

### §3. Многочлены и расширения полей

Всюду в этом параграфе мы обозначаем через  $K$  произвольное коммутативное кольцо с единицей, а через  $\mathbb{k}$  — произвольное поле.

**3.1. Степенные ряды и многочлены.** Бесконечное выражение вида

$$A(x) = \sum_{v \geq 0} a_v x^v = a_0 + a_1 x + a_2 x^2 + \dots \quad \text{с } a_i \in K \quad (3-1)$$

называется *формальным степенным рядом* от переменной  $x$  с коэффициентами в кольце  $K$ . Два формальных степенных ряда

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ B(x) &= b_0 + b_1 x + b_2 x^2 + \dots \end{aligned} \quad (3-2)$$

*равны*, если  $a_i = b_i$  для всех  $i$ . Сложение и умножение рядов (3-2) определяется стандартными правилами раскрытия скобок и приведения подобных слагаемых: коэффициенты рядов  $A(x) + B(x) = s_0 + s_1 x + s_2 x^2 + \dots$  и  $A(x)B(x) = p_0 + p_1 x + p_2 x^2 + \dots$  суть<sup>1</sup>

$$\begin{aligned} s_m &= a_m + b_m \\ p_m &= \sum_{\alpha + \beta = m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \dots + a_m b_0 \end{aligned} \quad (3-3)$$

Упражнение 3.1. Убедитесь, что операции (3-3) удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной  $x$  с коэффициентами в кольце  $K$  обозначается через  $K[[x]]$ . Начальный коэффициент  $a_0$  ряда (3-1) называется *свободным членом* этого ряда. Первый ненулевой коэффициент ряда  $A$  называется *младшим коэффициентом*.

Если в кольце  $K$  нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца тоже является целостным.

Кольцо  $K[[x_1, x_2, \dots, x_n]]$  формальных степенных рядов от  $n$  переменных  $x_1, x_2, \dots, x_n$  определяется по индукции:  $K[[x_1, x_2, \dots, x_n]] = K[[x_1, x_2, \dots, x_{n-1}]][[x_n]]$  и представляет собой множество формальных сумм вида

$$F(x) = \sum_{v_1, \dots, v_n \in \mathbb{Z}_{\geq 0}} a_{v_1 \dots v_n} x_1^{v_1} x_2^{v_2} \dots x_n^{v_n}.$$

**3.1.1. Алгебраические операции над формальными рядами.** Назовём  $n$ -арной *алгебраической операцией* в  $K[[x]]$  всякое правило, сопоставляющее рядам  $f_1, f_2, \dots, f_n \in K[[x]]$  новый ряд  $g \in K[[x]]$  так, что каждый коэффициент ряда  $g$  вычисляется по коэффициентам рядов  $f_1, f_2, \dots, f_n$  при помощи конечного числа сложений и умножений (возможно, зависящего от номера коэффициента).

<sup>1</sup>формально говоря, мы определяем здесь операции над *последовательностями*  $(a_v)$  и  $(b_v)$  элементов кольца  $K$ , а буква  $x$  используется лишь для облегчения восприятия этих операций

Например, сложение и умножение рядов — это алгебраические операции, а подстановка вместо  $x$  численного значения  $\alpha \in K$  алгебраической операцией обычно не является<sup>2</sup>. Напротив, подстановка в ряд  $f(x)$  вместо  $x$  любого ряда без свободного члена  $g(x) = b_1x + b_2x^2 + \dots$  — это алгебраическая операция, дающая ряд

$$\begin{aligned} f(g(x)) &= \sum a_k (b_1x + b_2x^2 + \dots)^k = \\ &= a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 + \dots \\ &= a_0 + (a_1b_1) \cdot x + (a_1b_2 + a_2b_1^2) \cdot x^2 + (a_1b_3 + 2a_2b_1b_2 + a_3b_1^3) \cdot x^3 + \dots, \end{aligned}$$

в котором на коэффициент при  $x^m$  влияют лишь начальные члены первых  $m$  слагаемых. Ещё одним примером алгебраической операции является обращение рядов.

**Предложение 3.1**

Ряд  $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[[x]]$  тогда и только тогда обратим в  $K[[x]]$ , когда его свободный член  $a_0$  обратим в  $K$ . Если обратный ряд существует, то операция обращения  $f \mapsto f^{-1}$  является алгебраической.

**Доказательство.** Если существует ряд  $f^{-1}(x) = b_0 + b_1x + b_2x^2 + \dots$ , такой что  $f(x) \cdot f^{-1}(x) = 1$ , то  $a_0b_0 = 1$ , откуда  $a_0$  обратим. Наоборот, допустим, что  $a_0 \in K$  обратим. Приравнявая коэффициенты при одинаковых степенях  $x$  в правой и левой части равенства

$$(a_0 + a_1x + a_2x^2 + \dots) \cdot (b_0 + b_1x + b_2x^2 + \dots) = 1,$$

мы получаем на коэффициенты  $b_i$  бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \dots &\dots \dots \dots \end{aligned} \tag{3-4}$$

из которой  $b_0 = a_0^{-1}$  и  $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$  при  $k \geq 1$ . Это позволяет рекурсивно вычислить все коэффициенты.  $\square$

**Упражнение 3.2.** Вычислите в  $\mathbb{Q}[[x]]$  а)  $(1-x)^{-1}$  б)  $(1-x^2)^{-1}$  в)  $(1-x)^{-2}$ .

**3.1.2. Многочлены.** Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от переменных  $x_1, x_2, \dots, x_n$  с коэффициентами в кольце  $K$  образуют в кольце всех формальных степенных рядов подкольцо, которое обозначается

$$K[x_1, x_2, \dots, x_n] \subset K[[x_1, x_2, \dots, x_n]]$$

Многочлен от одной переменной  $x$  представляет собой формальное выражение вида

$$f(x) = a_0 + a_1x + \dots + a_nx^n.$$

<sup>2</sup>очевидным исключением из этого правила служит вычисление значения ряда  $f(x)$  при  $x = 0$ , дающее в качестве результата свободный член этого ряда; похожий эффект иногда возникает при вычислении значений некоторых очень специальных рядов в некоторых очень специальных точках  $\alpha$ ; но при произвольных  $\alpha$  и  $f$  вычисление  $f(\alpha)$  требует, вообще говоря, выполнения бесконечно большого количества сложений

Последний ненулевой коэффициент этого выражения называется *старшим* коэффициентом многочлена  $f$ , а его номер называется *степенью* многочлена  $f$  и обозначается  $\deg f$ . Многочлены со старшим коэффициентом 1 называются *приведёнными*. Многочлены степени нуль называются *константами*.

Предложение 3.2

Если кольцо  $K$  целостное<sup>1</sup>, то для любых многочленов  $f_1, f_2 \in K[x]$  выполняется равенство  $\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)$ . В частности, кольцо  $K[x]$  тоже целостное, и его обратимыми элементами являются только обратимые константы.

Доказательство. Все утверждения следуют из того, что старший коэффициент произведения равен произведению старших коэффициентов сомножителей.  $\square$

Упражнение 3.3. Покажите, что в кольце  $\mathbb{Z}[x, y]$  двучлен  $(y^n - x^n)$  делится нацело на двучлен  $(y - x)$  и найдите частное.

**3.1.3. Дифференциальное исчисление.** Подставим в степенной ряд

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

вместо  $x$  сумму  $x + t$ , где  $t$  — ещё одна переменная. Получится ряд

$$f(x + t) = a_0 + a_1(x + t) + a_2(x + t)^2 + \dots \in K[[x, t]].$$

Раскроем в нём все скобки и сгруппируем слагаемые по степеням переменной  $t$ , обозначив через  $f_m(x) \in K[[x]]$  ряд, возникающий как коэффициент при  $t^m$ :

$$f(x + t) = f_0(x) + f_1(x) \cdot t + f_2(x) \cdot t^2 + f_3(x) \cdot t^3 + \dots = \sum_{i \geq 0} f_m(x) \cdot t^m. \quad (3-5)$$

Упражнение 3.4. Убедитесь, что  $f_0(x) = f(x)$  совпадает с исходным рядом  $f$ .

Ряд  $f_1(x)$  называется *производной* от исходного ряда  $f$  и обозначается  $f'$  или  $\frac{d}{dx}f$ . Он однозначно определяется равенством

$$f(x + t) = f(x) + f'(x) \cdot t + (\text{члены, делящиеся на } t^2)$$

и может быть вычислен при помощи [упр. 3.3](#) как значение при  $t = 0$  ряда

$$\begin{aligned} \frac{f(x + t) - f(x)}{t} &= a_1 \cdot \frac{(x + t) - x}{t} + a_2 \cdot \frac{(x + t)^2 - x^2}{t} + a_3 \cdot \frac{(x + t)^3 - x^3}{t} + \dots = \\ &= \sum_{k \geq 1} a_k \cdot ((x + t)^{k-1} + (x + t)^{k-2}x + (x + t)^{k-3}x^2 + \dots + x^{k-1}). \end{aligned}$$

Получаем хорошо известную формулу

$$f'(x) = \sum_{k \geq 1} k a_k x^{k-1} = a_1 + 2 a_2 x + 3 a_3 x^2 + \dots \quad (3-6)$$

<sup>1</sup>т. е. с единицей и без делителей нуля

Пример 3.1 (ряды с нулевой производной)

Из формулы (3-6) вытекает, что производная от константы равна нулю. Если  $\text{char } K = 0$ , то верно и обратное:  $f' = 0$  тогда и только тогда, когда  $f = \text{const}$ . Однако, когда кольцо  $K$  имеет положительную характеристику, производная от всех мономов  $x^m$ , показатель которых делится на характеристику, обращается в нуль, поскольку согласно проделанному выше вычислению коэффициент  $m$  в формуле

$$\frac{d}{dx} x^m = \underbrace{x^{m-1} + \dots + x^{m-1}}_m = m \cdot x^{m-1}$$

представляет собою сумму  $m$  единиц кольца. В частности, над полем  $\mathbb{k}$  характеристики  $p > 0$  производная от ряда  $f(x)$  равна нулю тогда и только тогда, когда

$$\exists g \in \mathbb{k}[[x]] : f(x) = g(x^p) = g(x)^p \quad (3-7)$$

(второе равенство справедливо, поскольку возведение в  $p$ -ю степень является гомоморфизмом).

Предложение 3.3 (правила дифференцирования)

Для любого  $\alpha \in K$  и любых  $f, g \in K[[x]]$  справедливы равенства

$$(\alpha f)' = \alpha \cdot f', \quad (f + g)' = f' + g', \quad (fg)' = f' \cdot g + f \cdot g'. \quad (3-8)$$

Кроме того, если ряд  $g$  не имеет свободного члена, то

$$(f(g(x)))' = g'(x) \cdot f'(g(x)), \quad (3-9)$$

а если ряд  $f$  обратим, то

$$\frac{d}{dx} f^{-1} = -f' / f^2. \quad (3-10)$$

Доказательство. Первые два равенства в (3-8) вытекают прямо из формулы (3-6). Для доказательства третьего перемножим ряды

$$\begin{aligned} f(x+t) &= f(x) + t \cdot f'(x) + (\text{члены, делящиеся на } t^2) \\ g(x+t) &= g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2). \end{aligned}$$

С точностью до членов, делящихся на  $t^2$ , получим

$$f(x+t)g(x+t) = f(x)g(x) + t \cdot (f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } t^2),$$

откуда  $(fg)' = f' \cdot g + f \cdot g'$ . Формула (3-9) доказывается похожим образом. Подставим в  $f(x)$  вместо  $x$  ряд  $g(x+t)$ :  $f(g(x+t)) = f(g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2))$  и обозначим ряд, который прибавляется к  $g(x)$  в аргументе  $f$ , через

$$\tau(x, t) = t \cdot g'(x) + (\text{члены, делящиеся на } t^2).$$

Тогда

$$\begin{aligned} f(g(x+t)) &= f(g(x) + \tau(x, t)) = \\ &= f(g(x)) + \tau(x, t) \cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x, t)^2) = \\ &= f(g(x)) + t \cdot g'(x) \cdot f'(g(x)) + (\text{члены, делящиеся на } t^2), \end{aligned}$$

откуда  $(f(g(x)))' = g'(x) \cdot f'(g(x))$ . Для доказательства формулы (3-10) продифференцируем обе части равенства  $f \cdot f^{-1} = 1$ . Получим  $f' \cdot f^{-1} + f \cdot (f^{-1})' = 0$ , откуда  $(f^{-1})' = -f'/f^2$ .  $\square$

Упражнение 3.5. Покажите, что в разложении (3-5)  $f_m(x) = \frac{1}{m!} \frac{d^m}{dx^m} f(x)$  (здесь и далее через  $\frac{d^m}{dx^m} = \left(\frac{d}{dx}\right)^m$  обозначается  $m$ -тая производная, т. е. результат  $m$ -кратного применения операции  $\frac{d}{dx}$ ).

**3.2. Делимость в кольце многочленов.** Известная из школы процедура деления многочленов «уголком» может быть формализована следующим образом.

Предложение 3.4 (деление с остатком)

Пусть  $K$  — произвольное коммутативное кольцо с единицей, и многочлен  $u \in K[x]$  имеет обратимый старший коэффициент. Тогда для любого многочлена  $f \in K[x]$  существуют многочлены  $q \in K[x]$  и  $r \in K[x]$ , такие что  $f = u \cdot q + r$  и либо  $\deg(r) < \deg(u)$ , либо  $r = 0$ . Если кольцо  $K$  целостное, то такие  $q$  и  $r$  определяются по  $f$  и  $u$  однозначно.

Доказательство. При  $\deg f < \deg u$  можно взять  $q = 0$  и  $r = f$ . Далее по индукции можно считать, что  $q$  и  $r$  существуют для всех многочленов  $f$  степени  $\deg f < n$ , где  $n \geq \deg u$ . Если  $f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  и  $u = b_0x^k + b_1x^{k-1} + \dots + b_{k-1}x + b_k$ , то степень многочлена  $f - a_0b_0^{-1}x^{n-k}u$  строго меньше  $n$ , и по индукции он представляется в виде  $qu + r$  с  $r = 0$  или  $\deg r < \deg u$ . Тогда  $f = (q + a_0b_0^{-1}x^{n-k}) \cdot u + r$  также представляется в требуемом виде. Если кольцо  $K$  целостное, и  $p, s$  — другая пара многочленов, таких что  $\deg(s) < \deg(u)$  и  $up + s = f = uq + r$ , то  $u(q - p) = r - s$ . При  $p - q \neq 0$  степень многочлена в левой части не менее  $\deg u$ , т. е. строго больше, чем степень многочлена в правой части. Следовательно,  $p - q = 0$ , откуда и  $r - s = 0$ .  $\square$

Определение 3.1

Многочлены  $q$  и  $r$ , удовлетворяющие условиям предл. 3.4 называются *неполным частным остатком* от деления  $f$  на  $u$  в  $K[x]$ .

Следствие 3.1

Для любых многочленов  $f, g \in \mathbb{k}[x]$  с коэффициентами в произвольном поле  $\mathbb{k}$  существует единственная пара многочленов  $q, r \in \mathbb{k}[x]$ , таких что  $f = g \cdot q + r$  и либо  $\deg(r) < \deg(g)$ , либо  $r = 0$ .

Пример 3.2 (вычисление значения многочлена в точке)

Остаток от деления любого многочлена  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  на линейный двучлен  $u(x) = x - \alpha$  — это константа, равная значению  $f(\alpha)$  многочлена  $f$  при  $x = \alpha$ , в чём легко убедиться, подставляя  $x = \alpha$  в равенство  $f(x) = (x - \alpha) \cdot q(x) + r$ . Отметим, что «деление уголком» является значительно более быстрым способом вычисления  $f(\alpha)$ , чем лобовая подстановка  $x = \alpha$  в  $a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ .

Упражнение 3.6 (схема Горнера). Убедитесь, что

$$f(\alpha) = a_0 + \alpha \cdot \left( a_1 + \alpha \cdot \left( a_2 + \dots + \alpha \cdot \left( a_{n-2} + \alpha \cdot \left( a_{n-1} + \alpha \cdot a_n \right) \dots \right) \right) \right)$$

Предложение 3.5

Пусть  $\mathbb{k}$  — произвольное поле. Для любого набора многочленов  $f_1, f_2, \dots, f_n \in \mathbb{k}[x]$  существует единственный приведённый многочлен  $d \in \mathbb{k}[x]$ , который делит каждый из многочленов  $f_i$  и делится на любой многочлен, делящий каждый из многочленов  $f_i$ . Многочлен  $d$  представляется в виде

$$f_1 h_1 + f_2 h_2 + \dots + f_n h_n, \quad \text{где } h_i \in \mathbb{k}[x]. \quad (3-11)$$

Произвольно взятый многочлен  $g \in \mathbb{k}[x]$  представим в виде (3-11) тогда и только тогда, когда он делится на  $d$ .

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены.

Существование доказывается тем же рассуждением, что и в н° 2.4.2. Обозначим множество всех многочленов  $g \in \mathbb{k}[x]$ , представимых в виде (3-11), через

$$(f_1, f_2, \dots, f_n) = \{f_1 h_1 + f_2 h_2 + \dots + f_n h_n \mid h_i \in \mathbb{k}[x]\}. \quad (3-12)$$

Это подкольцо в  $\mathbb{k}[x]$ , содержащее вместе с каждым многочленом  $g$  и все кратные ему многочлены  $hg$  (с любым  $h \in \mathbb{k}[x]$ ). Кроме того,  $(f_1, f_2, \dots, f_n)$  содержит каждый из многочленов  $f_i$ , и все многочлены из  $(f_1, f_2, \dots, f_n)$  делятся на любой общий делитель всех многочленов  $f_i$ . Возьмём в качестве  $d$  приведённый многочлен наименьшей степени в  $(f_1, f_2, \dots, f_n)$ . Остаток  $r = g - qd$  от деления произвольного многочлена  $g \in (f_1, f_2, \dots, f_n)$  на  $d$  лежит в  $(f_1, f_2, \dots, f_n)$ . Так как его степень не может быть строго меньше  $\deg d$ , он нулевой. Тем самым, все многочлены в  $(f_1, f_2, \dots, f_n)$  делятся на  $d$ .  $\square$

Определение 3.2

Многочлен  $d$  из предл. 3.5 называется *наибольшим общим делителем* многочленов  $f_i$  и обозначается  $\text{нод}(f_1, f_2, \dots, f_n)$ .

**3.2.1. Взаимная простота.** Из предл. 3.5 вытекает, что в кольце  $\mathbb{k}[x]$  многочленов с коэффициентами в поле *взаимная простота* многочленов  $f_1, f_2, \dots, f_m$ , т. е. возможность представить единицу в виде  $1 = h_1 f_1 + h_2 f_2 + \dots + h_n f_n$ , равносильна равенству  $\text{нод}(f_1, f_2, \dots, f_n) = 1$ , т. е. отсутствию у многочленов  $f_1, f_2, \dots, f_n$  общих делителей положительной степени — точно так же, как это происходит в кольце целых чисел  $\mathbb{Z}$ .

Определение 3.3

Многочлен  $f \in K[x]$  с коэффициентами в целостном<sup>1</sup> кольце  $K$  называется *неприводимым*, если из равенства  $f = gh$  вытекает, что  $g$  или  $h$  является обратимой константой.

Упражнение 3.7. Пусть  $\mathbb{k}$  — любое поле. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце  $\mathbb{k}[x]$ : любой многочлен  $f$  является произведением конечного числа неприводимых многочленов, причём любые два таких представления  $p_1 p_2 \dots p_k = f = q_1 q_2 \dots q_m$  имеют одинаковое число сомножителей  $k = m$ , и эти сомножители можно перенумеровать так, чтобы  $\forall i \ p_i = \lambda_i q_i$ , где  $\lambda_i \in \mathbb{k}$  — некоторые ненулевые константы.

<sup>1</sup>т. е. с единицей и без делителей нуля

Предложение 3.6 (китайская теорема об остатках)

Пусть  $\mathbb{k}$  — произвольное поле, и многочлен  $f \in \mathbb{k}[x]$  является произведением  $m$  сомножителей:  $f = f_1 f_2 \cdots f_m$ , таких что  $\text{нод}(f_i, f_j) = 1 \forall i, j$ . Отображение

$$\begin{aligned} \varphi : \mathbb{k}[x]/(f) &\rightarrow (\mathbb{k}[x]/(f_1)) \times (\mathbb{k}[x]/(f_2)) \times \cdots \times (\mathbb{k}[x]/(f_m)) \\ \varphi : [g]_f &\mapsto ([g]_{f_1}, [g]_{f_2}, \dots, [g]_{f_m}) \end{aligned}$$

является корректно определённым изоморфизмом колец.

Доказательство. Проверки того, что  $\varphi$  корректно определён<sup>1</sup>, является гомоморфизмом и имеет нулевое ядро, дословно повторяют рассуждения из н° 2.7, и мы оставляем их читателю. Покажем, что  $\varphi$  сюръективен. Для этого, как и в н° 2.7, построим для любого заданного набора классов  $[r_i]_{f_i} \in \mathbb{k}[x]/(f_i)$  многочлен  $g \in \mathbb{k}[x]$ , такой что  $g \equiv r_i \pmod{f_i}$  при всех  $i$ . Для каждого  $i$  обозначим произведение всех сомножителей  $f_v$  кроме  $f_i$  через

$$F_i = \prod_{v \neq i} f_v.$$

Поскольку  $f_i$  взаимно прост со всеми  $f_v$  с  $v \neq i$ , он, согласно лем. 2.3, взаимно прост и с  $F_i$ , а значит, существует многочлен<sup>1</sup>  $h_i \in \mathbb{k}[x]$ , такой что

$$F_i \cdot h_i \equiv 1 \pmod{f_i}.$$

Итак, многочлен  $g_i = F_i \cdot h_i \equiv 1 \pmod{f_i}$  и делится на все  $f_v$  с  $v \neq i$ . Следовательно,  $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m \equiv r_i \pmod{f_i}$  при всех  $i$ .  $\square$

**3.2.2. Алгоритм Евклида** из н° 2.2.2 дословно переносится на многочлены с коэффициентами в произвольном поле  $\mathbb{k}$ . А именно, для пары многочленов  $f_1, f_2 \in \mathbb{k}[x]$  с  $\deg(f_1) \geq \deg(f_2)$  положим  $E_0 = f_1, E_1 = f_2, E_k =$  остатку от деления  $E_{k-2}$  на  $E_{k-1}$  при  $k \geq 1$ . Степени многочленов  $E_k$  строго убывают до тех пор, пока какой-то  $E_r$  не разделит нацело предыдущий  $E_{r-1}$ , в результате чего  $E_{r+1}$  обратится в нуль. Последний ненулевой многочлен  $E_r = \text{нод}(f_1, f_2)$ .

Упражнение 3.8. Докажите это.

Если при вычислении каждого  $E_k$  представлять его в виде  $E_k = h_1^{(k)} f_1 + h_2^{(k)} f_2$ , то  $E_r = \text{нод}(f_1, f_2)$  и  $E_{r+1} = 0$  тоже получатся представленными в таком виде, причём в выражении  $E_{r+1} = 0 = h_1^{(r+1)} f_1 + h_2^{(r+1)} f_2$  многочлены  $h_1^{(r+1)}$  и  $h_2^{(r+1)}$  будут взаимно простыми множителями, дополняющими  $f_1$  и  $f_2$  до их наименьшего общего кратного

$$\text{нок}(f_1, f_2) = h_1^{(r+1)} f_1 = -h_2^{(r+1)} f_2.$$

Упражнение 3.9. Докажите это.

Вот как выглядит это вычисление для многочленов

$$f_1(x) = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \quad \text{и} \quad f_2(x) = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 :$$

<sup>1</sup>т. е.  $\varphi([g]_f)$  не зависит от выбора представителя  $g \in \mathbb{k}[x]$  в классе  $[g]_f \subset \mathbb{k}[x]$

<sup>1</sup>чтобы найти его явно, можно, например, взять остаток  $R_i$  от деления  $F_i$  на  $f_i$  и применить к паре  $E_0 = f_i, E_1 = R_i$  алгоритм Евклида

$$\begin{aligned} E_0 &= x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \\ E_1 &= x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 \\ E_2 &= -4x^4 - 13x^3 - 21x^2 - 10x - 8 = E_0 - (x^2 - 2x + 3) E_1 \end{aligned}$$

далее делить на  $E_2$  удобнее не  $E_1$ , а  $16E_1$ , а потом поделить результат на 16

$$E_3 = \frac{1}{16} (x^3 + 5x^2 + 10x + 8) = \frac{1}{16} (16E_1 + (4x + 7)E_2) = \frac{4x + 7}{16} E_0 - \frac{4x^3 - x^2 - 2x + 5}{16} E_1$$

следующий шаг уже даёт наибольший общий делитель

$$E_4 = -16(x^2 + 3x + 4) = E_2 + 16(4x - 7)E_3 = 16(x^2 - 3)E_0 - 16(x^4 - 2x^3 + 2x - 2)E_1$$

поскольку  $E_5 = E_3 + (x + 2) \cdot E_4 / 256 = ((x^3 + 2x^2 + x + 1) \cdot E_0 - (x^5 + x^2 + 1) \cdot E_1) = 0$ . Откуда

$$\begin{aligned} \text{нод}(f_1, f_2) &= x^2 + 3x + 4 = -(x^2 - 3)f_1(x) + (x^4 - 2x^3 + 2x - 2)f_2(x) \\ \text{нок}(f_1, f_2) &= (x^3 + 2x^2 + x + 1)f_1(x) = (x^5 + x^2 + 1)f_2(x). \end{aligned}$$

**3.3. Корни многочленов.** Элемент  $\alpha \in K$  называется *корнем* многочлена  $f \in K[x]$ , если  $f(\alpha) = 0$ . Как мы видели в [прим. 3.2](#), это условие равносильно тому, что  $f(x)$  делится в  $K[x]$  на  $(x - \alpha)$ .

Предложение 3.7

Пусть  $K$  — целостное кольцо и  $f \in K[x]$  имеет  $s$  различных корней  $\alpha_1, \alpha_2, \dots, \alpha_s \in K$ . Тогда  $f$  делится в  $K[x]$  на произведение  $\prod_i (x - \alpha_i)$ . В частности, если  $f \neq 0$ , то  $\deg(f) \geq s$ .

Доказательство. Так как в  $K$  нет делителей нуля и  $(\alpha_i - \alpha_1) \neq 0$  при  $i \neq 1$ , подставляя в равенство  $f(x) = (x - \alpha_1) \cdot q(x)$  значения  $x = \alpha_2, \alpha_3, \dots, \alpha_s$ , убеждаемся, что  $\alpha_2, \alpha_3, \dots, \alpha_s$  являются корнями многочлена  $q(x)$ , и применяем индукцию.  $\square$

Следствие 3.2

Ненулевой многочлен  $f$  с коэффициентами из целостного кольца не может иметь в этом кольце более  $\deg(f)$  различных корней.

Упражнение 3.10 (формула Лагранжа). Пусть  $\mathbb{k}$  — поле, и  $a_0, a_1, \dots, a_n \in \mathbb{k}$  — любые  $n + 1$  различных его элементов. Покажите, что для произвольного набора значений  $b_0, b_1, \dots, b_n \in \mathbb{k}$  существует единственный многочлен  $f(x) \in \mathbb{k}[x]$  степени  $\leq n$ , такой что  $f(a_i) = b_i$  при всех  $i = 0, 1, \dots, n$ .

Следствие 3.3

Пусть кольцо  $K$  целостное, и  $f, g \in K[x]$  имеют степени, не превосходящие  $n$ . Если  $f(\alpha_i) = g(\alpha_i)$  для более, чем  $n$  попарно разных  $\alpha_i \in K$ , то  $f = g$  в  $K[x]$ .

Доказательство. Многочлен  $f - g$  нулевой, поскольку имеет степень  $\leq n$  и больше, чем  $n$  корней.  $\square$

Упражнение 3.11. Пусть  $\mathbb{k}$  — поле. Проверьте, что многочлен степени 2 или 3 неприводим в  $\mathbb{k}[x]$  тогда и только тогда, когда у него нет корней в поле  $\mathbb{k}$ .



**3.3.1. Общие корни нескольких многочленов.** Пусть  $\mathbb{k}$  — поле. Число  $\alpha$  тогда и только тогда является общим корнем многочленов  $f_1, f_2, \dots, f_m \in \mathbb{k}[x]$ , когда  $\alpha$  является корнем их наибольшего общего делителя. В самом деле, если  $(x - \alpha)$  делит каждый из  $f_i$ , то по [предл. 3.5](#)  $(x - \alpha)$  делит  $\text{нод}(f_1, f_2, \dots, f_m)$ , и наоборот. Таким образом, отыскание общих корней набора многочленов сводится к отысканию корней их наибольшего общего делителя, что часто бывает проще, чем отыскание корней любого из  $f_i$  в отдельности, т. к. степень  $\text{нод}(f_1, f_2, \dots, f_m)$  обычно меньше степени любого  $f_i$ .

Если многочлены  $f_1, f_2, \dots, f_m \in \mathbb{k}[x]$  взаимно просты, то они не имеют общих корней не только в поле  $\mathbb{k}$ , но и ни в каком большем кольце  $K \supset \mathbb{k}$ . В самом деле, поскольку существуют многочлены  $h_i \in \mathbb{k}[x]$ , такие что  $f_1 h_1 + f_2 h_2 + \dots + f_m h_m = 1$ , многочлены  $f_i$  не могут одновременно обратиться в нуль ни при каком значении  $x$ .

**3.3.2. Кратные корни.** Пусть  $\mathbb{k}$  — произвольное поле. Число  $\alpha \in \mathbb{k}$  называется  $m$ -кратным корнем многочлена  $f \in \mathbb{k}[x]$ , если  $f(x) = (x - \alpha)^m \cdot g(x)$ , где  $g(\alpha) \neq 0$ . Корни кратности  $m \geq 2$  называются *кратными*.

Предложение 3.8

Для того, чтобы  $\alpha \in \mathbb{k}$  был кратным корнем  $f \in \mathbb{k}[x]$  необходимо и достаточно, чтобы  $f(\alpha) = f'(\alpha) = 0$ .

Доказательство. Если  $\alpha$  — кратный корень многочлена  $f$ , то  $f(x) = (x - \alpha)^2 g(x)$ . Дифференцируя, получаем  $f'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$ , откуда  $f'(\alpha) = 0$ . Если  $\alpha$  не является кратным корнем, то  $f(x) = (x - \alpha)g(x)$ , где  $g(x) \neq 0$ . Тогда  $f'(x) = (x - \alpha)g'(x) + g(x)$  и  $f'(\alpha) = g(\alpha) \neq 0$ .  $\square$

Предложение 3.9

Если  $\text{char } \mathbb{k} = 0$ , то  $\alpha \in \mathbb{k}$  является  $m$ -кратным корнем многочлена  $f \in \mathbb{k}[x]$  тогда и только тогда, когда  $\alpha$  является корнем  $f$  и первых  $(m - 1)$  производных от  $f$ , но не является корнем  $m$ -той производной.

Доказательство. Если  $f(x) = (x - \alpha)^m \cdot g(x)$  то  $f'(x) = (x - \alpha)^{m-1} \cdot (m \cdot g(x) + (x - \alpha) \cdot g'(x))$ . При  $g(\alpha) \neq 0$  второй сомножитель в этом равенстве отличен от нуля при  $x = \alpha$ . Поэтому  $\alpha$  является  $m$ -кратным корнем  $f$  тогда и только тогда, когда  $\alpha$  является  $(m - 1)$ -кратным корнем  $f'$ .  $\square$

Предложение 3.10

Если  $\text{char}(\mathbb{k}) = p > 0$ , то  $f' = 0$  тогда и только тогда, когда  $f = g^p$  для некоторого  $g \in \mathbb{k}[x]$ .

Доказательство. Согласно [прим. 3.1](#), равенство  $f' = 0$  равносильно тому, что  $f(x) = g(x^p)$  для некоторого  $g \in \mathbb{k}[x]$ . Поскольку в характеристике  $p$  возведение в  $p$ -тую степень является гомоморфизмом (см. [прим. 2.6](#)),  $g(x^p) = g(x)^p$ .  $\square$

Следствие 3.4

Для произвольного поля  $\mathbb{k}$  неприводимый многочлен  $f \in \mathbb{k}[x]$  не имеет кратных корней ни в каком кольце  $K \supset \mathbb{k}$ .

Доказательство. Согласно [предл. 3.10](#) производная неприводимого многочлена отлична от нуля над любым полем. Поскольку  $f$  неприводим, он взаимно прост с  $f'$ . В силу [л<sup>е</sup> 3.3.1](#) в взаимно простых многочленах нет общих корней ни в каком кольце  $K \supset \mathbb{k}$ .  $\square$

**3.3.3. Присоединение корней.** Кольцо вычетов  $\mathbb{k}[x]/(f)$  определяется аналогично кольцу  $\mathbb{Z}/(n)$ . Зафиксируем произвольный отличный от константы многочлен  $f \in \mathbb{k}[x]$  и обозначим через  $(f) = \{fh \mid h \in \mathbb{k}[x]\}$  подкольцо всех многочленов, делящихся на  $f$ . Отношение  $g_1 \equiv g_2 \pmod{f}$ , означающее по определению, что  $g_1 - g_2 \in (f)$ , является отношением эквивалентности и разбивает  $\mathbb{k}[x]$  в объединение непересекающихся классов  $[g]_f = g + (f) = \{g + fh \mid h \in \mathbb{k}[x]\}$ , которые называются *классами вычетов* по модулю  $f$ . Сложение и умножение этих классов задаётся формулами

$$[g] + [h] \stackrel{\text{def}}{=} [g + h], \quad [g] \cdot [h] \stackrel{\text{def}}{=} [gh]. \quad (3-13)$$

Упражнение 3.12. Проверьте корректность<sup>2</sup> этого определения, а также выполнение в  $\mathbb{k}[x]/(f)$  всех аксиом коммутативного кольца с единицей.

Нулевым элементом кольца  $\mathbb{k}[x]/(f)$  является класс  $[0]_f = (f)$ , единицей является класс  $[1]_f = 1 + (f)$ . Поскольку никакая константа не может делиться на многочлен положительной степени, классы всех констант  $c \in \mathbb{k}$  различны по модулю  $f$ . Иначе говоря, поле  $\mathbb{k}$  гомоморфно вкладывается в кольцо  $\mathbb{k}[x]/(f)$  в качестве подполя, образованного классами констант. Поэтому для классов чисел  $c \in \mathbb{k}$  мы всюду далее пишем  $c$  вместо  $[c]_f$ .

Упражнение 3.13. Покажите, что поле  $\mathbb{k}[x]/(x - a)$  изоморфно полю  $\mathbb{k}$ .

Так как любой многочлен  $g \in \mathbb{k}[x]$  единственным образом записывается в виде  $g = fh + r$ , где  $\deg(r) < \deg(f)$ , в каждом классе  $[g]_f$  имеется единственный представитель  $r \in [g]_f$  степени  $\deg(r) < \deg(f)$ . Тем самым, каждый класс *однозначно* записывается как

$$[a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}, \quad \text{где } \vartheta = [x]_f \text{ и } a_i \in \mathbb{k}.$$

Класс  $\vartheta = [x]_f$  удовлетворяет в кольце  $\mathbb{k}[x]/(f)$  уравнению  $f(\vartheta) = 0$ , т. к.

$$f(\vartheta) = f([x]_f) = [f(x)]_f = [0]_f.$$

Поэтому сложение и умножение классов по правилам (3-13) можно интерпретировать как формальное сложение и умножение записей

$$a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}, \quad (3-14)$$

по стандартным правилам раскрытия скобок и приведения подобных с учётом того, что символ  $\vartheta$  удовлетворяет соотношению  $f(\vartheta) = 0$ . По этой причине кольцо  $\mathbb{k}[x]/(f)$  часто обозначают через  $\mathbb{k}[\vartheta] : f(\vartheta) = 0$  и называют *расширением* поля  $\mathbb{k}$  посредством *присоединения* к нему корня  $\vartheta$  многочлена  $f \in \mathbb{k}[x]$ .

Например, кольцо  $\mathbb{Q}[x]/(x^2 - 2)$  можно воспринимать как множество формальных записей вида  $a + b\sqrt{2}$ , где  $\sqrt{2} \stackrel{\text{def}}{=} [x]$ . Сложение и умножение таких записей происходит по стандартным правилам раскрытия скобок с учётом того, что  $(\sqrt{2})^2 = 2$ :

$$\begin{aligned} (a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (cb + ad)\sqrt{2} \end{aligned}$$

Упражнение 3.14. Проверьте, что  $\mathbb{Q}[\sqrt{2}]$  является полем, и выясните, являются ли полями кольца  $\mathbb{Q}[\vartheta]$ , в которых а)  $\vartheta^3 + 1 = 0$  б)  $\vartheta^3 + 2 = 0$ .

<sup>2</sup>т. е. независимость классов  $[g + h]$  и  $[gh]$  от выбора представителей  $g \in [g]$  и  $h \in [h]$

Предложение 3.11

Пусть  $\mathbb{k}$  — произвольное поле. Кольцо  $\mathbb{k}[x]/(f)$  является полем тогда и только тогда, когда многочлен  $f$  неприводим в  $\mathbb{k}[x]$ .

Доказательство. Если  $f = gh$ , где оба многочлена  $f, g$  имеют строго меньшую, чем  $f$ , степень, то ненулевые классы  $[g], [h]$  будут делителями нуля в  $\mathbb{k}[x]/(f)$ , что невозможно в поле. Если же  $f$  неприводим, то для любого  $g \notin (f)$   $\text{нод}(f, g) = 1$ , а значит,  $fh + gq = 1$  для некоторых  $h, q \in \mathbb{k}[x]$ , откуда  $[q] \cdot [g] = [1]$  в  $\mathbb{k}[x]/(f)$ .  $\square$

Упражнение 3.15. Напишите явную формулу для вычисления обратного элемента к числу  $a_0 + a_1\vartheta$  в поле  $\mathbb{Q}(\vartheta)$  с  $\vartheta^2 + \vartheta + 1 = 0$ .

Теорема 3.1

Для любого поля  $\mathbb{k}$  и любого многочлена  $f \in \mathbb{k}[x]$  существует такое поле  $\mathbb{F} \supset \mathbb{k}$ , что  $f$  разлагается в  $\mathbb{F}[x]$  в произведение  $\deg f$  линейных множителей.

Доказательство. Индукция по  $n = \deg f$ . Пусть для любого поля  $\mathbb{k}$  и для всех многочленов степени  $< n$  из  $\mathbb{k}[x]$  мы умеем строить такое поле<sup>1</sup>. Если  $f$  приводим:  $f = gh$ , где  $\deg g < n$  и  $\deg h < n$ , мы можем построить поле  $\mathbb{F}' \supset \mathbb{k}$  над которым  $g$  полностью разложится на линейные множители, а затем поле  $\mathbb{F} \supset \mathbb{F}'$  над которым разложится  $h$ , а тем самым, и  $f$ . Если  $f$  неприводим, рассмотрим поле  $\mathbb{F}' = \mathbb{k}[x]/(f)$ . Оно содержит  $\mathbb{k}$  в качестве классов констант, и многочлен  $f$  делится в  $\mathbb{F}'[x]$  на  $(x - \vartheta)$ , где  $\vartheta = [x] \pmod{f}$ . Частное от этого деления имеет степень  $n - 1$  и по индукции раскладывается на линейные множители над некоторым полем  $\mathbb{F} \supset \mathbb{F}'$ . Тогда и  $f$  полностью разложится над  $\mathbb{F}$ .  $\square$

**3.4. Поле комплексных чисел**  $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2 + 1)$  является расширением поля  $\mathbb{R}$  при помощи корня квадратного уравнения  $x^2 + 1 = 0$  и состоит из классов  $[x + yt] = x + y \cdot i$ , где  $x, y \in \mathbb{R}$  и  $i \stackrel{\text{def}}{=} [t]$  удовлетворяет соотношению  $i^2 = -1$ . Поскольку многочлен  $t^2 + 1$  не имеет вещественных корней, он неприводим в  $\mathbb{R}[t]$ , так что  $\mathbb{C}$  действительно является полем: если  $x + yi \neq 0$ , то

$$\frac{1}{x + yi} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} \cdot i.$$

Удобно изображать комплексное число  $z = x + yi$  *радиус-вектором*, ведущим из начала координат  $(0, 0)$  в точку  $z = (x, y)$  на плоскости  $\mathbb{R}^2$  с фиксированной прямоугольной системой координат  $XOY$  (см. рис. 3♦1). Координаты  $(x, y)$  называются при этом *действительной* и *мнимой* частями числа комплексного числа  $z \in \mathbb{C}$  и обозначаются через  $\text{Re}(z)$  и  $\text{Im}(z)$  соответственно. Длина радиус вектора  $|z| = \sqrt{x^2 + y^2}$  называется *модулем* (или *абсолютной величиной*) комплексного числа  $z$ . Множество всех  $\vartheta \in \mathbb{R}$ , таких что поворот плоскости  $\mathbb{C}$  вокруг нуля на угол  $\vartheta$  совмещает координатный луч  $OX$  с лучом, идущим в направлении радиус вектора  $z$ , называется *аргументом* числа  $z$  и обозначается

$$\text{Arg}(z) = \{\varphi + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R},$$

<sup>1</sup>заметим, что при  $n = 2$  это так: достаточно взять  $\mathbb{F} = \mathbb{k}$

где  $\varphi$  — ориентированная длина дуги<sup>1</sup>, идущей по единичной окружности из точки  $(1, 0)$  в точку  $z / |z|$  (ср. с н° 1.6.1). Таким образом,  $z = x + yi \in \mathbb{C}$  имеет  $\operatorname{Re}(z) = |z| \cdot \cos \varphi$ ,  $\operatorname{Im}(z) = |z| \cdot \sin \varphi$  и может быть записан как  $z = |z| \cdot (\cos \varphi + i \cdot \sin \varphi)$ , где  $\vartheta \in \operatorname{Arg}(z)$ .

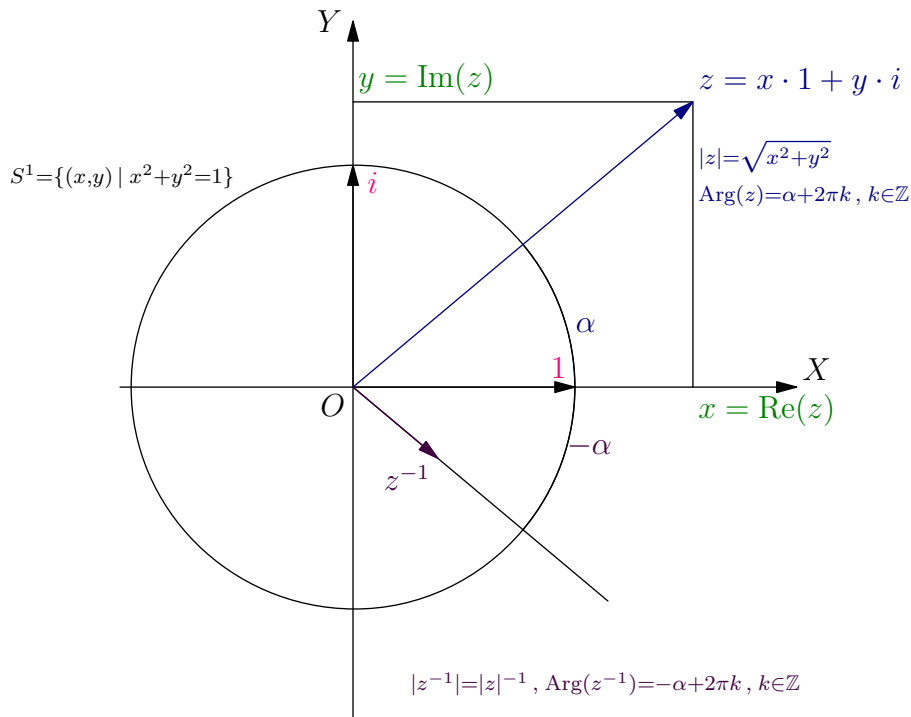


Рис. 3◊1.

## Лемма 3.1

Множество радиус-векторов точек  $z$  декартовой координатной плоскости  $\mathbb{R}^2$  с операцией сложения векторов и операцией умножения, заданной правилами<sup>1</sup>

$$|z_1 z_2| \stackrel{\text{def}}{=} |z_1| \cdot |z_2| \quad (3-15)$$

$$\operatorname{Arg}(z_1 z_2) \stackrel{\text{def}}{=} \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) = \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \operatorname{Arg}(z_1), \vartheta_2 \in \operatorname{Arg}(z_2)\} \quad (3-16)$$

образует поле, изоморфное полю  $\mathbb{C}$ . Изоморфизм сопоставляет числу  $x + iy \in \mathbb{C}$  точку  $z = (x, y) \in \mathbb{R}^2$ .

Упражнение 3.16. Проверьте, что сложение аргументов (3-16) определено корректно.

Доказательство лем. 3.1. Векторы на плоскости образуют абелеву группу по сложению, а ненулевые векторы — абелеву группу относительно операции умножения, задаваемой правилами (3-15) и (3-16): единицей служит единичный направляющий вектор оси  $OX$ , а обратным к ненулевому вектору  $z$  является вектор  $z^{-1}$  с

$$|z^{-1}| = 1/|z|, \quad \operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z) \quad (3-17)$$

<sup>1</sup>отметим, что таких дуг имеется бесконечно много, но все они отличаются друг от друга на целое число оборотов; эпитет «ориентированная» означает, что длину следует брать со знаком «+», если движение происходит против часовой стрелки, и со знаком «-», если по часовой стрелке

<sup>1</sup>иначе говоря, при умножении комплексных чисел их модули перемножаются, а аргументы складываются

(см. рис. 3◊1). Для проверки дистрибутивности заметим, что отображение  $\lambda_a : z \mapsto az$  умножения на фиксированный вектор  $a$  представляет собою *поворотную гомотегию*<sup>1</sup> плоскости  $\mathbb{R}^2$  относительно начала координат на угол  $\text{Arg}(a)$  с коэффициентом  $|a|$ . Аксиома дистрибутивности  $a(b+c) = ab+ac$  означает, что поворотная гомотегия перестановочна со сложением векторов:  $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$ . Это действительно так, поскольку и повороты и гомотегии переводят параллелограммы в параллелограммы.

Таким образом векторы образуют поле. Векторы, параллельные прямой  $OX$  образуют в нём подполе, изоморфное полю  $\mathbb{R}$ . Произвольный вектор  $z = (x, y)$  записывается в виде  $z = x + iy$ , где  $i$  — единичный направляющий вектор оси  $OY$ ,  $x, y \in \mathbb{R}$  понимаются как точки оси  $OX$ , а сложение и умножение происходят по правилам из условия леммы. При этом  $i^2 = -1$  и для любых векторов  $z_1 = x_1 + iy_1$  и  $z_2 = x_2 + iy_2$

$$\begin{aligned} z_1 + z_2 &= (x_1 + x_2) + i(y_1 + y_2) \\ z_1 z_2 &= (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) \end{aligned}$$

что полностью согласуется с умножением классов вычетов  $[x + yt]$  в  $\mathbb{R}[t]/(t^2 + 1)$ .  $\square$

**3.4.1. Сопряжение.** Число  $\bar{z} \stackrel{\text{def}}{=} x - iy$  называется *комплексно сопряжённым* к числу  $z = x + iy$ . В терминах комплексного сопряжения формулу для обратного числа можно записать в виде  $z^{-1} = \bar{z}/|z|^2$ . Геометрически, комплексное сопряжение  $z \mapsto \bar{z}$  представляет собою симметрию комплексной плоскости относительно вещественной оси  $OX$ . С алгебраической точки зрения сопряжение является инволютивным<sup>0</sup> автоморфизмом поля  $\mathbb{C}$ , т. е.  $\forall z \in \mathbb{C} \quad \bar{\bar{z}} = z$  и  $\forall z_1, z_2 \in \mathbb{C} \quad \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$  и  $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$ .

**3.4.2. Тригонометрия.** Большая часть школьной тригонометрии представляет собою не самую удобную для восприятия запись заурядных вычислений с комплексными числами  $z$ , лежащими на единичной окружности. Например, произведение  $z_1 z_2$  двух таких чисел

$$z_1 = \cos \varphi_1 + i \sin \varphi_1 \quad \text{и} \quad z_2 = \cos \varphi_2 + i \sin \varphi_2$$

по лем. 3.1 равно  $\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)$ . С другой стороны,

$$z_1 z_2 = \left( \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 \right) + i \left( \cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2 \right),$$

откуда  $\cos(\varphi_1 + \varphi_2) = \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2$  и  $\sin(\varphi_1 + \varphi_2) = \cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2$ . Тем самым, мы *доказали* тригонометрические формулы сложения аргументов.

Пример 3.3 (тригонометрические функции кратных углов)

По лем. 3.1  $z = \cos \varphi + i \sin \varphi$  имеет  $z^n = \cos(n\varphi) + i \sin(n\varphi)$ . Раскрывая в  $(\cos \varphi + i \sin \varphi)^n$

<sup>1</sup>поворотной гомотетией относительно точки  $O$  на угол  $\alpha$  с коэффициентом  $\varrho > 0$  называется композиция поворота на угол  $\alpha$  вокруг точки  $O$  и растяжения в  $\varrho$  раз относительно  $O$  (поскольку растяжения коммутируют с поворотами, всё равно, в каком порядке эта композиция выполняется)

<sup>0</sup>отличный от тождественного эндоморфизм  $\iota : X \rightarrow X$  произвольного множества  $X$  называется *инволюцией*, если  $\iota \circ \iota = \text{Id}_X$ ; по предл. 1.4 на стр. 14 всякая инволюция автоматически биективна

скобки по форм. (1-9) на стр. 8, получаем равенство

$$\begin{aligned} \cos(n\varphi) + i \sin(n\varphi) &= (\cos \varphi + i \sin \varphi)^n = \\ &= \cos^n \varphi + i \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi - i \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \dots = \\ &= \left( \binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots \right) + \\ &\quad + i \cdot \left( \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi - \dots \right) \end{aligned}$$

закрывающее в себе сразу все мыслимые формулы для кратных углов:

$$\begin{aligned} \cos(n\varphi) &= \binom{n}{0} \cos^n \varphi - \binom{n}{2} \cos^{n-2} \varphi \sin^2 \varphi + \binom{n}{4} \cos^{n-4} \varphi \sin^4 \varphi - \dots \\ \sin(n\varphi) &= \binom{n}{1} \cos^{n-1} \varphi \sin \varphi - \binom{n}{3} \cos^{n-3} \varphi \sin^3 \varphi + \binom{n}{5} \cos^{n-5} \varphi \sin^5 \varphi - \dots \end{aligned}$$

Например,  $\cos 3\varphi = \cos^3 \varphi - 3 \cos \varphi \cdot \sin^2 \varphi = 4 \cos^3 \varphi - 3 \cos \varphi$ .

Упражнение 3.17. Выразите  $\sin(2\pi/5)$  и  $\cos(2\pi/5)$  через радикалы от рациональных чисел.

**3.4.3. Корни из единицы и круговые многочлены.** Решим в поле  $\mathbb{C}$  уравнение

$$z^n = 1.$$

Сравнивая модули левой и правой части, получаем  $|z^n| = |z|^n = 1$ , откуда  $|z| = 1$ . Сравнивая аргументы, получаем  $n \operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$ . Поскольку

$$n\varphi \in \{2\pi k \mid k \in \mathbb{Z}\} \iff \varphi \in \{2\pi k/n \mid k \in \mathbb{Z}\},$$

имеется ровно  $n$  различных классов эквивалентности вещественных чисел по модулю добавления целых кратных  $2\pi$ , которые при умножении их представителей на  $n$  превращаются в класс  $\{2\pi k \mid k \in \mathbb{Z}\}$ . Это классы  $n$  геометрически различных углов  $2\pi k/n$  с  $0 \leq k \leq n-1$ . Таким образом, уравнение  $z^n = 1$  имеет ровно  $n$  корней

$$\zeta_k = \cos(2\pi k/n) + i \sin(2\pi k/n) \quad (\text{где } k = 0, 1, \dots, (n-1)),$$

расположенных в вершинах правильного  $n$ -угольника, вписанного в единичную окружность так, что вершина  $\zeta_0$  находится в точке 1 (см. рис. 3◊2). Они образуют абелеву группу относительно операции умножения. Эта группа обозначается  $\mu_n$  и называется группой корней  $n$ -той степени из единицы<sup>0</sup>.

Корень  $\zeta \in \mu_n$  называются *первообразным корнем* степени  $n$  из единицы, если все остальные элементы группы  $\mu_n$  представляются в виде  $\zeta^k$  с  $k \in \mathbb{N}$ . Например, корень с наименьшим положительным аргументом  $\zeta_1 = \cos(2\pi/n) + i \sin(2\pi/n)$  является первообразным. Но есть и другие: скажем, на рис. 3◊2 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, а в группе  $\mu_6$  на рис. 3◊3 на стр. 44 первообразными являются только  $\zeta_1$  и  $\zeta_5 = \zeta_1^{-1}$ .

Упражнение 3.18. Покажите, что корень  $\zeta_1^k = \cos(2\pi k/n) + i \sin(2\pi k/n)$  является первообразным тогда и только тогда, когда  $\operatorname{nod}(k, n) = 1$ .

<sup>0</sup>фактически мы уже встречались с ней в н° 1.6.1, где эта группа называлась *циклической группой порядка n*

Приведённый многочлен, имеющий корнями все первообразные корни степени  $n$  из единицы и только их

$$\Phi_n(z) = \prod_{\substack{1 \leq k < n : \\ \text{нод}(k,n)=1}} (z - z_1^k), \quad (3-18)$$

называется  $n$ -тым *круговым* (или *циклотомическим*) многочленом.

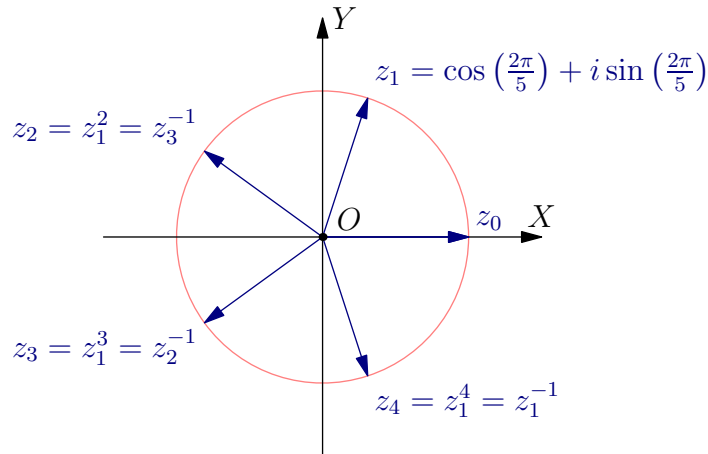


Рис. 3◊2. Корни уравнения  $z^5 = 1$ .

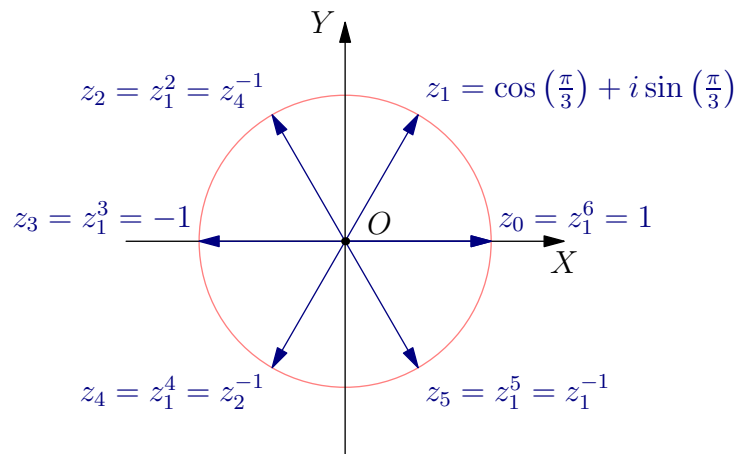


Рис. 3◊3. Корни уравнения  $z^6 = 1$ .

Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4) = z^4 + z^3 + z^2 + z + 1$$

$$\Phi_6(z) = (z - z_1)(z - z_4) = z^2 - z + 1.$$

Упражнение 3.19\*. Покажите, что  $\forall n \Phi_n \in \mathbb{Z}[x]$  и неприводим<sup>0</sup> в  $\mathbb{Q}[x]$ .

<sup>0</sup>т. е. не являются произведениями многочленов строго меньшей степени

Пример 3.4 (уравнение  $z^n = a$ )

Корни уравнения  $z^n = a$  это числа  $z = |z| \cdot (\cos \varphi + i \sin \varphi)$  с  $|z|^n = |a|$ , а  $n\varphi \in \text{Arg}(a)$ . При  $a = |a| \cdot (\cos \alpha + i \sin \alpha) \neq 0$  имеется ровно  $n$  таких чисел

$$z_k = \sqrt[n]{|a|} \cdot \left( \cos \frac{\alpha + 2\pi k}{n} + i \cdot \sin \frac{\alpha + 2\pi k}{n} \right), \quad 0 \leq k \leq n-1.$$

Они располагаются в вершинах правильного  $n$ -угольника, вписанного в окружность радиуса  $\sqrt[n]{|a|}$  с центром в нуле так, что радиус-вектор одной из его вершин располагается под углом  $\alpha/n$  к оси  $OX$ .

Пример 3.5 (гауссовы числа)

Рассмотрим в  $\mathbb{C}$  подкольцо, состоящее из всех чисел с целыми координатами

$$\mathbb{Z}[i] \stackrel{\text{def}}{=} \{z = x + iy \mid x, y \in \mathbb{Z}\}.$$

Оно называется кольцом *гауссовых целых чисел* и часто используется в арифметике. Например, классическая задача о представлении натурального числа в виде суммы двух квадратов целых чисел существенно проясняется расширением кольца  $\mathbb{Z}$  до кольца  $\mathbb{Z}[i]$ , в котором  $x^2 + y^2 = (x + iy)(x - iy)$ , так что разрешимость в кольце  $\mathbb{Z}$  уравнения  $x^2 + y^2 = n$  равносильна разрешимости в кольце  $\mathbb{Z}[i]$  уравнения  $n = z \cdot \bar{z}$ . Из второго уравнения сразу же видно, что если числа  $m_1$  и  $m_2$  представляются в виде суммы двух квадратов

$$\begin{aligned} m_1 &= a_1^2 + b_1^2 = (a_1 + ib_1)(a_1 - ib_1) = z_1 \bar{z}_1 \\ m_2 &= a_2^2 + b_2^2 = (a_2 + ib_2)(a_2 - ib_2) = z_2 \bar{z}_2 \end{aligned}$$

то их произведение  $m = m_1 m_2$  также является суммой двух квадратов:

$$m = z_1 z_2 \cdot \overline{z_1 z_2} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

(это соотношение известно как *тождество Эйлера*). В сочетании с теоремой о единственности разложения на простые множители в кольце  $\mathbb{Z}[i]$ , которую мы докажем в §5, тождество Эйлера сводит вопрос о представимости произвольного натурального числа в виде суммы двух квадратов к анализу представимости простых чисел. Мы ещё вернёмся к этому в [прим. 5.5](#) на стр. 77.

Упражнение 3.20. Покажите, что обратимыми элементами кольца  $\mathbb{Z}[i]$  являются четыре числа:  $\pm 1$  и  $\pm i$ .

**3.5. Конечные поля.** Для конечного поля  $\mathbb{F}_p = \mathbb{Z}/(p)$  из  $p$  элементов и неприводимого многочлена  $f \in \mathbb{F}_p[x]$  степени  $n$  поле вычетов  $\mathbb{F}_p[x]/(f)$  состоит из  $p^n$  элементов вида

$$a_0 + a_1 \vartheta + \dots + a_{n-1} \vartheta^{n-1}, \quad \text{где } a_i \in \mathbb{F}_p \text{ и } f(\vartheta) = 0.$$

Например,  $x^2 + x + 1 \in \mathbb{F}_2[x]$  неприводим, поскольку не имеет корней в  $\mathbb{F}_2$ . Соответствующее поле  $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_2[\omega] : \omega^2 + \omega + 1 = 0$  состоит из четырёх элементов<sup>0</sup>:  $0, 1, \omega, 1 + \omega = \omega^2 = \omega^{-1}$ .

Упражнение 3.21. Убедитесь, что мультипликативная группа  $\mathbb{F}_4^*$  поля  $\mathbb{F}_4$  изоморфна циклической группе  $\mu_3$ .

<sup>0</sup>отметим, что в силу равенства  $-1 = 1$  в поле  $\mathbb{F}_2$  можно обходиться без «минусов»



Расширение  $\mathbb{F}_2 \subset \mathbb{F}_4$  аналогично расширению  $\mathbb{R} \subset \mathbb{C} \simeq \mathbb{R}[\omega] : \omega^2 + \omega + 1 = 0$ , получающемуся присоединением к полю  $\mathbb{R}$  первообразного комплексного кубического корня из единицы<sup>0</sup>. Аналогом комплексного сопряжения, переводящего  $\omega$  в  $\bar{\omega} = \omega^2$ , в поле  $\mathbb{F}_4$  является гомоморфизм Фробениуса<sup>0</sup>  $F_2 : \mathbb{F}_4 \rightarrow \mathbb{F}_4, a \mapsto a^2$ , который тождественно действует на простом подполе  $\mathbb{F}_2 = \{0, 1\}$  и переводит корни многочлена  $x^2 + x + 1$  друг в друга.

Рассмотрим ещё один пример. Многочлен  $x^2 + 1 \in \mathbb{F}_3[x]$  не имеет корней в  $\mathbb{F}_3$ , и значит, неприводим. Соответствующее поле  $\mathbb{F}_9 = \mathbb{F}_3[i]$  состоит из девяти элементов  $a + bi$  где  $a, b \in \{-1, 0, 1\} = \mathbb{F}_3$ , а  $i^2 = -1$ . Автоморфизм Фробениуса  $F_3 : a \mapsto a^3$  переводит элемент  $a + bi$  в  $a - bi$ .

Упражнение 3.22. Составьте для поля  $\mathbb{F}_9$  таблицу умножения и таблицу обратных элементов, перечислите все имеющиеся в  $\mathbb{F}_9$  квадраты и кубы и выясните, не изоморфна ли мультипликативная группа  $\mathbb{F}_9^*$  группе  $\mu_8$ .

Теорема 3.2

Для каждого  $n \in \mathbb{N}$  и простого  $p \in \mathbb{N}$  существует конечное поле  $\mathbb{F}_q$ , состоящее из  $q = p^n$  элементов.

Доказательство. Рассмотрим в  $\mathbb{F}_p[x]$  многочлен  $f(x) = x^q - x$ . По теор. 3.1 существует такое поле  $\mathbb{F} \supset \mathbb{F}_p$ , что  $f$  полностью раскладывается в  $\mathbb{F}[x]$  в произведение  $q$  линейных множителей. Поскольку производная  $f'(x) \equiv 1$ , все эти множители различны, т. е. в поле  $\mathbb{F}$  имеется ровно  $q$  различных чисел  $\alpha$ , таких что  $\alpha^q = \alpha$ . Они образуют поле: если  $\alpha^q = \alpha$ , то  $(-\alpha)^q = -\alpha$  и  $(\alpha^{-1})^q = \alpha^{-1}$ , и для любого  $\beta = \beta^q$  имеем  $\alpha\beta = \alpha^q\beta^q = (\alpha\beta)^q$  и

$$\alpha + \beta = \alpha^{p^n} + \beta^{p^n} = F_p^n(\alpha) + F_p^n(\beta) = F_p^n(\alpha + \beta) = (\alpha + \beta)^q,$$

где  $F_p : \mathbb{F} \rightarrow \mathbb{F}, x \mapsto x^p$ , это гомоморфизм Фробениуса. □

Упражнение 3.23. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

**3.5.1. Конечные мультипликативные подгруппы в поле.** Рассмотрим абелеву группу  $A$ , операцию в которой будем записывать мультипликативно.

Группа  $A$  называется *циклической*, если в ней имеется элемент  $a \in A$ , такой что все элементы группы  $A$  представляются в виде  $a^n$  с некоторым  $n \in \mathbb{Z}$ . Всякий элемент  $a \in A$ , обладающий этим свойством, называется *образующей* циклической группы  $A$ .

Например, группа комплексных корней из единицы  $\mu_n \subset \mathbb{C}$ , рассматривавшаяся нами в н° 3.4.3, является циклической, а её образующими являются первообразные корни.

Если группа  $A$  конечна, то среди степеней любого элемента  $b \in A$  будут встречаться одинаковые, скажем  $b^k = b^m$  с  $k > m$ . Домножая обе части этого равенства на  $b^{-m}$ , получаем равенство  $b^{k-m} = 1$ . Таким образом, для каждого элемента  $b \in A$  существует показатель  $t \in \mathbb{N}$ , такой что  $b^t = 1$ . Наименьший такой показатель называется *порядком* элемента  $b$  и обозначается  $\text{ord } b$ .

Если  $\text{ord } b = n$ , то элементы  $b^0 = 1, b^1 = b, b^2, \dots, b^{n-1}$  попарно различны, и любая целая степень  $b^m$  совпадает с одним из них: если  $m = nq + r$ , где  $r$  — остаток от деления  $m$  на  $n$ , то  $b^m = (b^n)^q b^r = b^r$ .

<sup>0</sup>т. е. комплексного корня того же самого многочлена  $x^2 + x + 1$

<sup>0</sup>см. н° 2.8.2 на стр. 29

Предложение 3.12

Любая конечная подгруппа  $A$  в мультипликативной группе  $\mathbb{k}^*$  произвольного поля  $\mathbb{k}$  является циклической.

Доказательство. Обозначим через  $m$  максимальный из порядков элементов группы  $A$ . Достаточно убедиться, что порядок любого элемента группы  $A$  делит  $m$ : тогда все элементы группы  $A$  будут корнями многочлена  $x^m - 1 = 0$ , а значит, их не более  $m$  и все они исчерпываются степенями имеющегося в  $A$  элемента  $m$ -того порядка.

Чтобы увидеть, что порядки всех элементов группы являются делителями максимального порядка, достаточно для любых двух элементов  $b_1, b_2 \in A$ , имеющих порядки  $m_1, m_2$ , построить элемент  $b \in A$ , порядок которого равен  $\text{нок}(m_1, m_2)$ .

Упражнение 3.24. Покажите, что при  $\text{нод}(m_1, m_2) = 1$  в качестве такого элемента подойдёт  $b = b_1 b_2$ .

Если  $m_1$  и  $m_2$  не взаимно просты, то, раскладывая их согласно [упр. 2.8](#) в произведение простых чисел, мы можем представить  $\text{нок}(m_1, m_2)$  в виде произведения  $\ell_1 \ell_2$  так, что  $m_1 = k_1 \ell_1$ ,  $m_2 = k_2 \ell_2$  и  $\text{нод}(\ell_1, \ell_2) = 1$ .

Упражнение 3.25. Убедитесь в этом.

Элементы  $b'_1 = b_1^{k_1}$  и  $b'_2 = b_2^{k_2}$  имеют взаимно простые порядки  $\ell_1$  и  $\ell_2$ , а их произведение  $b'_1 b'_2$  по [упр. 3.24](#) имеет порядок  $\ell_1 \ell_2 = \text{нок}(m_1, m_2)$ , что и требовалось.  $\square$

Теорема 3.3

Всякое конечное поле изоморфно одному из полей  $\mathbb{F}_q$ , построенных в [теор. 3.2](#).

Доказательство. Если  $\text{char } \mathbb{F} = p$ , то по [упр. 3.23](#) поле  $\mathbb{F}$  состоит из  $q = p^n$  элементов (для подходящего  $n \in \mathbb{N}$ ), а его ненулевые элементы образуют по [предл. 3.12](#) циклическую группу по умножению, порождённую некоторым элементом  $\zeta \in \mathbb{F}^*$ , так что

$$\mathbb{F} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}.$$

Мы построим сейчас ещё одно поле из  $q$  элементов, которое будет изоморфно как полю  $\mathbb{F}$ , так и полю  $\mathbb{F}_q$  из [теор. 3.2](#).

Обозначим через  $g \in \mathbb{F}_p[x]$  приведённый многочлен наименьшей степени, такой что  $g(\zeta) = 0$ . Тогда правило  $h(x) \pmod{g} \mapsto h(\zeta)$  корректно определяет сюръективный гомоморфизм колец  $\text{ev}_\zeta : \mathbb{F}_p[x]/(g) \rightarrow \mathbb{F}$ .

Упражнение 3.26. Покажите, что  $g$  неприводим в  $\mathbb{F}_p[x]$  и нацело делит любой многочлен  $f \in \mathbb{F}_p[x]$ , для которого  $f(\zeta) = 0$ .

Из упражнения вытекает, что кольцо вычетов  $\mathbb{F}_p[x]/(g)$  является полем. Поэтому гомоморфизм  $\text{ev}_\zeta$  инъективен и  $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$ .

С другой стороны, поскольку  $\zeta$  является корнем многочлена  $f(x) = x^q - x$ , из [упр. 3.26](#) вытекает, что  $f = gu$  для некоторого  $u \in \mathbb{F}_p[x]$ . Подставляя в это равенство  $q$  элементов поля  $\mathbb{F}_q$ , построенного в [теор. 3.2](#) и состоящего в точности из  $q$  корней многочлена  $f$ , заключаем, что хотя бы один из них — назовём его  $\xi \in \mathbb{F}_q$  — является корнем и для  $g$ . Тогда правило  $h(x) \pmod{g} \mapsto h(\xi)$  корректно задаёт вложение полей  $\text{ev}_\xi : \mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$ , сюръективное, поскольку оба поля состоят из  $q$  элементов. Тем самым,  $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$ .  $\square$

**3.5.2. Квадратичные вычеты.** Зафиксируем целое простое  $p > 2$ . Ненулевые элементы поля  $\mathbb{F}_p$ , являющиеся квадратами, называются *квадратичными вычетами* по модулю  $p$ . Они образуют мультипликативную подгруппу в  $\mathbb{F}_p^*$  — образ мультипликативного гомоморфизма  $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$  возведения в квадрат  $x \mapsto x^2$ . Ядро этого гомоморфизма состоит из двух элементов, поскольку уравнение  $x^2 = 1$  имеет в поле  $\mathbb{F}_p$  ровно два корня  $x = \pm 1$ . Тем самым, квадратичных вычетов имеется ровно  $(p-1)/2$ .

Судить о том, является ли данный элемент  $a \in \mathbb{F}_p^*$  квадратом, можно при помощи малой теоремы Ферма<sup>0</sup>, согласно которой  $a^{p-1} = 1$  для любого  $a \in \mathbb{F}_p^*$ . Если  $b = a^2$ , то  $b^{(p-1)/2} = a^{p-1} = 1$ . Мультипликативный гомоморфизм

$$\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*, \quad x \mapsto x^{(p-1)/2} \quad (3-19)$$

нетривиален, т. к. уравнение  $x^{(p-1)/2} = 1$  имеет не более  $(p-1)/2 < p-1$  корней в поле  $\mathbb{F}_p$ . Поскольку образ гомоморфизма (3-19) содержится среди корней всё того же уравнения  $x^2 = 1$ , он состоит в точности из двух элементов  $\pm 1$ . Тем самым, ядро гомоморфизма (3-19) в точности совпадает с подгруппой квадратов, т. е.  $a \in \mathbb{F}_p^*$  является квадратом тогда и только тогда, когда  $a^{(p-1)/2} = 1$ . Например,  $-1$  является квадратом в  $\mathbb{F}_p$  в точности тогда, когда  $(p-1)/2$  чётно.

Для произвольного  $n \in \mathbb{N}$  и простого  $p > 2$  число

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} [n]_p^{(p-1)/2} = \begin{cases} 1 & \text{когда } n \text{ ненулевой квадрат по модулю } p \\ 0 & \text{когда } n : p \\ -1 & \text{когда } n \text{ не является квадратом по модулю } p \end{cases} \quad (3-20)$$

называется *символом Лежандра – Якоби*. Из определения очевидно, что он зависит только от класса  $[n]_p \in \mathbb{Z}/(p)$  и мультипликативен по  $n$ :

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Упражнение 3.27\*. Покажите, что для простого  $p > 2$  символ  $\left(\frac{2}{p}\right) = 1$  тогда и только тогда, когда  $p \equiv \pm 1 \pmod{8}$ .

В общем случае символ Лежандра – Якоби легко вычисляется благодаря следующей замечательной теореме, открытой Гауссом.

**Теорема 3.4 (квадратичный закон взаимности)**

Для любых простых  $p, q > 2$   $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ . □

Два доказательства этой теоремы, предложенные Эйзенштейном и Золотарёвым, намечены в задачах из необязательного листка № 3½. Вот пример того, как она работает:

$$\left(\frac{57}{179}\right) = \left(\frac{179}{57}\right) = \left(\frac{8}{57}\right) = \left(\frac{2}{57}\right)^3 = 1,$$

т. е. 57 это квадрат по модулю 179.

---

<sup>0</sup>см. сл. 2.1 на стр. 23

### Ответы и указания к некоторым упражнениям

Упр. 3.3. Ответ:  $(y^n - x^n)/(y - x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \dots + yx^{n-2} + x^{n-1}$ .

Упр. 3.5. Если  $f(x) = \sum a_k x^k$ , то  $f(x+t) = \sum_{k,v} a_k \binom{k}{v} \cdot x^{k-v} t^v = \sum_v t^v \cdot f_v(x)$ , где

$$f_v(x) = \sum_{k \geq v} a_k \binom{k}{v} \cdot x^{k-v} = \frac{1}{v!} \frac{d^k}{dx^k} \sum_{k \geq 0} a_k x^k.$$

Упр. 3.7. Годаются дословно те же аргументы, что и в [упр. 2.8](#).

Существование. если  $f$  неприводим, то он сам и будет своим разложением, если  $f$  приводим, то он является произведением многочленов строго меньшей степени, которые в свою очередь или неприводимы или являются произведениями многочленов строго меньшей степени и т. д. Поскольку степень не может бесконечно уменьшаться, мы в конце концов получим требуемое разложение.

Единственность. Для любого приведённого неприводимого многочлена  $p$  и любого многочлена  $g$  выполняется следующая альтернатива: либо  $\text{нод}(p, g) = p$ , и тогда  $g$  делится на  $p$ , либо  $\text{нод}(p, g) = 1$ , и тогда  $g$  взаимно прост с  $p$ . Пусть в равенстве

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

все сомножители неприводимы. Деля  $p_1$  на старший коэффициент, мы можем считать, что он приведён. Поскольку  $\prod q_i$  делится на  $p_1$ , многочлен  $p_1$ , в силу [лем. 2.3](#), не может быть взаимно прост с каждым  $q_i$ . Согласно упомянутой выше альтернативе, найдётся  $q_i$  (скажем,  $q_1$ ), который делится на  $p_1$ . Так как  $q_1$  неприводим,  $q_1 = \lambda p_1$ , где  $\lambda$  — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 3.10. Единственность вытекает из [сл. 3.2](#): разность двух многочленов степени  $n$ , принимающих одинаковые значения в  $n+1$  точках, обращается в нуль в этих  $n+1$  точках, т. е. имеет  $n+1$  разных корней, что возможно только если эта разность нулевая. Существование: приведённый многочлен степени  $n$ , равный нулю во всех точках  $a_v$ , кроме  $i$ -той, есть  $\prod_{v \neq i} (x - a_v)$ . Деля этот многочлен на его значение в точке  $a_i$ , получаем многочлен  $f_i(x) = \prod_{v \neq i} (x - a_v) / \prod_{v \neq i} (a_i - a_v)$ , такой что

$$f_i(a_v) = \begin{cases} 1, & \text{при } v = i \\ 0, & \text{при } v \neq i. \end{cases}$$

Таким образом, искомый многочлен равен  $\sum_{i=0}^n b_i \cdot f_i(x) = \sum_{i=0}^n b_i \prod_{v \neq i} (x - a_v) / (a_i - a_v)$ .

Упр. 3.11. Если многочлен степени  $\leq 3$  приводим, то он имеет делитель степени один, корень которого будет корнем исходного многочлена.

Упр. 3.12. См. [упр. 1.9](#) на стр. 11.

Упр. 3.13. Вложение  $\varphi : \mathbb{k} \hookrightarrow \mathbb{k}[x]/(x - \alpha)$  в качестве констант сюръективно, поскольку число  $\alpha \in \mathbb{k}$  переходит в класс  $[x]$ , и значит, для любого  $g \in \mathbb{k}[x]$  число  $g(\alpha)$  переходит в класс  $[g]$ .

- Упр. 3.14. Обратным элементом к произвольному ненулевому  $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$  является  $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ . Кольцо в (а) содержит делители нуля:  $[t+1] \cdot [t^2-t+1] = [0]$  и, тем самым, не является полем. Кольцо в (б) является полем: многочлен  $p = \vartheta^3 + 2$  не имеет корней в  $\mathbb{Q}$ , и значит, не делится в  $\mathbb{Q}[x]$  ни на какой многочлен первой или второй степени; следовательно,  $p$  взаимно прост со всеми  $g \in \mathbb{Q}[x]$ , не делящимися на  $p$ , т. е. для любого  $[g] \neq [0]$  существуют  $h_1, h_2 \in \mathbb{Q}[x]$ , такие что  $h_1g + h_2p = 1$ ; тем самым,  $[h_1] = [g]^{-1}$ .
- Упр. 3.15. Указание: достаточно рассмотреть случай  $a_1 = 1$  и найти обратные ко всем элементам  $\vartheta - a$ ; для этого воспользуйтесь алгоритмом Евклида (см. п. 3.2.2): класс  $h(\vartheta)$ , обратный к классу  $\vartheta - a$ , задаётся таким многочленом  $h \in \mathbb{Q}[x]$ , что

$$h(x)(x - a) + g(x)(x^2 + x + 1) = 1$$

для некоторого  $g \in \mathbb{Q}[x]$ ; остаток от деления  $x^2 + x + 1$  на  $x - a$  равен  $a^2 + a + 1$ , так что алгоритм Евклида остановится уже на втором шагу.

- Упр. 3.17. Число  $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$  является корнем многочлена

$$z^5 - 1 = (z - 1)(z^4 + z^3 + z^2 + z + 1).$$

Уравнение  $z^4 + z^3 + z^2 + z + 1 = 0$  можно решить в радикалах, деля обе части на  $z^2$  и вводя новую переменную  $t = z + z^{-1}$ .

- Упр. 3.18. Пусть  $\zeta = \zeta_1 = \cos(2\pi/n) + i \sin(2\pi/n)$  — первообразный корень с наименьшим положительным аргументом, и  $\xi = \zeta^k$ . Докажите более сильное утверждение: среди целых степеней корня  $\xi$  встречаются те и только те степени первообразного корня  $\zeta$ , которые делятся на  $\text{нод}(k, n)$ , ибо равенство  $\zeta^m = \xi^x$  означает, что  $m = kx + ny$  для некоторого  $y \in \mathbb{Z}$ .

- Упр. 3.19. См. листок № 3 $\frac{2}{3}$ .

- Упр. 3.20. Из равенства  $z_1z_2 = 1$  вытекает равенство  $|z_1| \cdot |z_2| = 1$  на длины. Поскольку гауссово число  $z \neq 0$  имеет  $|z|^2 \in \mathbb{N}$ , обратимым может быть только  $z$  с  $|z| = 1$ . Таких чисел в  $\mathbb{Z}[i]$  ровно четыре:  $\pm 1$  и  $\pm i$ , и все они обратимы.

- Упр. 3.23. Это сразу следует из теоремы сл. 6.1 на стр. 88 о существовании базиса в конечномерном векторном пространстве: если  $\text{char } \mathbb{F} = p$ , то  $\mathbb{F} \supset \mathbb{F}_p$  и является конечномерным векторным пространством над  $\mathbb{F}_p$ . Выбирая в нём базис  $e_1, e_2, \dots, e_n$ , заключаем, что  $\mathbb{F}$  состоит из  $p^n$  векторов  $x_1e_1 + x_2e_2 + \dots + x_n e_n$ , где каждый коэффициент  $x_i$  независимо пробегает  $\mathbb{F}_p$  (см. прим. 6.10 на стр. 89). Менее геометрическое решение заключается в том, чтобы получить конечное поле  $\mathbb{F}$  последовательными расширениями простого подполя  $\mathbb{F}_p \subset \mathbb{F}$ . Каждый шаг этого построения заключается в присоединении к очередному, уже построенному полю  $\mathbb{F}'$ , такому что  $\mathbb{F}_p \subset \mathbb{F}' \subset \mathbb{F}$ , какого-нибудь элемента  $\zeta \in \mathbb{F} \setminus \mathbb{F}'$ . Число элементов в получающемся поле  $\mathbb{F}[\zeta] \supset \mathbb{F}'$  является  $n$ -той степенью числа элементов в поле  $\mathbb{F}'$ , откуда нужное утверждение следует по индукции.

- Упр. 3.24. Равенство  $(b_1b_2)^k = 1$  равносильно равенству  $b_1^k = b_2^{m_2-k}$ . Тогда

$$b_2^{m_1(m_2-k)} = b_1^{m_1k} = 1,$$

откуда  $m_1(m_2 - k)$  делится на  $m_2$ , а значит,  $k$  делится на  $m_2$ . В силу симметрии между  $b_1$  и  $b_2$ , показатель  $k$  делится также и на  $m_1$ . А так как  $m_1$  и  $m_2$  взаимно просты,  $k$  делится на  $m_1m_2$ . Поскольку  $(b_1b_2)^{m_1m_2} = 1$ ,  $\text{ord}(b_1b_2) = m_1m_2$ .

Упр. 3.25. Надо отправить в  $\ell_1$  все простые делители числа  $m_1$ , входящие в разложение числа  $m_1$  в бóльшей степени, чем в разложение числа  $m_2$ .

Упр. 3.26. Если  $g(x) = h_1(x) \cdot h_2(x)$ , то  $h_1(\zeta) = 0$  или  $h_2(\zeta) = 0$ , поэтому степень одного из сомножителей не меньше, чем  $\deg g$ . Если  $f(\zeta) = 0$ , то деля  $f$  на  $g$  с остатком:  $f = gh + r$ , и вычисляя при  $x = \zeta$ , получаем  $r(\zeta) = 0$ . Так как  $\deg r < \deg g$ , заключаем, что  $r = 0$ .

Упр. 3.27. Запишите элементы поля  $\mathbb{F}_p$  в строку вида:

$$-[(p-1)/2], \dots, -[1], [0], [1], \dots, [(p-1)/2]$$

и покажите, что<sup>0</sup>  $a \in \mathbb{F}_p^*$  тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» от умножения на  $a$ , чётно, после чего примените это к  $a = 2$ .

---

<sup>0</sup>это утверждение известно как *лемма Гаусса о квадратичных вычетах*