epsilon, Q_\epsilon, R_\epsilon \in E$ такие, что точки

$$O, P_\epsilon, Q_\epsilon, R_\epsilon, P_\epsilon + Q_\epsilon, \overline{P_\epsilon + Q_\epsilon}, Q_\epsilon + R_\epsilon, \overline{Q_\epsilon + R_\epsilon}, \overline{(P_\epsilon + Q_\epsilon) + R_\epsilon}$$

попарно различны.

Доказательство первого утверждения следует из непрерывной зависимости корней многочлена от коэффициентов (см. явные формулы в теореме 4.5.7 для частного случая, когда O – точка перегиба). Доказательство второго утверждения мы оставляем читателю.

Теперь мы можем рассмотреть два отображения

$$\phi, \psi \colon E \times E \times E \longrightarrow E,$$

заданные формулами $\phi(P,Q,R) = (P+Q)+R$ и $\psi(P,Q,R) = P+(Q+R)$. Эти отображения непрерывны и совпадают на всюду плотном множестве. Значит они совпадают всюду. Последнее рассуждение может быть модифицировано и для случая произвольного поля. Для этого нужно вместо классической хаусдорфовой топологии рассматривать топологию Зарисского (см. определение 3.1.6). □

Выведем теперь явную формулу для группового закона.

Теорема 4.5.7 *Рассмотрим кривую E в вейерштрассовой форме $y^2 = x^3 + ax + b$ и пусть $O = (0:1:0)$. Для двух*

точек $P=(x_1,y_1)$ *и* $Q=(x_2,y_2)$ *на* E *положим*

$$\begin{aligned}\lambda &:= \frac{y_2-y_1}{x_2-x_1}, \qquad \mu := \frac{y_1x_2-x_1y_2}{x_2-x_1} && \text{при } x_1\neq x_2,\\ \lambda' &:= \frac{3x_1^2+a}{2y_1}, \qquad \mu' := \frac{-x_1^3+ax_1+2b}{2y_1} && \text{при } y_1\neq 0.\end{aligned} \tag{4.5.8}$$

Тогда

$$\begin{aligned}-P &= \bar{P}=(x_1,-y_1),\\ P+Q &= \big(\lambda^2-x_1-x_2,\ -\lambda(\lambda^2-x_1-x_2)-\mu\big),\\ 2P &= \big(\lambda'^2-2x_1,\ -\lambda'(\lambda'^2-2x_1)-\mu'\big).\end{aligned} \tag{4.5.9}$$

Отметим, что явные формулы (4.5.9) показывают, что отображения $E\to E$, $P\to -P$ и $E\times E\to E$, $(P,Q)\to P+Q$ являются непрерывными (в классической топологии для $\Bbbk=\mathbb{C}$ и в топологии Зарисского для произвольного $\Bbbk$).

Доказательство. Первое соотношение (4.5.9) очевидно, поскольку прямая, соединяющая P и O имеет вид $x=x_1$. Пусть $P\neq Q$ и $P\neq -Q$. Прямая L_{PQ} имеет параметрические уравнения

$$x=(x_2-x_1)t+x_1, \qquad y=(y_2-y_1)t+y_1.$$

Точки пересечения L_{PQ} и E находятся из уравнения

$$g(t)=((y_2-y_1)t+y_1)^2-((x_2-x_1)t+x_1)^3-a((x_2-x_1)t+x_1)-b=0.$$

Корень $t=0$ соответствует точке P (это действительно корень поскольку свободный член равен $y_1^2-x_1^3-ax_1-b=0$). Далее $g(t)/t$ имеет вид

$$\begin{aligned}g(t)/t=(3x_1x_2^2+x_1^3-3x_2x_1^2-x_2^3)(t-1)^2+\\ (y_1^2+3x_1x_2^2-2x_2^3-2y_2y_1+y_2^2-x_1^3)(t-1)-\\ -y_1^2+x_1^3+ax_1-ax_2+y_2^2-x_2^3.\end{aligned}$$

Снова учитывая, что P и Q лежат на E, получим обращение в нуль свободного члена. Корень $t=1$ многочлена $g(t)$ соответствует точке Q. Далее,

$$g(t)/t(t-1) = -(x_2-x_1)^3(t-1)+ \\ (y_1^2 - 2y_2y_1 + y_2^2 + 3x_1x_2^2 - 2x_2^3 - x_1^3).$$

Получаем третий корень многочлена $g(t)$:

$$t_0 = \frac{(y_2-y_1)^2 + 3x_2x_1^2 - 2x_1^3 - x_2^3}{(x_2-x_1)^3}.$$

Координатами точки $P+Q$ будут

$$x_0 = (x_2-x_1)t_0 + x_1, \qquad y_0 = -(y_2-y_1)t_0 - y_1.$$

Учитывая (4.5.8), получим

$$x_0 = \lambda^2 - x_1 - x_2, \qquad y_0 = -\lambda x_0 - \mu.$$

Для доказательства последнего соотношения (4.5.9) найдем уравнение касательной прямой $T_{P,E}$ в точке P:

$$(-3x_1^2 - a)(x-x_1) + 2y_1(y-y_1) = 0.$$

Его можно переписать в виде

$$y = \frac{3x_1^2+a}{2y_1}x + \frac{2y_1^2 - 3x_1^3 - ax_1}{2y_1} = \lambda' x + \mu'.$$

Отсюда находим третью точку R пересечения E и $T_{P,E}$:

$$-(x-x_1)^3 + \left(\lambda'^2 - 3x_1\right)(x-x_1)^2 + y_1^2 - x_1^3 - ax_1 - b = 0.$$

Так как $y_1^2 - x_1^3 - ax_1 - b = 0$, то $x = \lambda'^2 - 2x_1$. Учитывая, что $2P = \overline{R}$, получаем требуемое. □

Пусть теперь кривая задана в обобщенной форме Вейерштрасса (4.2.7). Тогда

$$-P = (x_1, -y_1 - a_1x_1 - a_3).$$

Определим λ и μ формулами (4.5.8) при $x_1 \neq x_2$ и формулами

$$\lambda := \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \qquad \mu := \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

при $x_1 = x_2$ и $P+Q \neq 0$. Если $P+Q \neq 0$, то эта точка имеет координаты

$$x_0 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \qquad y_0 = -(\lambda + a_1)x_0 - \mu - a_3.$$

$\Bbbk$-точки эллиптических кривых

Пусть кривая определена над некоторым полем $\Bbbk \subsetneq \bar{\Bbbk}$. Точка $P = (a_0 : a_1 : a_2)$ называется $\Bbbk$-*рациональной* (или определенной над $\Bbbk$), если существует $\lambda \in \bar{\Bbbk}$ такое, что $\lambda a_i \in \Bbbk$ для всех i. Множество всех $\Bbbk$-рациональных точек обозначается через $E(\Bbbk)$. Предположим, что неособая кубическая кривая определена над $\Bbbk$ и пусть $E(\Bbbk) \neq \varnothing$. Пусть $O \in E(\Bbbk)$ – любая $\Bbbk$-точка. Так как конструкция группового закона использует лишь решение линейных уравнений, то множество $E(\Bbbk)$ является подгруппой в группе (E, O). Если можно выбрать O точкой перегиба, то последнее также является следствием явных формул (4.5.9).

Строение группы $E(\Bbbk)$ – очень интересная алгебро-геометрическая и теоретико-числовая проблема. Например в случае $\Bbbk = \mathbb{Q}$ теорема Морделла утверждает, что группа $E(\mathbb{Q})$ конечно порождена.

Пример 4.5.10 На кривой Ферма $x^3 + y^3 = z^3$ имеется лишь три рациональные точки: $(1 : -1 : 0)$, $(1 : 0 : 1)$ и $(0 : 1 : 1)$. Выбирая одну из них за нейтральный элемент, получим, что $E(\mathbb{Q}) \simeq \mathbb{Z}_3$.

Точки конечного порядка

Рассмотрим эллиптическую кривую $E \subset \mathbb{P}^2$ (с фиксированной точкой $O \in E$). В группе (E имеет место умножение на $n \in \mathbb{N}$: $nP := \underbrace{P + \cdots + P}_{n}$. Рассмотрим подгруппу n-*кручения*:

$$E[n] := \{P \in E \mid nP = 0 \quad \text{в группе } E\}.$$

Примеры 4.5.11 (i) Вычислим $E[2]$ на эллиптической кривой E. Для этого поместим нулевой элемент группы в точку перегиба. Каждая точка $P \in E[2]$ удовлетворяет условию $P = -P$. Согласно предложению 4.5.3 $-Q$ – третья точка пересечения прямой OQ с E. Следовательно, $E[2]$ состоит из точек P, для которых касательная $T_{P,E}$ проходит через O. Пусть $\operatorname{char}\Bbbk \neq 2$. Тогда по теореме 4.2.3 в некоторой системе координат E может

быть задана неоднородным уравнением $y^2 = g(x)$, где многочлен $g(x)$ не имеет кратных корней. Точка O лежит на бесконечной прямой и имеет координаты $(0:1:0)$. Прямые, проходящие через O имеют вид $x = c = \mathrm{Const}$. Такая прямая касается E тогда и только тогда, когда уравнение $y^2 = g(c)$ – имеет одно решение относительно y, а это, в свою очередь выполняется, когда c – корень $g(x)$. Следовательно, $E[2]$ состоит из нуля (бесконечной точки) и трех точек $\{y = g(x) = 0\}$. Эта группа изоморфна $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Это также можно доказать исходя из явных формул в теореме 4.5.7.

(ii) Предположим теперь, что $\operatorname{char} \Bbbk = 2$. Тогда E задается уравнением в развернутой форме Вейерштрасса (4.2.7):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где снова $O = (0:1:0)$. Как и выше, получаем, что группа $E[2]$ состоит из точек $P = (y, c)$, для которых уравнение

$$y^2 + a_1cy + a_3y = c^3 + a_2c^2 + a_4c + a_6$$

имеет одно решение относительно y. Вычисляя дискриминант при условии $\operatorname{char} \Bbbk = 2$, получим $(a_1c + a_3)^2 = 0$. Заметим, что при $a_1 = a_3 = 0$ кривая E особа (проверьте!). Поэтому возможны два случая:

- $a_1 \neq 0$ и тогда $E[2] \simeq \mathbb{Z}_2$;
- $a_1 = 0$ и тогда $E[2] = \{0\}$.

(iii) Точки порядка 3 можно найти из условия $2P = -P = \bar{P}$, $P \neq O$. Согласно геометрической интерпретации группового закона 4.5.1, точка P должна быть точкой перегиба, отличной от нуля (при нашем условии, что нуль – также точка перегиба). Если $\operatorname{char} \Bbbk \neq 3$, то по теореме 4.3.1 и упражнению (11), стр. 99 имеется ровно восемь таких точек P и поэтому $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Если же $\operatorname{char} \Bbbk = 3$, то согласно упражнению (4), стр. 98 имеется два случая:

$$E[3] \simeq \begin{cases} \mathbb{Z}_3 & \text{если } c \neq 0, \\ \{0\} & \text{если } c = 0. \end{cases}$$

(iv) Если $\Bbbk = \mathbb{C}$, то как мы увидим ниже (E, O) (как абстрактная группа) изоморфна $\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$. Следовательно, $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ в этом случае. В общем случае группа $E[n]$ изоморфна $\mathbb{Z}_n \oplus \mathbb{Z}_n$, если характеристика основного поля не делит n. Если же $n = p$, то $E[n]$ изоморфна $\mathbb{Z}_p$ или 0 (это зависит от кривой).

Упражнения. **(1)** Покажите на примере, что кривые четвертой степени, проходящие через 13 точек, не обязаны иметь еще одну точку, общую им всем.

(2) Докажите, что конструкция 4.5.3 задает также групповой закон на неособых точках декартова листа и полукубической параболы (см. упражнения (3) и (4), стр. 92. Как устроены эти группы?

(3) Выведите формулы, аналогичные формулам (4.5.8), для кривой Ферма $x^3 + y^3 = z^3$.

(4) Выпишите явные формулы для группового закона на эллиптической кривой $y^2 + y = x^3$ над полем характеристики 2 (в качестве нейтрального элемента возьмите бесконечную точку).

(5) Воспользуйтесь групповым законом и постройте семейство рациональных решений уравнения $y^2 = x^3 + x - 1$.

(6) Выбрав в качестве нейтрального элемента точку $(0 : 1 : 0)$, на кривой $y^2 + y = x^3 - x$ найдите nP для $P = (0, 0)$ и любого n.

(7) Найдите все точки порядка 2 на кривой $y^2 = x^3 + x$.

(8) Найдитевсе точки порядка 3 на кривой $y^2 - x^3 + 2 = 0$.

(9) Сколько существует точек порядка 3 на эллиптической кривой $y^2 + y = x^3$ над полем $\mathbb{F}_q$ для $q = 3, 5, 7, 9$?

(10) Найдите порядок точки P на эллиптической кривой E:

(i) $P = (0, 1)$, $y^2 = x^3 + x + 1$ над полем $\mathbb{F}_3$.

(ii) $P = (2, 2)$, $y^2 = x^3 + 1$ над полем $\mathbb{F}_5$.

(iii) $P = (2, 2)$, $y^2 = x^3 + x + 1$ над полем $\mathbb{F}_7$,

(iv) $P = (1, 3)$, $y^2 = x^3 + 1$ над полем $\mathbb{F}_7$,

(v) $P = (3, 4)$, $y^2 = x^3 + x$ над полем $\mathbb{F}_7$.

(11) Найти порядок точки P на эллиптической кривой E над $\mathbb{C}$:

(i) $P = (1, \sqrt{2})$, $y^2 = x^3 - x$,

(ii) $P := (0, 4)$, $y^2 = x^3 + 16$,

(iii) $P = (0, -1)$, $\quad y^2 = x^3 + 1$,

(iv) $P := (2, 4)$, $\quad y^2 = x^3 + 4\,x$,

(v) $P := (2i, 0)$, $\quad y^2 = x^3 + 4\,x$,

(vi) $P := (3, 8)$, $\quad y^2 = x^3 - 43x + 166$,

(12) Каков геометрический смысл точек четвертого порядка на эллиптической кривой?

(13) Пусть $\Bbbk = \bar{\mathbb{F}}_p$. Докажите, что группа эллиптической кривой E является группой кручения. *Указание.* Любая точка $P \in E$ является $\mathbb{F}_q$-рациональной для некоторого $\mathbb{F}_q \supset \mathbb{F}_p$.

(14) Докажите, что если (алгебраически замкнутое) поле $\Bbbk$ неалгебраично над своим простым подполем, то группа эллиптической кривой E не является группой кручения.

4.6. Рациональные кривые. Нерациональность эллиптической кривой

Определение 4.6.1 Неприводимая (аффинная) кривая $X \subset \mathbb{A}^2$, заданная неприводимым многочленом $f(x, y)$, называется *рациональной*, если существуют рациональные функции $\varphi(t)$, $\psi(t)$ такие, что хотя бы одна из них непостоянна и $f(\varphi(t), \psi(t)) = 0$. Проективная кривая называется *рациональной*, если рационально пересечение ее с одной из аффинных карт.

Функции $\varphi(t)$, $\psi(t)$ задают отображение

$$U \longrightarrow X, \qquad t \longmapsto (\varphi(t), \psi(t)),$$

где $U \subset \mathbb{A}^1$ – непустое, открытое в топологии Зарисского множество, дополнение к конечному множеству, заданному обращением в нуль знаменателей функций φ и ψ. Такие отображения называются в алгебраической геометрии *рациональными отображениями*. Их принято обозначать пунктирными стрелками: $\mathbb{A}^1 \dashrightarrow X$ (считается, что сплошные стрелки задают определенные всюду отображения, а пунктирные – определенные на непустом, открытом в топологии Зарисского подмножестве).

Теорема 4.6.2 (теорема Люрота) *Пусть* $\Bbbk(t)$ *– поле рациональных дробей над (необязательно алгебраически замкнутым) полем* $\Bbbk$. *Каждое промежуточное подполе* $\mathbb{K}$, $\Bbbk \subsetneqq \mathbb{K} \subset \Bbbk(t)$ *также изоморфно полю рациональных дробей.*

Предложение 4.6.3 *Пусть* $X \subset \mathbb{A}^2$ *– неприводимая рациональная кривая. Существуют рациональные функции* $\varphi_1(\vartheta)$, $\psi_1(\vartheta)$ *и* $\Psi(x,y)$ *такие, что* $\Psi(\varphi_1(\vartheta),\psi_1(\vartheta)) = \vartheta$. *В частности, отображение* $\Phi\colon \vartheta \longmapsto (\varphi_1(\vartheta),\psi_1(\vartheta))$ *является биекцией между непустыми открытыми в топологии Зарисского подмножествами в* $\Bbbk$ *и в* X.

Отображение Φ называется *рациональной параметризацией* кривой X.

Доказательство. Пусть f, φ и ψ – такие как в определении 4.6.1. Рассмотрим гомоморфизм колец $\Bbbk[x,y] \to \Bbbk[t]$, $x \mapsto \varphi(t)$, $y \mapsto \psi(t)$. Поскольку он зануляется на f, то по теореме о гомоморфизме имеет место разложение в композицию

$$\Bbbk[x,y] \to \Bbbk[x,y]/(f) = \Bbbk[X] \xrightarrow{h} \Bbbk[t].$$

Если h не является вложением, то существует многочлен $g(x,y)$, не делящийся на f и такой, что $g(\varphi(t),\psi(t)) = 0$ Но тогда, подставляя различные t в $x = \varphi(t)$, $y = \psi(t)$, мы получим бесконечное число решений системы $f(x,y) = g(x,y) = 0$. Это противоречит теореме 3.1.12. Таким образом гомоморфизм h инъективен и задает вложение полей $\Bbbk(X) \hookrightarrow \Bbbk(t)$. По теореме Люрота $\Bbbk(X) = \Bbbk(\vartheta)$ для некоторого $\vartheta = \vartheta(t) \in \Bbbk(t)$. Поскольку функции $\varphi(t)$ и $\psi(t)$ принадлежат образу вложения $\Bbbk(X) \hookrightarrow \Bbbk(t)$, то $\varphi(t) = \varphi_1(\vartheta)$ и $\psi(t) = \psi_1(\vartheta)$. Более того, поскольку образы x и y порождают поле $\Bbbk(\vartheta)$, то ϑ рационально выражается через φ_1 и ψ_1: $\vartheta = \Psi(\varphi_1,\psi_1)$ для некоторой рациональной функции $\Psi(x,y)$. Запишем Ψ в виде несократимой дроби: $\Psi = \Psi_1/\Psi_2$. В этом случае знаменатель Ψ_2 обращается в нуль лишь в конечном числе точек на кривой X. Действительно, иначе по теореме 3.1.12 многочлен Ψ_2 делится на f. Так как

$$\Psi_1(\varphi(t),\psi(t)) = \vartheta(t)\Psi_2(\varphi(t),\psi(t)),$$

то Ψ_1 делится на f. Противоречие.

Положим $\Phi(\vartheta) = (\varphi_1(\vartheta), \psi_1(\vartheta))$. Тогда $\Psi \circ \Phi(\vartheta) = \vartheta$, т.е., $\Psi \circ \Phi$ – тождественное отображение. Функции Φ и Ψ не определены в конечном множестве точек – там, где знаменатели функций φ_1, ψ_1 и Ψ обращаются в нуль. $\square$

Следствие 4.6.4 *Неприводимая кривая $X \subset \mathbb{A}^2$ рациональна тогда и только тогда, когда ее поле рациональных функций $\Bbbk(X)$ изоморфно полю рациональных дробей от одной переменной.*

Доказательство. Поле $\Bbbk(X)$ порождается образами координатных функций x, y. Поэтому требуемый изоморфизм $\Bbbk(X) \simeq \Bbbk(\vartheta)$ может быть задан формулами $x \to \varphi_1(\vartheta)$, $y \to \psi_1(\vartheta)$. $\square$

Примеры 4.6.5 (i) Любая прямая $X \subset \mathbb{A}^2$ может быть записана параметрически: $x = at + x_0$, $y = bt + y_0$. Поэтому она рациональна.

(ii) Рассмотрим конику $X \subset \mathbb{A}^2$, заданную уравнением $x^2 + y^2 = 1$. Зададим ее рациональную параметризацию, как стереографическую проекцию из точки $(0, 1)$ на ось x. Эта проекция определяется формулами $t = \Psi(x, y) = -x/(y-1)$. Выражая y через t и x и подставляя это в уравнение коники, находим

$$x = \frac{2t}{t^2+1}, \qquad y = \frac{t^2-1}{t^2+1}. \tag{4.6.6}$$

Это и есть искомая рациональная параметризация. Поскольку все неприводимые коники над алгебраически замкнутым полем проективно эквивалентны, то все они являются рациональными кривыми.

(iii) Кривая $X \subset \mathbb{A}^2$, заданная уравнением $x^2 - y^3 = 0$ также рациональна. Рациональная параметризация задается формулами $t \to (t^3, t^2)$, а обратное отображение – формулой $(x, y) \to x/y$.

Предположим, что рациональная кривая $X \subset \mathbb{A}^2$ определена над подполем $\Bbbk_0 \subset \Bbbk$. Если существует рациональная параметризация $x = \varphi(t)$, $y = \psi(t)$, для которой все коэффициенты

функций φ и ψ лежат в $\Bbbk_0$, то говорят, что X *рациональна над* $\Bbbk_0$. В этом случае параметризация может быть использована для нахождения $\Bbbk_0$-точек кривой X.

Другое приложение рациональных параметризаций связано с вычислением интегралов. Уравнение $f(x,y)=0$ задает y как неявную функцию от x. Если кривая $f(x,y)=0$ рациональна, то рациональная параметризация сводит вычисление интеграла $\int y(x)dx$ к интегрированию рациональных функций $\int y(t)dx(t)$.

Предложение 4.6.3 показывает, что рациональные кривые "очень похожи" на проективную прямую. В действительности, можно строго доказать, что неприводимая неособая проективная кривая является рациональной тогда и только тогда когда она *изоморфна* $\mathbb{P}^1$ (ср. упражнение (2), стр. 74). Мы покажем, что эллиптические кривые нерациональны.

Теорема 4.6.7 *Неособая кубическая кривая $E \subset \mathbb{P}^2$ нерациональна.*

Мы предположим, что характеристика основного поля отлична от 2. Тогда, согласно теореме 4.2.3 можно считать, что E задана уравнением

$$y^2 = x(x-1)(x-\lambda).$$

Таким образом, достаточно доказать следующее

Предложение 4.6.8 *Пусть $\Bbbk$ – поле, характеристика которого не равна 2, а $\lambda \in \Bbbk$, $\lambda \neq 0,1$. Пусть $\varphi, \psi \in \Bbbk(t)$ – такие рациональные функции, что*

$$\varphi^2 = \psi(\psi-1)(\psi-\lambda). \tag{4.6.9}$$

Тогда $\varphi, \psi \in \Bbbk$.

Доказательство. Используя тот факт, что $\Bbbk[t]$ – кольцо с однозначным разложением на множители, представим φ и ψ в виде несократимых дробей: $\varphi = r/s$, $\psi = p/q$, где $r,s,p,q \in \Bbbk[t]$, причем НОД $(r,s)=1$ и НОД $(p,q)=1$. После приведения к общему знаменателю (4.6.9) принимает вид

$$r^2q^3 = s^2p(p-q)(p-\lambda q).$$

Далее, так как r и s взаимно просты, то сомножитель s^2, стоящий в правой части, должен делить q^3; аналогично, так как p и q взаимно просты, то сомножитель q^3, стоящий в левой части, должен делить s^2. Итак, $s^2 \mid q^3$ и $q^3 \mid s^2$, а значит, $s^2 = aq^3$, где $a \in \Bbbk$ (a является обратимым элементом в кольце $\Bbbk[t]$ и, следовательно, лежит в $\Bbbk$).

Тогда $aq = (s/q)^2$ является квадратом в $\Bbbk[t]$. Кроме того,

$$r^2 = ap(p-q)(p-\lambda q).$$

Из разложения в произведение простых сомножителей вытекает теперь, что p, $p-q$, $p-\lambda q$ являются квадратами в $\Bbbk[t]$. Если нам удастся доказать, что p и q – константы, то из сказанного выше будет следовать, что r и s – также константы, и теорема будет доказана. Согласно сказанному выше, многочлены p и q удовлетворяют условиям следующей леммы.

Лемма 4.6.10 *Пусть $p, q \in \Bbbk[t]$ – взаимно простые многочлены. Предположим, что четыре элемента*

$$p, \quad q, \quad p-q, \quad p-\lambda q.$$

являются квадратами в $\Bbbk[t]$ для $\lambda \neq 0, 1$. Тогда $p, q \in \Bbbk$.

Доказательство (метод бесконечного спуска Ферма). Имеем $p = u^2$, $q = v^2$, где $u, v \in \Bbbk[t]$ взаимно просты и

$$\max\{\deg u, \deg v\} < \max\{\deg p, \deg q\}.$$

Предположим от противного, что $\max\{\deg p, \deg q\}$ положителен и является минимальным на множестве всех пар p, q, удовлетворяющих условиям леммы (с произвольным $\lambda \in \Bbbk \setminus \{0, 1\}$). Тогда справедливы два следующих равенства:

$$\begin{aligned} p-q &= u^2 - v^2 = (u-v)(u+v), \\ p-\lambda q &= u^2 - \lambda v^2 = (u-\mu v)(u+\mu v) \end{aligned}$$

(где $\mu = \sqrt{\lambda}$). Эти выражения являются квадратами в $\Bbbk[t]$, а в силу взаимной простоты u и v квадратами будут также $u-v$, $u+v$, $u-\mu v$, $u+\mu v$. Положим

$$p' := \frac{1}{2}(\mu+1)(u-v), \qquad q' := \frac{1}{2}(\mu-1)(u+v).$$

Тогда элементы

$$p', \quad q', \quad p' - q' = u - \mu v,$$

являются квадратами в $\Bbbk[t]$. Возьмем $\delta \in \Bbbk$ так, что

$$\frac{\delta(\mu-1)+\mu+1}{\delta(\mu-1)-(\mu+1)} = \mu.$$

Тогда квадратом также является и

$$p' - \delta q' = 2\big(\mu + 1 - \delta(\mu-1)\big)(u + \mu v)$$

Это противоречит минимальности $\max\{\deg p, \deg q\}$. □

□

Упражнения. **(1)** Воспользуйтесь параметризацией (4.6.6) для описания целочисленных решений уравнения $x^2 + y^2 = z^2$.

(2) Пусть $X \subset \mathbb{A}^2$ – неприводимая кривая, заданная уравнением $f_{d-1}(x,y) + f_d(x,y) = 0$, где f_{d-1} и f_d – многочлены степеней $d-1$ и d соответственно. Докажите, что X рациональна.

(3) Докажите, что если многочлен x^3+ax+b имеет кратный корень, то кривая, заданная в $\mathbb{A}^2$ уравнением $y^2 = x^3 + ax + b$ рациональна.

(4) Докажите, что кривая $y^3 = x^4 - 4x^3 + 6x^2 - 4x + 3y^2 - 3y + 2$ рациональна. Выпишите рациональную параметризацию.

(5) Приведите другое доказательство теоремы 4.6.7, использующее существование группового закона. *Указание.* Бирациональное отображение $E \dashrightarrow \mathbb{P}^1$ может быть продолжено до изоморфизма. На $\mathbb{P}^1$ любой автоморфизм имеет неподвижную точку, в то время как на неособой кубической кривой имеются автоморфизмы без неподвижных точек – сдвиги.

(6) Пусть $d \geq 3$ и характеристика основного поля не делит d. Докажите, что кривая Ферма, заданная в $\mathbb{P}^2$ уравнением $x^d + y^d = z^d$, не является рациональной.

(7) Пусть $E \subset \mathbb{P}^2$ – эллиптическая кривая и пусть x, y – однородные координаты, в которых E имеет вейерштрассову форму. Докажите, что образ отображения $E \to \mathbb{P}^3$, $(x,y) \to (1 : x : y : x^2)$ является неособым пересечением двух квадрик (поверхностей степени 2).

(8) Пусть $Y \subset \mathbb{P}^3$ – кривая, являющаяся пересечением двух квадрик. Докажите, что в некоторой системе координат $t_0 : \cdots : t_3$ эта кривая может быть записана в виде

$$\begin{array}{ccccc} t_0^2 & + & t_2^2 & = & t_0 t_3, \\ t_1^2 & + & \lambda t_2^2 & = & t_2 t_3. \end{array}$$

При каких значениях параметра λ эта кривая неособа?

(9) Докажите утверждение, обратное к задаче (7): каждая неособая кривая $Y \subset \mathbb{P}^3$, являющаяся пересечением двух квадрик в $\mathbb{P}^3$, изоморфно отображается на неособую кубическую кривую $E \subset \mathbb{P}^2$. *Указание.* Используйте проекцию из точки $P \in Y$.

(10) В условиях задач (8) и (9) выразить j-инвариант кривой E через параметр λ.

4.7. Эллиптические кривые над полем комплексных чисел

Для понимания этого параграфа читателю придется вспомнить основные понятия теории функций комплексного переменного, см., например, [Шаб76].

Римановы поверхности

Определение 4.7.1 *Римановой поверхностью* называется хаусдорфово топологическое пространство X, обладающее открытым покрытием $X = \bigcup\limits_{\alpha} U_\alpha$ и набором отображений $\phi\colon U_\alpha \to \mathbb{C}$ таких, что

(i) каждое ϕ_α – гомеоморфизм U_α на открытое подмножество комплексной плоскости $\mathbb{C}$ (рассматриваемой с классической хаусдорфовой топологией);

(ii) композиции

$$\phi_\beta \circ \phi_\alpha^{-1}\colon \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$$

являются голоморфными (т.е., аналитическими) функциями.

Голоморфные функции $\phi_\beta \circ \phi_\alpha^{-1}$ называются *функциями перехода*.

Пример 4.7.2 Пусть $X = \mathbb{P}^1$ – проективная прямая над полем $\mathbb{C}$ с однородными координатами $(z_0 : z_1)$. Рассмотрим открытые подмножества $U_i := \{(z_0 : z_1) \mid z_i \neq 0\}$ и гомеоморфизмы $\phi_i \colon U_i \to \mathbb{C}$, $\phi_0(z_0 : z_1) = z_1/z_0$, $\phi_1(z_0 : z_1) = z_0/z_1$. Функции перехода имеют вид $z \to 1/z$. Они являются голоморфными в своей области определения. Поэтому $X = \mathbb{P}^1$ – риманова поверхность.

Пример 4.7.3 Любая неособая алгебраическая кривая является римановой поверхностью. Мы покажем это в простейшем случае аффинной кривой в $\mathbb{A}^2$. Пусть $X \subset \mathbb{A}^2$ – неособая аффинная алгебраическая кривая, заданная уравнением $f(x, y) = 0$. В каждой точке $P = (x_0, y_0) \in X$ градиент отличен от нуля. Мы можем считать, что $\partial f/\partial y(x_0, y_0) \neq 0$. Пусть $h \colon \mathbb{A}^2 \to \mathbb{C}$ – проекция на первую координату. Согласно аналитическому варианту теоремы о неявной функции, существует голоморфная функция $y = g(x)$ такая, что в некоторой окрестности V_P точки P

$$f(x, y) = 0 \quad \Longleftrightarrow \quad y = g(x).$$

Полагая $U_P := V_P \cap X$, получим гомеоморфизм $\phi_P = h|_{U_P} \colon U_P \to h(U_P)$ на открытое подмножество в $\mathbb{C}$.

Факторы по дискретным группам

Пусть X – риманова поверхность. Будем говорить, что группа G действует на X *свободно* и *дискретно*, если выполняются следующие условия:

(i) любая точка $P \in X$ имеет окрестность U_P такую, что $gU_P \cap U_P = \varnothing$ для всех $g \in G$, $g \neq 1$;

(ii) для любых двух точек $P, Q \in X$ из разных G-орбит существуют окрестности $U_P \ni P$ и $U_Q \ni Q$ такие, что $gU_P \cap U_Q = \varnothing$ для всех $g \in G$.

Тогда факторпространство X/G также является римановой поверхностью.

Пример 4.7.4 (Полной) *решеткой* Ω в комплексной плоскости $\mathbb{C}$ называется свободная абелева подгруппа ранга 2, порождающая $\mathbb{C}$ как векторное пространство над над $\mathbb{R}$. Ясно, что Ω действует на $\mathbb{C}$ свободно и дискретно. Следовательно, $E := \mathbb{C}/\Omega$ – компактная риманова поверхность. Она называется *одномерным комплексным тором*. Топологически, E является параллелограммом с отождествленными противоположными сторонами (см. рис. 4.4). Тор E также имеет групповую структу-

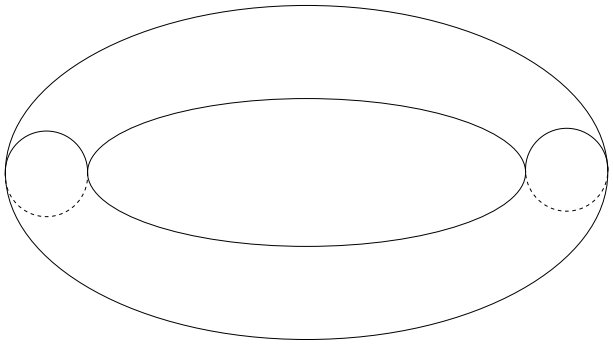


Рис. 4.4 Комплексный тор

ру, которая согласована со структурой римановой поверхности: отображения $E \times E \to E$ и $E \to E$ взятия суммы и обратного элемента голоморфны. Таким образом, E является компактной (связной) комплексной группой Ли.

Далее мы покажем, что каждый одномерный комплексный тор E "является" эллиптической кривой над полем $\mathbb{C}$. Для того, чтобы построить голоморфное вложение $E \hookrightarrow \mathbb{P}^2$ мы определим некоторые мероморфные функции на E. Такие функции, в свою очередь, могут быть интерпретированы как Ω-периодические мероморфные функции на $\mathbb{C}$.

Эллиптические функции

Рассмотрим решетку $\Omega \subset \mathbb{C}$. Каждая решетка в $\mathbb{C}$ имеет базис над $\mathbb{Z}$, состоящий из двух векторов ω_1, ω_2. В этом случае мы будем писать $\Omega = \langle \omega_1, \omega_2 \rangle$. Мероморфная на всей комплексной

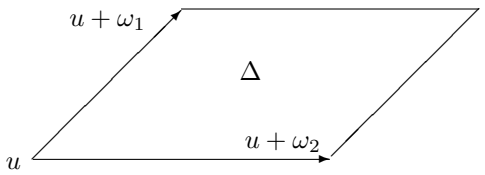
плоскости функция f называется *эллиптической* по отношению к решетке Ω, если она Ω-периодична, т.е. $f(z+\omega) = f(z)$ для всех $z \in \mathbb{C}$ и всех $\omega \in \Omega$. Отметим, что голоморфная всюду эллиптическая функция f должна быть константой: она ограничена на компакте – параллелограмме, натянутом на ω_1 и ω_2, а так как она Ω-периодична, то f ограничена и на $\mathbb{C}$. По теореме Лиувилля функция – константа. Все эллиптические функции образуют подполе $\mathscr{E}_\Omega$ в поле всех мероморфных функций.

Наша цель – доказать, что поле $\mathscr{E}_\Omega$ изоморфно полю рациональных функций на некоторой неособой кубической кривой $E \subset \mathbb{P}^2$ над полем $\mathbb{C}$ и наоборот, для любой неособой кубической кривой $E \subset \mathbb{P}^2$ над $\mathbb{C}$ существует решетка $\Omega \subset \mathbb{C}$ такая, что ее поле рациональных функций изоморфно полю $\mathscr{E}_\Omega$.

Пусть $\Omega = \langle \omega_1, \omega_2 \rangle$ – решетка в $\mathbb{C}$. Для любого $u \in \mathbb{C}$ множество

$$\Delta := \{u + x\omega_1 + y\omega_2 \mid 0 \le x, y < 1\}$$

называется *основным параллелограммом.*



Напомним, что особой точкой мероморфной функции называется ее нуль или полюс. Порядок особой точки z_0 обычно записывается со знаком: он положителен, если z_0 — нуль и отрицателен, если z_0 – полюс.

Предложение 4.7.5 (теоремы Лиувилля) *Пусть Δ – такой основной параллелограмм, что эллиптическая функция не имеет особых точек (т.е. нулей и полюсов) на его границе. Пусть $z_1, \dots, z_r$ – все особые точки внутри Δ, а $m_1, \dots, m_r$ – их порядки. Тогда*

(i) $\sum \operatorname{res}_{z_i} f(z) = 0$;

(ii) $\sum m_i = 0$;

(iii) $\sum m_i z_i \equiv 0 \mod \Omega$.

Доказательство. (i) следует из теоремы Коши о вычетах

$$2\pi\,\mathrm{i}\sum \operatorname{res}_{z_i} f(z) = \int\limits_{\partial\Delta} f(z)dz = 0.$$

Здесь правая часть обращается в нуль, поскольку интегралы по противоположным сторонам параллелограмма уничтожаются в силу периодичности.

(ii) Найдем сумму логарифмических вычетов функции $f(z)$ (принцип аргумента). Ясно, что функции $f'(z)$ и $f'(z)/f(z)$ являются эллиптическими. Как и в пункте (i) имеем

$$0 = \int\limits_{\partial\Delta} \frac{f'(z)}{f(z)}dz = 2\pi\,\mathrm{i}\sum \operatorname{res}_{z_i} \frac{f'(z)}{f(z)} = 2\pi\,\mathrm{i}\sum m_i.$$

(iii) Аналогично (ii) запишем

$$\begin{aligned}
2\pi\,\mathrm{i}\sum m_i z_i = 2\pi\,\mathrm{i}\sum \operatorname{res}_{z_i} \frac{zf'(z)}{f(z)} = \int\limits_{\partial\Delta} \frac{zf'(z)}{f(z)}dz = \\
= \int\limits_{u}^{u+\omega_1} \frac{zf'(z)}{f(z)}dz - \int\limits_{u+\omega_2}^{u+\omega_1+\omega_2} \frac{zf'(z)}{f(z)}dz - \int\limits_{u}^{u+\omega_2} \frac{zf'(z)}{f(z)}dz + \\
+ \int\limits_{u+\omega_1}^{u+\omega_1+\omega_2} \frac{zf'(z)}{f(z)}dz = -\omega_2 \int\limits_{u}^{u+\omega_1} \frac{f'(z)}{f(z)}dz + \\
+ \omega_1 \int\limits_{u}^{u+\omega_2} \frac{f'(z)}{f(z)}dz = 2\pi\,\mathrm{i}(k_1\omega_1 + k_2\omega_2),
\end{aligned}$$

где $k_1, k_2 \in \mathbb{Z}$ (мы сделали замены переменной и воспользовались периодичностью f'/f). □

Поскольку эллиптическая функция должна иметь по крайней мере один полюс, из (i) мы немедленно получаем следующее

Следствие 4.7.6 *Эллиптическая функция имеет по крайней мере два полюса (с учетом кратностей).*

Построим пример эллиптической функции. Для этого рассмотрим ряд

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega\in\Omega\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{4.7.7}$$

Мы покажем, что $\wp(z)$ – эллиптическая функция. Она называется *функцией Вейерштрасса*.

Лемма 4.7.8 *Ряд*

$$\sum_{\omega\in\Omega\setminus\{0\}} \frac{1}{|\omega|^q} \tag{4.7.9}$$

сходится при $q > 2$.

Доказательство. Разобьем комплексную плоскость на круговые кольца

$$K_n := \{w \in \mathbb{C} \mid n-1 < |w| \le n\}.$$

и запишем частичные суммы нашего ряда в виде

$$\sum_{|\omega|\le N} \frac{1}{|\omega|^q} = \sum_{n=1}^{N} \sum_{\omega\in K_n} \frac{1}{|\omega|^q}. \tag{4.7.10}$$

Оценим число точек k_n решетки Ω в K_n. Существует $\delta > 0$ такое, что расстояние между любыми двумя различными точками Ω не меньше 2δ (докажите самостоятельно!). Следовательно, круги радиуса δ с центрами в точках $K_n \cap \Omega$ не пересекаются. Эти круги содержатся в кольце $\{w \in \mathbb{C} \mid n-1-\delta < |w| \le n+\delta\}$ площади

$$S_n = \pi(n+\delta)^2 - \pi(n-1-\delta)^2 = \pi(1+2\delta)(2n-1).$$

Отсюда получаем оценки для k_n и для слагаемых в (4.7.10):

$$k_n \le S_n/(\pi\delta^2) = \frac{1}{\delta^2}(1+2\delta)(2n-1) \le \frac{2}{\delta^2}(1+2\delta)n,$$

$$\sum_{\omega\in K_n} \frac{1}{|\omega|^q} \le \frac{k_n}{(n-1)^q} \le \frac{2}{\delta^2}(1+2\delta)\frac{n}{(n-1)^q} \le \frac{4}{\delta^2}\frac{1+2\delta}{(n-1)^{q-1}}.$$

Хорошо известно, что ряд $\sum \frac{1}{n^s}$ сходится при $s > 1$, поэтому сходится и ряд (4.7.9). □

Предложение 4.7.11 *Ряд в* (4.7.7) *сходится абсолютно и равномерно на любом компактном подмножестве в* $\mathbb{C} \setminus \Omega$.

Доказательство. Мы можем считать, что $|z| < R$ и $|z-\omega| > \epsilon$ для некоторых констант $R, \epsilon > 0$ и для всех $\omega \in \Omega$. Предположим, что $|\omega| > 4R$. Тогда $|2 - z/\omega| < 7/4$ и

$$|z-\omega|^2 \geq |\omega|^2 + |z|^2 - 2|z\omega| \geq |\omega|^2 - 2R|\omega| \geq \frac{1}{2}|\omega|^2.$$

Отсюда

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2-z/\omega)}{(z-\omega)^2\omega}\right| \leq \frac{7R}{2|\omega|^3}.$$

Для $0 < |\omega| \leq 4R$ члены ряда оцениваются следующим образом:

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \left|\frac{1}{(z-\omega)^2}\right| + \left|\frac{1}{\omega^2}\right| \leq \frac{1}{\epsilon^2} + \max_{0<|\omega|\leq 4R} \frac{1}{|\omega|^2}.$$

Таким образом, существует константа $c(\epsilon, R)$ такая, что $\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq c(\epsilon, R)$ для любых $z \in \mathbb{C}$, $\omega \in \Omega \setminus \{0\}$, удовлетворяющих условиям $|z| < R$ и $|z-\omega| > \epsilon$. По лемме 4.7.8 ряд

$$\sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{|\omega|^3}.$$

сходится. Согласно признаку равномерной сходимости Вейерштрасса, сходится и ряд в (4.7.7). □

Продифференцируем формально ряд (4.7.7):

$$\wp'(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}. \tag{4.7.12}$$

Аналогично предложению 4.7.11 доказывается следующее

Предложение 4.7.13 *Ряд в* (4.7.12) *сходится абсолютно и равномерно на любом компактном подмножестве в* $\mathbb{C} \setminus \Omega$.

Следствие 4.7.14 (i) *Функция* $\wp(z)$ *голоморфна на множестве* $\mathbb{C} \setminus \Omega$.

(ii) *Функция $\wp'(z)$ нечетна и Ω-периодична.*

(iii) *Функция $\wp(z)$ четна и также Ω-периодична.*

(iv) *Функция $\wp(z)$ имеет двойной полюс в точках решетки Ω.*

Доказательство. (i) получается из предложений 4.7.11 и 4.7.13. Для доказательства (ii) заметим, что при замене z на $z+\omega_i$ члены ряда (4.7.12) просто переставляются, а при замене z на $-z-$ меняют знак. Аналогично доказывается четность $\wp(z)$. Ω-периодичность функции $\wp'(z)$ очевидна. Для доказательства Ω-периодичности $\wp(z)$ рассмотрим функцию $f(z) := \wp(z+\omega_i) - \wp(z)$. Так как $f'(z) = \wp'(z+\omega_i) - \wp'(z) = 0$, то $f(z) = \mathrm{Const}$. С другой стороны, $\mathrm{Const} = f(-\frac{1}{2}\omega_i) = \wp(-\frac{1}{2}\omega_i) - \wp(\frac{1}{2}\omega_i) = 0$. Это доказывает (iii).

(iv) Зафиксируем $\omega_0 \in \Omega$ и рассмотрим функцию $g(z) := \wp(z) - (z-\omega_0)^{-2}$. Полностью повторяя доказательство предложения 4.7.11, можно показать, что ряд для $g(z)$ (аналогичный 4.7.7) сходится абсолютно и равномерно вблизи ω_0. Это показывает, что функция $g(z)$ непрерывна в ω_0. По теореме об аналитическом продолжении $g(z)$ голоморфна в ω_0. Таким образом, ω_0 – двойной полюс для $\wp(z)$. □

Теорема 4.7.15 *Поле эллиптических функций $\mathscr{E}_\Omega$ порождается функциями $\wp(z)$ и $\wp'(z)$: $\mathscr{E}_\Omega = \mathbb{C}(\wp, \wp')$. Подполе $\mathscr{E}_\Omega^+ \subset \mathscr{E}_\Omega$ четных эллиптических функций порождается $\wp(z)$.*

Доказательство. Во-первых, первое утверждение теоремы является легким следствием второго. Действительно, любая эллиптическая функция $f(z)$ представляется в виде

$$f(z) = \frac{f(z)+f(-z)}{2} + \wp'(z)\frac{f(z)-f(-z)}{2\wp'(z)},$$

где $\frac{f(z)+f(-z)}{2}$ и $\frac{f(z)-f(-z)}{2\wp'(z)}$ – четные эллиптические функции.

Таким образом, достаточно показать, что любая четная эллиптическая функция $g(z)$ выражается как рациональная дробь

от $\wp(z)$. Для этого мы построим функцию $g_1(z) \in \mathscr{E}_\Omega^+$, имеющую тот же набор особых точек, что и $g(z)$ (с учетом порядков). Тогда отношение $g(z)/g_1(z)$ не будет иметь особых точек и, поэтому, должно быть константой.

Конечно, нетривиальная функция $g(z)$ должна иметь бесконечное множество особых точек. Однако, мы их можем рассматривать по модулю решетки Ω и умножения на -1: порядки в точках $z = z_1$ и $z = \pm z_1 + \omega$ совпадают для всех $\omega \in \Omega$.

Пусть $\{z_1, \dots, z_r\}$ – множество всех особых точек функции $g(z)$ на множестве $\mathbb{C}\backslash\Omega$, выписанных по модулю преобразований $z \to \pm z + \omega$, т.е. мы считаем, что $z_i \not\equiv \pm z_j \mod \Omega$ при $i \neq j$. Припишем каждой точке z_i число m_i:

$$m_i := \begin{cases} \text{порядок } g(z) \text{ в } z_i, & \text{если } 2z_i \not\equiv 0 \mod \Omega \\ \frac{1}{2}(\text{порядок } g(z) \text{ в } z_i), & \text{если } 2z_i \equiv 0 \mod \Omega \end{cases}$$

Заметим, что по модулю решетки Ω имеется ровно три точки $\alpha \in \mathbb{C} \setminus \Omega$ с условием $2\alpha \equiv 0 \mod \Omega$:

$$\alpha \in \left\{ \frac{\omega_1}{2}, \quad \frac{\omega_2}{2}, \quad \frac{\omega_1 + \omega_2}{2} \right\}.$$

В такой точке порядок нуля (или полюса) четен. Действительно, пусть

$$g(z) = a_m(z-\alpha)^m + a_{m+1}(z-\alpha)^{m+1} + \cdots$$

– разложение Лорана в точке α, где $a_m \neq 0$. Так как функция g четна и Ω-периодична, то

$$g(z) = g(-z) = g(2\alpha - z) = a_m(\alpha - z)^m + a_{m+1}(\alpha - z)^{m+1} + \cdots$$

Это возможно только если $a_m(z-\alpha)^m = a_m(\alpha - z)^m$, т.е. m четно. Поэтому все m_i – целые.

Функция $\wp(z) - \wp(z_i)$ имеет ровно один полюс по модулю Ω и этот полюс имеет порядок 2 (см. (iv) следствия 4.7.14). По предложению 4.7.5 она имеет по модулю Ω ровно два нуля (с учетом кратностей). Легко видеть, что эти нули будут в точках z_i и $-z_i$ при $2z_i \not\equiv 0 \mod \Omega$ и двойной нуль в точке z_i при $2z_i \equiv 0 \mod \Omega$.

Положим

$$g_1(z) := \prod_{i=0}^{r} (\wp(z) - \wp(z_i))^{m_i}.$$

Тогда $g(z)$ и $g_1(z)$ имеют одинаковые порядки во всех точках z_i (и, очевидно, во всех точках $\mathbb{C} \setminus \Omega$). По предложению 4.7.5 они имеют одинаковые порядки и в точках Ω. Отсюда $g(z)/g_1(z) = \mathrm{Const}$. что и доказывает теорему. □

Следствие 4.7.16 (дифференциальное уравнение для $\wp$). *Существует кубический многочлен $f(t) \in \mathbb{C}[t]$ без кратных корней такой, что*

$$\wp'^2 = f(\wp), \tag{4.7.17}$$

Доказательство. Отметим, что эллиптическая функция $\wp'(z)^2$ является четной и имеет полюсы шестого порядка в точках решетки. В обозначениях доказательства теоремы 4.7.15 все m_i положительны и $\sum m_i = 3$. Отсюда

$$\wp'^2 = c(\wp - \wp(z_1))(\wp - \wp(z_2))(\wp - \wp(z_3)), \quad c \in \mathbb{C} \setminus \{0\},$$

т.е. $\wp'(z)^2$ выражается как кубический многочлен от $\wp(z)$. Предположим, что кубический многочлен $f(t)$ имеет кратный корень: $f(t) = c(t-a)^2(t-b)$. Тогда

$$\wp(z) - b = c^{-1} \left(\frac{\wp'(z)}{\wp(z) - a} \right)^2.$$

В этом случае эллиптическая функция $\wp'(z)/(\wp(z)-a)$ имеет по модулю Ω единственный полюс (в точках решетки). Это противоречит следствию 4.7.6. □

Рассмотрим на комплексной проективной плоскости с неоднородными координатами x, y эллиптическую кривую E, заданную уравнением $y^2 = f(x)$. Согласно следствию 4.7.16, функции $\wp$ и $\wp'$ задают отображение

$$\pi\colon (\mathbb{C}/\Omega) \setminus \{0\} \longrightarrow E \setminus \{\infty\}, \quad z \longmapsto (\wp(z), \wp'(z)). \tag{4.7.18}$$

Продолжим его до отображения $\pi\colon \mathbb{C}/\Omega \to E$, полагая $\pi(0) = \infty$. Теперь мы докажем следующую очень важную теорему.

Теорема 4.7.19 *Отображение π является биекцией и индуцирует изоморфизм полей $\mathscr{E}(\Omega)$ и $\mathbb{C}(E)$.*

Доказательство. Предположим, что $\wp(z_1) = \wp(z_2)$ и $\wp'(z_1) = \wp'(z_2)$ для некоторых $z_1 \not\equiv z_2 \mod \Omega$. Тогда $\wp - \wp(z_1)$ имеет двойной полюс в точках решетки и два простых нуля в z_1 и z_2. Функция $\wp' - \wp'(z_1)$ имеет тройной полюс в точках решетки и нули в z_1 и z_2. Но тогда отношение $(\wp - \wp(z_1))/(\wp' - \wp'(z_1))$ имеет лишь простые нули в точках решетки, что противоречит следствию 4.7.6. Это доказывает инъективность π.

Для доказательства сюръективности π рассмотрим точку $(x_0, y_0) \in E$. Функция $\wp(z) - x_0$ имеет (с учетом кратностей) ровно два нуля z_1, z_2 по модулю Ω. Таким образом, $\wp(z_1) = \wp(z_2) = x_0$. Отсюда $\wp'(z_i) = \pm y_0$. Предположим, что $\wp'(z_1) = \wp'(z_2) = -y_0$. Согласно доказанному выше это возможно только если $z_1 \equiv z_2 \mod \Omega$, т.е. z_1 – нуль кратности 2 для $\wp(z) - x_0$. Но тогда $\wp'(z_1) = 0 = y_0$. Противоречие доказывает сюръективность.

Наконец, несложно показать, что для каждой рациональной функции $\varphi\colon E \dashrightarrow \mathbb{C}$ композиция

$$\mathbb{C} \xrightarrow{\lambda} \mathbb{C}/\Omega \xrightarrow{\pi} E \overset{\varphi}{\dashrightarrow} \mathbb{C}$$

является эллиптической функцией. Это определяет вложение полей $\mathbb{C}(E) \hookrightarrow \mathscr{E}(\Omega)$. Так как $\mathbb{C}(E)$ является полем частных факторкольца $\mathbb{C}[x, y]/(y^2 - f(x))$, то оно порождается функциями x и y – образами $\wp$ и $\wp'$. Следовательно, вложение $\mathbb{C}(E) \hookrightarrow \mathscr{E}(\Omega)$ – изоморфизм. □

Поскольку риманова поверхность $\mathbb{C}/\Omega$ является также и группой, то теорема 4.7.19 дает еще одно описание группового закона на эллиптической кривой. Откуда немедленно получается

Следствие 4.7.20 *Имеют место следующие изоморфизмы групп $(E, O) \simeq \mathbb{C}/\Omega \simeq \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$.*

Иначе говоря, $\pi\colon (E, O) \to \mathbb{C}/\Omega$ является изоморфизмом групп.

Доказательство. Возьмем три (возможно совпадающие) точки P_1, P_2, $P_3 \in E$. Пусть z_1, z_2, $z_3 \in \mathbb{C}$ – прообразы этих точек. Мы можем выбрать их так, что они содержатся в основном параллелограмме Δ. Согласно упрощенному групповому закону, достаточно доказать, что если P_1, P_2, P_3 лежат на одной прямой L, то $z_1 + z_2 + z_3 = 0$. Пусть L задается (неоднородным) уравнением $\alpha x + \beta y + \gamma = 0$. Ясно, что $\alpha\wp(z_i) + \beta\wp'(z_i) + \gamma = 0$. Эллиптическая функция $f := \alpha\wp + \beta\wp' + \gamma$ имеет тройной полюс в элементах решетки Ω и не имеет других полюсов. Согласно предложению 4.7.5, все нули f в Δ (с учетом кратностей) исчерпываются точками z_1, z_2, z_3. Снова по предложению 4.7.5 имеем $z_1 + z_2 + z_3 = 0 \mod \Omega$. □

В заключение отметим, что многочлен $f(x)$ из следствия 4.7.16 допускает явное описание. Положим

$$G_k(\Omega) := \sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{\omega^{2k}}$$

По лемме 4.7.8 эти суммы сходятся абсолютно при $k > 1$. Они называются *рядами Эйзенштейна* веса k. Ясно, что они зависят от выбора решетки Ω. Далее пусть

$$g_2 := 60G_2, \qquad g_3 := 140G_3.$$

Теорема 4.7.21 (ср. теорема 4.2.3**)** *Точный вид соотношения* (4.7.17) *– следующий*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3, \tag{4.7.22}$$

Обратно, для любых g_2, $g_3 \in \mathbb{C}$ таких, что $g_2^3 - 27g_3^2 \neq 0$ существует решетка $\Omega \subset \mathbb{C}$, функция Вейерштрасса которой удовлетворяет соотношению (4.7.22).

Легко найти выражение дискриминанта и j-инварианта через g_2 и g_3:

$$\Delta = g_2^3 - 27g_3^2, \qquad j = 1728g_2^3/\Delta.$$

Исторически, эллиптические функции возникли при изучении *эллиптических интегралов*

$$\int_u^\infty \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}, \qquad g_2,\, g_3 \in \mathbb{C}.$$

Такой интеграл является многозначной функцией, ее значения определены по модулю некоторой решетки и обратной к ней является функция Вейерштрасса $\wp$.

Модулярная группа

Лемма 4.7.23 *Пусть Ω, $\Omega' \subset \mathbb{C}$ – полные решетки. Предположим, что существует нетривиальное голоморфное отображение $f\colon \mathbb{C}/\Omega \to \mathbb{C}/\Omega'$ такое, что $f(0) = 0$. Тогда существует $\alpha \in \mathbb{C} \setminus \{0\}$ такое, что $\alpha\Omega \subset \Omega'$, и коммутативная диаграмма*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\cdot\alpha} & \mathbb{C} \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda'} \\ \mathbb{C}/\Omega & \xrightarrow{f} & \mathbb{C}/\Omega' \end{array}$$

Доказательство. Вертикальные отображения в диаграмме существуют по конструкции факторов и они являются универсальными накрытиями. Поэтому, существует горизонтальное отображение $\tilde{f}\colon \mathbb{C} \to \mathbb{C}$ и оно непрерывно. Докажем, что $\tilde{f}$ голоморфно.

Зафиксируем $z_0 \in \mathbb{C}$. Положим $P := \lambda(z_0)$ и $P' := f(P)$. Пусть $z_0' \in \lambda'^{-1}(P')$ и пусть $U' \ni z_0'$ – достаточно малая окрестность z_0' такая, что $U' \cap (\omega' + U') = \varnothing$ для всех $\omega' \in \Omega' \setminus \{0\}$. Тогда ограничение $\lambda'|_{U'}\colon U' \to \lambda'(U')$ имеет обратное (голоморфное) отображение. Следовательно, в окрестности $\lambda^{-1}(f^{-1}(\lambda'(U')))$ точки z_0 отображение $\lambda'^{-1} \circ f \circ \lambda$ определено и является голоморфным.

Теперь мы докажем, что $\tilde{f}(z) = \alpha z$. Для любого $\omega \in \Omega$ имеем $\tilde{f}(z+\omega) - \tilde{f}(z) \in \Omega'$. Поскольку функция $\tilde{f}(z+\omega) - \tilde{f}(z)$ непрерывна, а множество Ω' дискретно, то это возможно только если $\tilde{f}(z+\omega) - \tilde{f}(z)$ – константа. Поэтому $\tilde{f}'(z+\omega) = \tilde{f}'(z)$, т.е. $\tilde{f}'$ эллиптическая голоморфная функция. Следовательно, $\tilde{f}' = \alpha$ – также константа. Таким образом, $\tilde{f}(z) = \alpha z$. Остальные утверждения очевидны. □

Будем говорить, что решетки Ω, $\Omega' \subset \mathbb{C}$ *эквивалентны*, если $\Omega' = \alpha\Omega$ для некоторого $\alpha \in \mathbb{C}$. По лемме 4.7.23 решетки

Ω, $\Omega' \subset \mathbb{C}$ эквивалентны тогда и только тогда, когда римановы поверхности $\mathbb{C}/\Omega$ и $\mathbb{C}/\Omega'$ изоморфны. Далее мы классифицируем решетки с точностью до отношения эквивалентности. Обозначим через $\mathfrak{H} \subset \mathbb{C}$ открытую верхнюю полуплоскость. Во первых заметим, что каждая решетка эквивалентна решетке $\Omega = \langle 1, \tau \rangle$. Заменяя τ на $-\tau$, можно добиться того, что $\tau \in \mathfrak{H}$.

Группа $SL_2(\mathbb{Z})$ целочисленных (2×2)-матриц с определителем 1 называется (полной) *модулярной группой*. Группа $SL_2(\mathbb{Z})$ действует на $\mathfrak{H}$ по правилу

$$Az = \frac{az+b}{cz+d}, \quad \text{где} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Действительно, хорошо известно и легко проверяемо, что эта формула задает действие $SL_2(\mathbb{C})$ на пополненной комплексной плоскости $\mathbb{C} \cup \{\infty\}$. С другой стороны,

$$\operatorname{Im}(Az) = \frac{\operatorname{Im} z}{|cz+d|^2}. \tag{4.7.24}$$

Поэтому полуплоскость $\mathfrak{H}$ переходит в себя при действии группы $SL_2(\mathbb{Z})$.

Найдем необходимое и достаточное условие для того, чтобы решетки $\Omega = \langle 1, \tau \rangle$ и $\Omega' = \langle 1, \tau' \rangle$, где τ, $\tau' \in \mathfrak{H}$, были эквивалентны. Пусть $\alpha\Omega = \Omega'$. Тогда $(\alpha, \alpha\tau)$ и $(1, \tau')$ – два $\mathbb{Z}$-базиса решетки Ω'. Они должны отличаться друг от друга невырожденными целочисленным преобразованием, т.е.

$$1 = d\alpha + c\alpha\tau, \qquad \tau' = b\alpha + a\alpha\tau, \quad a, b, c, d \in \mathbb{Z}.$$

Отсюда

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Обратная к этой матрице также должна быть целочисленной. Поэтому $\det A = \pm 1$. Как и в (4.7.24), имеем

$$\operatorname{Im} \tau' = \frac{(\det A)(\operatorname{Im} \tau)}{|c\tau + d|^2}$$

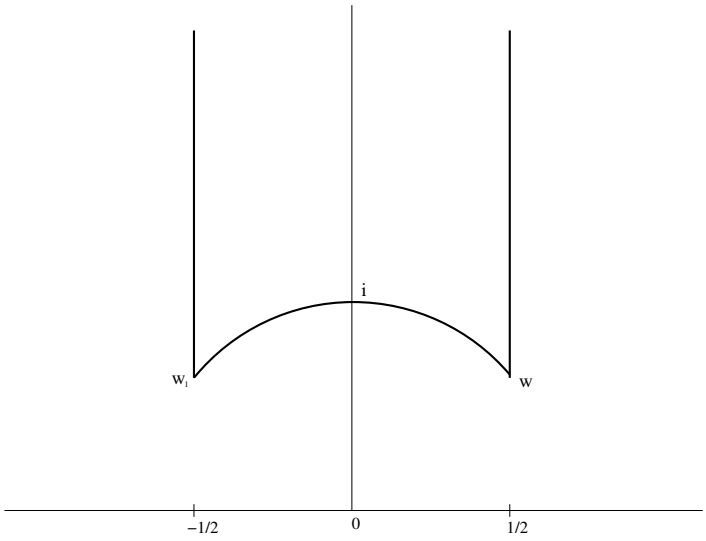


Рис. 4.5

Поскольку τ, $\tau' \in \mathfrak{H}$, то $\det A = 1$, т.е. τ и τ' отличаются друг от друга на преобразование из $SL_2(\mathbb{Z})$.

Будем говорить, что область $D \subset \mathfrak{H}$ является *фундаментальной* для действия $SL_2(\mathbb{Z})$, если каждая орбита $SL_2(\mathbb{Z})$ имеет хотя бы один элемент в D и два элемента из D принадлежат одной орбите тогда и только тогда, когда они лежат на границе D.

Предложение 4.7.25 (i) *Область*

$$D := \{z \mid -1/2 \le \operatorname{Re} z \le 1/2, \quad |z| \ge 1\} \subset \mathfrak{H}$$

(*см. рис.* 4.5) *является фундаментальной для действия* $SL_2(\mathbb{Z})$.

(ii) *Две различные точки* z_1, z_2 *на границе* D *принадлежат одной орбите только в следующих двух случаях:*

(a) $z_2 = z_1 \pm 1$, $|\operatorname{Re} z_i| = 1/2$,

(b) $|z_i| = 1$, $z_1 z_2 = -1$.

(iii) *Группа* $SL_2(\mathbb{Z})$ *порождается матрицами*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{и} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(iv) *Стационарная подгруппа* $\operatorname{St} z$ *точки* $z \in D$ *равна* $\{\pm\mathcal{E}\}$, *за исключением следующих трех случаев:*

(a) $\operatorname{St} z = \langle S \rangle$, $|\operatorname{St} z| = 4$ *при* $z = \mathrm{i}$,

(b) $\operatorname{St} z = \langle ST \rangle$, $|\operatorname{St} z| = 6$ *при* $z = w = -\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$,

(c) $\operatorname{St} z = \langle TS \rangle$, $|\operatorname{St} z| = 6$ *при* $z = \frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$.

(v) *Определяющие соотношения могут быть записаны в виде*

$$S^2 = (ST)^3 = -\mathcal{E}.$$

Доказательство. Пусть $\Gamma' \subset SL_2(\mathbb{Z})$ – подгруппа, порожденная матрицами S и T. Найдем пересечение орбиты $\Gamma' z$ точки $z \in \mathfrak{H}$ с нашей областью D. По определению имеем $T(z) = z + 1$ и $S(z) = -1/z$ для любой точки $z \in \mathfrak{H}$. Согласно (4.7.24) существует элемент $\Gamma' z$, для которого значение мнимой части максимально. Действительно, иначе существует последовательность $z_n \in \Gamma' z$ такая, что $\operatorname{Im} z_n$ строго возрастает. Так как T сохраняет мнимую часть, то $z_{n+1} = S z_n$. Но тогда $|z_n| < 1$ для любого n. Противоречие. Мы можем считать, что этот максимум достигается для z. Заменяя z на $T^k(z)$, мы можем также считать, что $-1/2 \leq \operatorname{Re} z \leq 1/2$. Но тогда $z \in D$. Действительно, иначе $|z| < 1$ и $\operatorname{Im} S(z) = \operatorname{Im} z/|z|^2 > \operatorname{Im} z$. Противоречие показывает, что $\Gamma' z \cap D \neq \varnothing$ для любой точки $z \in \mathfrak{H}$.

Рассмотрим две (необязательно различные) точки z_1, $z_2 \in D$ такие, что $A(z_1) = z_2$ для некоторого $A \in SL_2(\mathbb{Z})$. Мы можем считать, что $\operatorname{Im} z_2 \geq \operatorname{Im} z_1$. Из (4.7.24) получаем, что $|cz_1 + d| \leq 1$. Отсюда $|c| \leq 1$. Если $c = 0$, то $d = a = \pm 1$. Поэтому $\pm A = T^{\pm b}$ – сдвиг на $\pm b$. Так как $z_i \in D$, то либо $z_1 = z_2$ и $A = \pm\mathcal{E}$, либо $b = \pm 1$ и точки z_i лежат на вертикальных прямых $\operatorname{Re} z = \pm 1/2$.

Рассмотрим случай $c = \pm 1$. Тогда $|d| \leq 1$. Если $d = 0$, то $b = -c$, $|z_1| = 1$ и $A = \pm T^{\pm a} S$ (т.е. $A(z) = \pm a - 1/z$). Это возможно только если $a = 0$ или $a = \pm 1$ и $z_1 = z_2 = \pm\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$.

Пусть $d = c = \pm 1$. Тогда $b = a \mp 1$, $|z_1 + 1| \leq 1$ и $A(z) = \pm\frac{az+a\mp 1}{z+1}$. Так как z_1, $z_2 = A(z_1) \in D$, то либо $a = 0$ и $z_1 = z_2 = -\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$, либо $a = 1$ и $z_2 = z_1 + 1 = \frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$. Случай $b = -a$ рассматривается аналогично и оставляется читателю. Это доказывает утверждения (i), (ii) и (iv).

Для доказательства (iii) возьмем произвольную внутреннюю точку $z \in D$. Для любого $A \in SL_2(\mathbb{Z})$ орбита z относительно действия Γ' пересекается с D. Следовательно, существует $B \in \Gamma'$ такой, что $BA(z) \in D$. Так как D – фундаментальная область, то $BA(z) = z$. Из (iv) следует, что $BA = \pm\mathcal{E}$. Откуда $A \in \Gamma'$ и $\Gamma' = SL_2(\mathbb{Z})$. □

Упражнения. **(1)** Пусть $\Omega \subset \mathbb{C}$ – свободная подгруппа конечного ранга и пусть $f(z)$ – Ω-периодичная мероморфная функция. Докажите, что $\operatorname{rank}\Omega \leq 2$ и если $\operatorname{rank}\Omega = 2$, то Ω порождает $\mathbb{C}$, как векторное пространство над $\mathbb{R}$.

(2) Докажите, что по модулю решетки Ω нули функции $\wp'(z)$ – это в точности точки $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$ и порядок этих нулей равен 1.

(3) Как можно выразить $\wp''(z)$ через $\wp(z)$?

(4) Найдите количество точек порядка n на эллиптической кривой над $\mathbb{C}$.

(5) Пусть эллиптическая кривая E определена над $\mathbb{R}$. Какие возможности имеются для группы ее вещественных точек $E(\mathbb{R})$?

(6) Пусть $\overline{\Omega}$ – комплексно сопряженная решетка. Как связаны j-инварианты $\mathbb{C}/\Omega$ и $\mathbb{C}/\overline{\Omega}$?

(7) Чему изоморфен фактор $SL_2(\mathbb{Z})$ по коммутанту?

4.8. Теорема Римана-Роха на эллиптической кривой

Дивизоры

Пусть X – неособая проективная кривая. *Дивизором* на X называется (конечная) линейная комбинация $D = \sum_i n_i P_i$ точек $P_i \in X$ с коэффициентами $n_i \in \mathbb{Z}$. Все дивизоры на X образуют абелеву группу, которая обозначается через $\operatorname{Div}(X)$. Число

$\sum_i n_i$ называется *степенью* дивизора D. Таким образом, имеет место сюръективный гомоморфизм взятия степени

$$\deg\colon \operatorname{Div}(X) \longrightarrow \mathbb{Z}.$$

Его ядро обозначается через $\operatorname{Div}^0(X)$. Дивизор $D = \sum_i n_i P_i$ называется *эффективным* если $n_i \geq 0$ для всех i.

Для ненулевой рациональной функции $f \in \Bbbk(X)$, $f \notin \Bbbk$ обозначим $(f) := \sum\limits_P v_P(f)P$. По теореме 3.5.11 существует лишь конечное число точек таких, что $v_P(f) \neq 0$. Поэтому (f) – дивизор. Такие дивизоры называются *главными*. Они образуют подгруппу в $\operatorname{Div}(X)$. Факторгруппа группы всех дивизоров $\operatorname{Div}(X)$ по подгруппе главных дивизоров называется *группой Пикара* и обозначается через $\operatorname{Pic}(X)$. Будем говорить, что два дивизора $D = \sum n_i P_i$ и $H = \sum m_j P_j$ *линейно эквивалентны*, если $D - H$ – главный дивизор, т.е. $D - H = (f)$ для некоторой функции $f \in \Bbbk(X) \setminus \Bbbk$. Линейная эквивалентность дивизоров обозначается $D \sim H$. Это отношение является отношением эквивалентности (проверьте)! Более того, оно обладает следующим свойством согласованности со сложением: если $D \sim F$ и G – произвольный дивизор, то $D + G \sim F + G$. Так как степень главного дивизора равна нулю (теорема 3.5.11), то линейно эквивалентные дивизоры имеют одинаковую степень, а главные дивизоры содержатся в $\operatorname{Div}^0(X)$. Соответствующую факторгруппу $\operatorname{Div}^0(X)/\{\text{главные дивизоры}\}$ мы обозначим через $\operatorname{Pic}^0(X)$.

Пример 4.8.1 Пусть $X = \mathbb{P}^1$. Тогда $\Bbbk(X) \simeq \Bbbk(x)$ – поле рациональных функций. Для функции $f = (x-\alpha)/(x-\beta)$ имеются лишь два дискретных нормирования, не обращающихся в нуль на f: v_P и v_Q, где P и Q – точки $x = \alpha$ и $x = \beta$. Таким образом, $(f) = P - Q$. Отсюда несложно получить, что подгруппа главных дивизоров совпадает с подгруппой дивизоров степени нуль. Следовательно, гомоморфизм deg устанавливает изоморфизм $\operatorname{Pic}(X) \simeq \mathbb{Z}$ и $\operatorname{Pic}^0(X) = 0$.

Пример 4.8.2 Рассмотрим неособую плоскую кривую $X \subset \mathbb{P}^2$. Пусть L_1 и L_2 – две прямые на $\mathbb{P}^2$ (мы считаем, что L_1, $L_2 \neq X$).

Рассмотрим дивизоры $D_i = L_i \cap X$ (пересечение – с учетом кратностей). Тогда $D_1 \sim D_2$. Действительно, пусть L_i задается однородным уравнением $l_i(x, y, z) = 0$. Тогда l_1/l_2 – рациональная функция на X и мы имеем $D_1 = D_2 + (l_1/l_2)$.

Теорема 4.8.3 *Пусть X – неособая проективная кривая. Следующие условия равносильны*:

(i) $X \simeq \mathbb{P}^1$;

(ii) *любые две точки на X линейно эквивалентны*;

(iii) *существуют две различные линейно эквивалентные точки на X*;

(iv) *естественный гомоморфизм* $\deg\colon \operatorname{Pic} X \to \mathbb{Z}$ *является изоморфизмом.*

Доказательство. Импликации (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) и равносильность (ii) $\Leftrightarrow$ (iv) очевидны (см. пример 4.8.1). Докажем (iii) $\Rightarrow$ (i). Пусть $P_1 \sim P_2$. Тогда $P_1 - P_2 = (f)$ для некоторой ненулевой рациональной функции f. Рассмотрим отображение $\phi\colon X \to \mathbb{P}^1$, $P \to (f(P) : 1)$. Предположим, что $\phi(P) = \phi(P')$. Это означает, что $f(P) = f(P') = c$. Напомним, что каждая точка $Q \in X$ определяет дискретное нормирование v_Q поля $\Bbbk(X)$ такое, что $v_Q(g) \geq 0$ тогда и только тогда, когда функция g регулярна в Q. Имеем $v_{P_1}(f) = 1$, $v_{P_2}(f) = -1$ и $v_Q(f) = 0$ для любой точки $Q \neq P_1, P_2$. Положим $g := f - c$. Тогда $v_{P_2}(g) = \min(v_{P_2}(f), v_{P_2}(c)) = -1$ и $v_Q(g) \geq \min(v_Q(f), v_Q(c)) = 0$ для любой точки $Q \neq P_2$. Более того, $v_P(g) > 0$ и $v_{P'}(g) > 0$ (поскольку $g(P) = g(P') = 0$). Это противоречит теореме 3.5.11. $\square$

На множестве $\operatorname{Div}(X)$ всех дивизоров определено отношение частичной упорядоченности: $D = \sum d_i P_i \geq D' = \sum d'_i P_i$ если $d_i \geq d'_i$ для всех i (здесь допускаются нулевые коэффициенты). Зафиксируем дивизор D и рассмотрим множество

$$\mathscr{L}(D) = \{f \in \Bbbk(X)^* \mid D + (f) \geq 0\} \cup \{0\}.$$

Лемма 4.8.4 *Определенное выше множество $\mathscr{L}(D)$ является конечномерным векторным подпространством в $\Bbbk(X)$ (здесь $\Bbbk(X)$ рассматривается как бесконечномерное векторное пространство над $\Bbbk$).*

Доказательство. Пусть $f, g \in \mathscr{L}(D)^*$. Тогда $v_P(\alpha f + \beta g) \geq \min(v_P(f), v_P(g))$ для всех $\alpha, \beta \in \Bbbk$ и любой точки $P \in X$. Отсюда $D + (\alpha f + \beta g) \geq 0$ и $f + g \in \mathscr{L}(D)$, т.е. $\mathscr{L}(D)$ – векторное пространство. Доказательство конечномерности $\mathscr{L}(D)$ существенно более сложно. Мы его опускаем. □

Определение 4.8.5 Множество

$$|D| := \{F \in \mathrm{Div}(X) \mid F \geq 0,\, F \sim D\}$$

называется *полной линейной системой* дивизоров.

Переформулируя определение, можно записать

$$|D| = \{D + (f) \mid f \in \Bbbk(X)^*,\, D + (f) \geq 0\}.$$

Поэтому имеется естественное отображение

$$\mathscr{L}(D) \setminus \{0\} \longrightarrow |D|, \quad f \longmapsto D + (f).$$

При этом в один дивизор переходят пропорциональные функции из $\Bbbk(X)^*$. Следовательно, $|D|$ является проективизацией векторного пространства $\mathscr{L}(D)$, т.е. $|D|$ можно отождествить с множеством прямых в $\mathscr{L}(D)$, проходящих через начало координат. Через $\dim|D|$ будет обозначаться размерность линейной системы $|D|$ как проективного пространства. Для единообразия мы положим $\dim|D| = -1$, если $|D| = \varnothing$ и $\dim|D| = 0$, если $|D|$ – точка. Таким образом, всегда $\dim|D| = \dim\mathscr{L}(D) - 1$.

Множество точек, имеющих ненулевые коэффициенты в дивизоре D, называется *носителем* D и обозначается $\mathrm{Supp}(D)$. Если линейная система $|D|$ непуста, то множество

$$\mathrm{Bs}\,|D| := \bigcap_{F \in |D|} \mathrm{Supp}(F)$$

называется ее *базисным множеством*.

Пример 4.8.6 Поскольку любые две точки на $\mathbb{P}^1$ линейно эквивалентны, то любая непустая линейная система $|D|$ на $\mathbb{P}^1$ состоит из *всех* дивизоров степени $\deg D$. В частности, если $\deg D \geq 0$, то $\dim |D| = \deg D$. Любая непустая линейная система на $\mathbb{P}^1$ не имеет базисных точек.

4.8.7 Следующие свойства вытекают непосредственно из определения:

(i) $D \sim D' \implies |D| = |D'|$;

(ii) $|D| \neq \varnothing \implies \deg D \geq 0$;

(iii) если же $|D| \neq \varnothing$ и $\deg D = 0$, то $D \sim 0$;

(iv) $|D| \neq \varnothing$ и $|-D| \neq \varnothing \implies D \sim 0$;

(v) $D \geq D' \implies \mathscr{L}(D) \supset \mathscr{L}(D')$ и $\dim |D| \geq \dim |D'|$;

(vi) если $D \geq D'$ и $\dim |D| = \dim |D'|$, то любой элемент $F \in |D|$ единственным образом представляется в виде $F = F' + (D - D')$, где $F' \in |D'|$, а $D - D'$ – эффективный дивизор.

Лемма 4.8.8 *Для любого дивизора $D \in \operatorname{Div}(X)$ и любой точки $P \in X$ имеем*

$$\dim |D| \leq \dim |D + P| \leq \dim |D| + 1.$$

Более того, если линейная система $|D + P|$ непуста и P не является ее базисной точкой, то имеет место равенство $\dim |D + P| = \dim |D| + 1$.

Доказательство. Ясно, что мы можем считать дивизор D эффективным. Пусть $n \geq 0$ – коэффициент P в D. Тогда $\mathscr{L}(D + P) \supset \mathscr{L}(D)$, и

$$\mathscr{L}(D + P) \subset \{f \in \Bbbk(X)^* \mid v_P(f) \geq -n - 1\},$$
$$\mathscr{L}(D) = \{f \in \mathscr{L}(D + P) \mid v_P(f) \geq -n\}.$$

Пусть t – локальный параметр (т.е. порождающий элемент максимального идеала $\mathfrak{m}_{P,X} \subset \mathscr{O}_{P,X}$). Тогда $v_P(t) = 1$. Поэтому

$t^{n+1} \cdot f$ – регулярная в точке P функция для всех $f \in \mathscr{L}(D+P)$ и

$$\mathscr{L}(D) = \{f \in \mathscr{L}(D+P) \mid v_P(t^n \cdot f) \geq 0\}.$$

Таким образом, подпространство $\mathscr{L}(D) \subset \mathscr{L}(D+P)$ является множеством нулей линейной функции

$$\mathscr{L}(D+P) \longrightarrow \Bbbk, \quad f \longmapsto (t^{n+1} \cdot f)(P) = t(P)^{n+1} \cdot f(P).$$

Отсюда немедленно получается требуемое неравенство $\dim \mathscr{L}(D) \geq \dim \mathscr{L}(D+P) - 1$. Последнее утверждение следует из (iv) 4.8.7. □

Следствие 4.8.9 *Пусть D – дивизор на неособой проективной кривой. Тогда $\dim |D| \leq \deg D$. Если имеет место равенство, то кривая рациональна.*

Доказательство. Индукция по $\deg D$. □

Теорема 4.8.10 (Римана-Роха) *Пусть E – (неособая) эллиптическая кривая и пусть D – дивизор на E. Тогда*

$$\dim |D| - \dim |-D| = \deg D.$$

Доказательство. Замена D на $-D$ лишь меняет знаки в обеих частях равенства. Поэтому мы можем считать, что $\deg D \geq 0$.

Лемма 4.8.11 *Для любых трех (необязательно различных) точек P_1, P_2, Q_1 на эллиптической кривой E существует четвертая точка Q_2 такая, что $P_1 + P_2 \sim Q_1 + Q_2$.*

Доказательство. Проведем через P_1 и P_2 прямую L на $\mathbb{P}^2$ и пусть O – третья точка пересечения L и E (все учитывается с кратностями). Далее проведем прямую L' через O и Q_1 и пусть Q_2 – третья точка пересечения L' и E. Тогда $P_1+P_2+O = E \cap L$ и $Q_1 + Q_2 + O = E \cap L'$. Отсюда $P_1 + P_2 + O \sim Q_1 + Q_2 + O$ и $P_1 + P_2 \sim Q_1 + Q_2$. □

Следствие 4.8.12 *Пусть D – дивизор степени ≥ 1 на эллиптической кривой. Тогда линейная система $|D|$ непуста. Если $\deg D \geq 2$, то $|D|$ не имеет базисных точек.*

Доказательство. Запишем $D = D^+ - D^-$, где D^+ и D^- – эффективные дивизоры без общих точек (такая запись единственна). Тогда $\deg D = \deg D^+ - \deg D^- \geq 1$. Если $D^- \neq 0$, то $\deg D^+ \geq 2$. Выберем точку $Q_1 \in \operatorname{Supp}(D^-)$ и точки P_1, P_2 такие, что $D^+ \geq P_1 + P_2$. По лемме $D \sim (D^+ - P_1 - P_2) + (D^- - Q_1) + Q_2$. Заменим D новым дивизором в левой части. Продолжая процесс добьемся того, что $D^- = 0$, т.е. дивизор D эффективен.

Пусть теперь $\deg D \geq 2$. Достаточно доказать, что для любых двух точек P_1, P_2 на эллиптической кривой линейная система $|P_1 + P_2|$ не имеет базисных точек. Действительно, по лемме для любой точки Q_1 существует точка Q_2 такая, что $P_1 + P_2 \sim Q_1 + Q_2$. Мы можем взять Q_1 так, что $Q_1 \neq P_1$, P_2. Если же $Q_2 = P_2$, то $P_1 \sim Q_1$. Противоречие. Следовательно, $\operatorname{Bs}|P_1 + P_2| \subset \{P_1, P_2\} \cap \{Q_1, Q_2\} = \varnothing$. □

Закончим доказательство теоремы. Для $\deg D = 0$ имеем $\dim|D| = \dim|-D|$ по (iii)-(iv) 4.8.7. Пусть $\deg D > 0$. Тогда $|-D| = \varnothing$ и достаточно доказать $\dim|D| = \deg D - 1$. Из следствия 4.8.9 имеем $\dim|D| \leq \deg D - 1$. Далее применим индукцию по $\deg D$. Для $\deg D = 1$ из следствия 4.8.12 вытекает $\dim|D| = 0$. Если же $\deg D \geq 2$, то по следствию 4.8.12 линейная система $|D|$ не имеет базисных точек, а по лемме 4.8.8 $\dim|D| = \dim|D - P| + 1$. Это и является шагом индукции. □

Напомним, что через $\operatorname{Pic}^0(E)$ обозначается ядро естественного гомоморфизма $\deg\colon \operatorname{Pic}(E) \to \mathbb{Z}$.

Теорема 4.8.13 *Пусть E – эллиптическая кривая. Зафиксируем точку $O \in E$. Композиция*

$$p\colon (E, O) \longrightarrow \operatorname{Div}^0(E) \longrightarrow \operatorname{Pic}^0(E), \qquad P \longmapsto P - O$$

является изоморфизмом групп (E, O) и $\operatorname{Pic}^0(E)$.

Доказательство. Покажем, что наша конструкция задает тот же групповой закон, что и построенный ранее. Пусть $P+Q=\overline{R}$. Тогда тройки точек P, Q, R и O, R, $\overline{R}$ высекаются прямыми на E. Но это означает, что $P+Q+R\sim O+R+\overline{R}$. Тогда $P+Q\sim O+\overline{R}$. Перепишем последнее в виде $(P-O)+(Q-O)\sim\overline{R}-O$ или $p(P)+p(Q)=p(\overline{R})$.

Докажем сюръективность. Рассмотрим дивизор D степени 0. По теореме Римана-Роха $\dim|D+O|=\dim|D+O|-\dim|-D-O|=\deg(D+O)-1=0$. Следовательно, $|D+O|\neq\varnothing$ и поэтому существует эффективный дивизор D' линейно эквивалентный $D+O$. Так как степень D' равна 1, то $D'=P$ – точка. Это означает, что $D\sim P-O$, т.е. p сюръективно.

Наконец, докажем инъективность. Предположим, что $p(P)=p(P')$. Это означает, что $P-O\sim P'-O$, т.е. $P\sim P'$. Так как кривая E нерациональна, то это дает нам $P=P'$. $\square$

Таким образом биекция p задает групповую структуру на эллиптической кривой E. Отметим, что эта конструкция зависит от выбора точки O. Однако, при любом выборе O мы получаем изоморфные группы.

Упражнения. **(1)** Докажите аналог теоремы 4.8.10 для неприводимых кубических кривых кривых с особенностями (см. упражнения (3) и (4), стр. 92. Выведите отсюда существование группового закона на таких кривых. *Указание.* Нужно рассмотривать дивизоры, содержащиеся в неособой части.

(2) Пусть X – эллиптическая кривая над $\mathbb{C}$. Какую интерпретацию имеют пространства $\mathscr{L}(D)$ в терминах эллиптических функций соответствующей решетки?

Литература

BSS00. I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, *London Mathematical Society Lecture Note Series*. V. **265**. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

Sil86. J. H. Silverman. *The arithmetic of elliptic curves*, *Graduate Texts in Mathematics*. V. **106**. Springer-Verlag, New York, 1986.

Кос01. А. И. Кострикин. *Введение в алгебру. Часть III. Основные структуры.* Физ.-Мат. Лит., Москва, 2001.

Лен68. С. Ленг. *Алгебра.* Мир, Москва, 1968.

Рид91. М. Рид. *Алгебраическая геометрия для всех.* Современная математика. Вводные курсы. Мир, Москва, 1991.

Шаб76. Б. В. Шабат. *Введение в комплексный анализ. Т. 1.* Наука, Москва, 1976.

Шаф88. И. Р. Шафаревич. *Основы алгебраической геометрии. Алгебраические многообразия в проективном пространстве. Т. 1.* Наука, Москва, 2-е издание, 1988.

Прохоров Юрий Геннадьевич
Эллиптические кривые и криптография. Семестр 1.
М., Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 144 стр.

Оригинал макет изготовлен издательской группой механико-математического факультета МГУ

Подписано в печать 12.11.2007 г.
Формат 60×90 1/16. Объем 9 п.л.
Заказ 19 Тираж 100 экз.

Издательство ЦПИ при механико–математическом факультете МГУ
г. Москва, Воробьевы горы.
Лицензия на издательскую деятельность ИД № 04059 от 20.02.2001 г.

Отпечатано на типографском оборудовании механико-математического факультета