§3. Многочлены и расширения полей

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

3.1. Формальные степенные ряды и многочлены. Бесконечное выражение вида

$$A(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \dots, \quad \text{где} \quad a_i \in K \tag{3-1}$$

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

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

равны, если $a_i = b_i$ для всех i. Сложение и умножение рядов (3-2) определяется стандартными правилами раскрытия скобок и приведения подобных слагаемых[1]: коэффициенты s_m и p_m рядов $S(X) = A(x) + B(x) = s_0 + s_1 x + s_2 x^2 + \dots$ и $P(x) = A(x)B(x) = p_0 + p_1 x + p_2 x^2 + \dots$ суть

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

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

$$F(x) = \sum_{\nu_1, \dots, \nu_n \in \mathbb{Z}_{\geqslant 0}} a_{\nu_1 \dots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}.$$

3.1.1. Алгебраические операции над формальными рядами. Назовём *n-арной алгебраической операцией* в $K[\![x]\!]$ всякое правило, сопоставляющее n рядам

$$f_1, f_2, \dots, f_n \in K[\![x]\!]$$

новый ряд $f \in K[\![x]\!]$ так, что каждый коэффициент ряда f вычисляется по коэффициентам рядов $f_1, f_2, \dots, f_n$ при помощи конечного числа[2] сложений и умножений.

[1] Говоря формально, операции, о которых тут идёт речь, являются операциями над *последовательностями* (a_ν) и (b_ν) элементов кольца K. Буква x используется лишь для облегчения восприятия этих операций.

[2] Которое может зависеть от номера коэффициента.

Например, сложение и умножение рядов — это алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[1]. Напротив, подстановка в ряд $f(x)$ вместо x любого ряда $g(x) = b_1x + b_2x^2 + \cdots$ с нулевым свободным членом — это алгебраическая операция, дающая ряд

$$f(g(x)) = \sum a_k(b_1x + b_2x^2 + \cdots)^k = \\ a_0 + a_1(b_1x + b_2x^2 + \cdots) + a_2(b_1x + b_2x^2 + \cdots)^2 + a_3(b_1x + b_2x^2 + \cdots)^3 + \cdots \\ = a_0 + (a_1b_1)\cdot x + (a_1b_2 + a_2b_1^2)\cdot x^2 + (a_1b_3 + 2\,a_2b_1b_2 + a_3b_1^3)\cdot x^3 + \cdots,$$

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 $f(x) = a_0 + a_1x + a_2x^2 + \ldots \in K[\![x]\!]$ обратим в $K[\![x]\!]$ если и только если его свободный член a_0 обратим в K, и в этом случае обращение $f \mapsto f^{-1}$ является алгебраической операцией над рядом f.

Доказательство. Если имеется такой ряд $f^{-1}(x) = b_0 + b_1x + b_2x^2 + \ldots$, что

$$f(x)\cdot f^{-1}(x) = \big(a_0 + a_1x + a_2x^2 + \ldots\big)\cdot\big(b_0 + b_1x + b_2x^2 + \ldots\big) = 1\,, \tag{3-4}$$

то $a_0b_0 = 1$, откуда a_0 обратим. Наоборот, допустим, что $a_0 \in K$ обратим. Приравнивая коэффициенты при одинаковых степенях x в средней и правой части (3-4), мы получаем на коэффициенты b_i бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1\\ a_0b_1 + a_1b_0 &= 0\\ a_0b_2 + a_1b_1 + a_2b_0 &= 0\\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ &\end{aligned} \tag{3-5}$$

из которой $b_0 = a_0^{-1}$, и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0)$ при $k \geqslant 1$. □

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 $x_1, x_2, \ldots, x_n$ с коэффициентами в кольце K образуют в кольце всех формальных степенных рядов подкольцо, которое обозначается $K[x_1, x_2, \ldots, x_n] \subset K[\![x_1, x_2, \ldots, x_n]\!]$. Многочлен от одной переменной x представляет собой формальное выражение вида $f(x) = a_0 + a_1x + \cdots + a_nx^n$. 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[2], то для любых многочленов $f_1, f_2 \in K[x]$ выполняется равенство

[1] 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 α. Однако при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений.

[2] Т. е. с единицей и без делителей нуля.

$\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)$. 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. □

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:

$$f(x + t) = f_0(x) + f_1(x) \cdot t + f_2(x) \cdot t^2 + f_3(x) \cdot t^3 + \dots = \sum_{m \geqslant 0} f_m(x) \cdot t^m . \tag{3-6}$$

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

$$\frac{f(x+t) - f(x)}{t} = a_1 \cdot \frac{(x+t) - t}{t} + a_2 \cdot \frac{(x+t)^2 - t^2}{t} + a_3 \cdot \frac{(x+t)^3 - t^3}{t} + \dots = \\ = \sum_{k \geqslant 1} a_k \cdot \left((x+t)^{k-1} + (x+t)^{k-2} x + (x+t)^{k-3} x^2 + \dots + x^{k-1} \right) .$$

Получаем хорошо известную формулу

$$f'(x) = \sum_{k \geqslant 1} k\, a_k x^{k-1} = a_1 + 2\, a_2 x + 3\, a_3 x^2 + \dots \tag{3-7}$$

Пример 3.1 (ряды с нулевой производной)
Из формулы (3-7) вытекает, что производная от константы равна нулю. Если характеристика[1] $\operatorname{char} K = 0$, 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

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

[1] См. n° 2.8 на стр. 30.

представляет собою сумму m единиц кольца. В частности, над полем $\Bbbk$ характеристики $p > 0$ производная от ряда $f(x)$ равна нулю тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого $g \in \Bbbk[\![x]\!]$.

Упражнение 3.5. Покажите, что при простом $p \in \mathbb{N}$ для любого $g \in \mathbb{F}_p[\![x]\!]$ выполняется равенство $g(x^p) = g(x)^p$.

Предложение 3.3 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[\![x]\!]$ справедливы равенства

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

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

$$\big(f(g(x))\big)' = g'(x) \cdot f'\big(g(x)\big), \tag{3-9}$$

а если ряд f обратим, то

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

Доказательство. Первые два равенства в (3-8) вытекают прямо из формулы (3-7). Для доказательства третьего перемножим ряды

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

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: подставляя в $f(x)$ вместо x ряд $g(x+t)$, получаем

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

Введём ряд $\tau(x,t) \stackrel{\text{def}}{=} g(x+t) - g(x) = t \cdot g'(x) + (\text{члены, делящиеся на } t^2)$ и перепишем правую часть предыдущего разложения как

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

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

Упражнение 3.6. Покажите, что ряды f_m из разложения (3-6) имеют вид[1]

$$f_m(x) = \frac{1}{m!} \frac{d^m}{dx^m} f(x).$$

[1]Здесь и далее через $\frac{d^m}{dx^m} = \big(\frac{d}{dx}\big)^m$ 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. Пусть

$$f = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$
$$u = b_0 x^k + b_1 x^{k-1} + \cdots + b_{k-1} x + b_k,$$

где b_0 обратим. Если $n < k$, можно взять $q = 0$ и $r = f$. Если $k = 0$, т. е. $u = b_0$, можно взять $r = 0$, $q = b_0^{-1} f$. При $n \geqslant k > 0$ можно по индукции считать, что теорема верна для всех многочленов f степени, строго меньшей, чем n. Поскольку степень многочлена $f - a_0 b_0^{-1} x^{n-k} u$ строго меньше n, он представляется в виде $qu + r$, где $r = 0$ или $\deg r < \deg u$. Тогда

$$f = (q + a_0 b_0^{-1} x^{n-k}) \cdot u + r$$

также представляется в требуемом виде. Если кольцо K целостное, и p, s — другая такая пара многочленов, 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 $r - s = 0$. □

Определение 3.1
Многочлены q и r, удовлетворяющие условиям предл. 3.4 называются *неполным частным* и *остатком* от деления f на u в $K[x]$.

Следствие 3.1
Для любых многочленов $f, g \in \Bbbk[x]$ с коэффициентами в произвольном поле $\Bbbk$ существует единственная пара многочленов $q, r \in \Bbbk[x]$, 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 многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ на линейный двучлен $x - \alpha$ 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 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$.

Упражнение 3.7 (схема Горнера). Убедитесь, что

$$f(\alpha) = a_0 + \alpha \cdot \Big(a_1 + \alpha \cdot \Big(a_2 + \cdots + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n) \big) \cdots \Big) \Big)$$

Предложение 3.5
Пусть $\Bbbk$ — произвольное поле. Для любого набора многочленов $f_1, f_2, \dots, f_n \in \Bbbk[x]$ существует единственный приведённый многочлен $d \in \Bbbk[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i. Многочлен d представляется в виде

$$f_1 h_1 + f_2 h_2 + \cdots + f_n h_n, \quad \text{где} \quad h_i \in \Bbbk[x]. \tag{3-11}$$

Произвольно взятый многочлен $g \in \Bbbk[x]$ 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 n° 2.4.2 на стр. 25. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (3-11), через

$$(f_1, f_2, \dots, f_n) \stackrel{\text{def}}{=} \{f_1 h_1 + f_2 h_2 + \cdots + f_n h_n \mid h_i \in \Bbbk[x]\}. \tag{3-12}$$

Это подкольцо в $\Bbbk[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg (с любым $h \in \Bbbk[x]$). 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. □

Определение 3.2
Многочлен d из предл. 3.5 называется *наибольшим общим делителем* многочленов f_i и обозначается нод$(f_1, f_2, \dots, f_n)$.

3.2.1. Взаимная простота. Из предл. 3.5 вытекает, что в кольце $\Bbbk[x]$ многочленов с коэффициентами в поле *взаимная простота* многочленов $f_1, f_2, \dots, f_m$, т. е. возможность представить единицу в виде $1 = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n$, равносильна равенству 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[1] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 3.8. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: любой многочлен f является произведением конечного числа неприводимых многочленов, причём любые два таких представления $p_1 p_2 \cdots p_k = f = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\ i\ p_i = \lambda_i q_i$, где $\lambda_i \in \Bbbk$ — некоторые ненулевые константы.

[1] Т. е. с единицей и без делителей нуля.

3.2.2. Алгоритм Евклида из n° 2.2.2 дословно переносится на многочлены с коэффициентами в произвольном поле $\Bbbk$. А именно, для пары многочленов $f_1, f_2 \in \Bbbk[x]$ с $\deg(f_1) \geqslant \deg(f_2)$ положим $E_0 = f_1$, $E_1 = f_2$, $E_k =$ остатку от деления E_{k-2} на E_{k-1} при $k \geqslant 1$. 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 3.9. 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 $E_{r+1} = 0$ и $E_r = \text{нод}(f_1, f_2)$ тоже получатся представленными в таком виде, причём в выражении $0 = E_{r+1} = h_1^{(r+1)} f_1 + h_2^{(r+1)} f_2$ 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 3.10. Докажите это.

Вот как выглядит это вычисление для многочленов

$f_1(x) = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4$ и $f_2(x) = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4$:

$$E_0 = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4$$
$$E_1 = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4$$
$$E_2 = -4x^4 - 13x^3 - 21x^2 - 10x - 8 = E_0 - \left(x^2 - 2x + 3\right) E_1$$

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

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

следующий шаг уже даёт наибольший общий делитель

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

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 $\text{нод}(f_1, f_2) = x^2 + 3x + 4 = -\left(x^2 - 3\right) f_1(x) + \left(x^4 - 2x^3 + 2x - 2\right) f_2(x)$, а $\text{нок}(f_1, f_2) = \left(x^3 + 2x^2 + x + 1\right) f_1(x) = \left(x^5 + x^2 + 1\right) f_2(x)$.

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 равносильно тому, что $f(x)$ делится в $K[x]$ на $(x - \alpha)$.

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

Предложение 3.6
Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \alpha_2, \ldots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, $\deg(f) \geqslant s$ или $f = 0$.

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 $x = \alpha_2, \alpha_3, \ldots, \alpha_s$, убеждаемся, что $\alpha_2, \alpha_3, \ldots, \alpha_s$ являются корнями многочлена $q(x)$, и применяем индукцию. □

Следствие 3.2
Ненулевой многочлен f с коэффициентами из целостного кольца не может иметь в этом кольце более $\deg(f)$ различных корней.

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. Так как $\deg(f - g) \leqslant n$, и многочлен $f - g$ имеет больше n корней, он нулевой. □

Упражнение 3.12 (формула Лагранжа). Покажите, что для любых $n + 1$ попарно разных элементов поля $\Bbbk$ и произвольного набора значений $b_0, b_1, \ldots, b_n \in \Bbbk$ существует единственный такой многочлен $f(x) \in \Bbbk[x]$ степени $\deg f \leqslant n$, что $f(a_i) = b_i$ при всех i, и получите для него явную формулу.

3.3.1. Общие корни нескольких многочленов. Пусть $\Bbbk$ — поле. Число α тогда и только тогда является общим корнем многочленов $f_1, f_2, \ldots, f_m \in \Bbbk[x]$, когда α 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 нод$(f_1, f_2, \ldots, f_m)$, и наоборот. Таким образом, отыскание общих корней набора многочленов сводится к отысканию корней их наибольшего общего делителя, что бывает проще, чем отыскание корней любого из f_i в отдельности, т. к. степень нод$(f_1, f_2, \ldots, f_m)$ обычно меньше степеней всех f_i. Если многочлены $f_1, f_2, \ldots, f_m \in \Bbbk[x]$ взаимно просты, то они не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$. В самом деле, поскольку существуют многочлены $h_i \in \Bbbk[x]$, такие что $f_1 h_1 + f_2 h_2 + \cdots + f_m h_m = 1$, многочлены f_i не могут одновременно обратиться в нуль ни при каком значении x.

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

Предложение 3.7
Число $\alpha \in \Bbbk$ является кратным корнем многочлена $f \in \Bbbk[x]$ если и только если

$$f(\alpha) = f'(\alpha) = 0\,.$$

Доказательство. Если α — кратный корень многочлена f, то $f(x) = (x - \alpha)^2 g(x)$. Дифференцируя, получаем $f'(x) = (x - \alpha)\big(2g(x) + (x - \alpha)g'(x)\big)$, откуда $f'(\alpha) = 0$. Если α 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 $f'(\alpha) = g(\alpha) \neq 0$. □

Определение 3.4
Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если нод$(f, f') = 1$. По предл. 3.7 это означает, что многочлен f не имеет кратных корней ни в каком кольце $K \supset \Bbbk$.

Пример 3.3 (сепарабельность неприводимых многочленов)
Если многочлен $f \in \Bbbk[x]$ неприводим, то он взаимно прост со всеми ненулевыми многочленами меньшей степени. Поэтому нод$(f, f') = 1$, если только f' не обращается тождественно в нуль. Поскольку над полем характеристики нуль производная многочлена положительной степени отлична от нуля, все неприводимые многочлены над полем характеристики нуль сепарабельны. Над конечным полем $\mathbb{F}_p = \mathbb{Z}/(p)$ многочлен $f \in \mathbb{F}_p[x]$ имеет $f' = 0$ если и только если $f(x) = g(x^p)$ для некоторого $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \in \mathbb{F}_p[x]$. Поскольку возведение в p-тую степень является в характеристике p гомоморфизмом[1] и тождественно действует на элементах поля $\mathbb{F}_p$,

$$\begin{aligned} f(x) = g(x^p) = b_0x^{pm} + b_1x^{p(m-1)} + \cdots + b_{m-1}x^p + b_0 = \\ = b_0^px^{pm} + b_1^px^{p(m-1)} + \cdots + b_{m-1}^px^p + b_0^p = \\ = \left(b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m\right)^p = g^p(x)\,. \end{aligned}$$

Таким образом, над полем $\mathbb{F}_p = \mathbb{Z}/(p)$ всякий многочлен с нулевой производной является чистой p-той степенью некоторого другого многочлена. В частности, любой многочлен с нулевой производной приводим, и значит, неприводимые многочлены над полем $\mathbb{F}_p$ тоже сепарабельны. Над бесконечными полями $\Bbbk$ конечной характеристики $\operatorname{char}\Bbbk = p > 0$ неприводимые многочлены уже не обязательно сепарабельны. Например, можно показать, что над полем $\Bbbk = \mathbb{F}_p(t)$ рациональных функций от одной переменной t с коэффициентами в поле $\mathbb{F}_p$ многочлен $f(x) = x^p - t$ неприводим, однако $f' \equiv 0$, т. е. f не сепарабелен.

Предложение 3.8
Если $\operatorname{char}\Bbbk = 0$, то $\alpha \in \Bbbk$ является m-кратным корнем многочлена $f \in \Bbbk[x]$ тогда и только тогда, когда α является корнем f и первых $(m-1)$ производных от f, но не является корнем m-той производной.

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

3.3.3. Присоединение корней. Кольцо вычетов $\Bbbk[x]/(f)$, где $f \in \Bbbk[x]$, определяется аналогично кольцу[2] $\mathbb{Z}/(n)$. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$ и обозначим через $(f) = \{fh \mid h \in \Bbbk[x]\}$ 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 $\Bbbk[x]$ в объединение непересекающихся классов $[g]_f = g + (f) = \{g + fh \mid h \in \Bbbk[x]\}$, которые называются *классами вычетов* по модулю f. Сложение и умножение этих классов задаётся формулами

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

Упражнение 3.13. Проверьте корректность[3] этого определения, а также выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

[1] См. прим. 2.6 на стр. 26.
[2] См. n° 2.4 на стр. 25.
[3] Т. е. независимость классов $[g+h]$ и $[gh]$ от выбора представителей $g \in [g]$ и $h \in [h]$.

Нулём кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей — класс $[1]_f = 1 + (f)$. Так как константы не делятся на многочлены положительной степени, классы всех констант $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$ гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому для классов чисел $c \in \Bbbk$ мы всюду далее будем писать c вместо $[c]_f$.

Упражнение 3.14. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Поскольку любой многочлен $g \in \Bbbk[x]$ единственным образом записывается в виде

$$g = fh + r\,, \quad \text{где} \quad \deg r < \deg f\,,$$

в каждом классе $[g]_f$ имеется единственный представитель $r \in [g]_f$ с $\deg(r) < \deg(f)$, т. е. каждый класс $[g]_f \in \Bbbk[x]/(f)$ *однозначно* записывается в виде

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

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

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

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

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

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

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 $\left(\sqrt{2}\right)^2 = 2$:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2\,bd) + (cb + ad)\sqrt{2}$$

Упражнение 3.15. 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) $\vartheta^3 + 2 = 0$.

Предложение 3.9
Пусть $\Bbbk$ — произвольное поле. Кольцо $\Bbbk[x]/(f)$ является полем тогда и только тогда, когда многочлен f неприводим в $\Bbbk[x]$.

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

Упражнение 3.16. Напишите явную формулу для вычисления обратного элемента к числу $a_0 + a_1\vartheta$ в поле $\mathbb{Q}[\vartheta]$, где $\vartheta^2 + \vartheta + 1 = 0$.

Теорема 3.1
Для любого поля $\Bbbk$ и любого многочлена $f \in \Bbbk[x]$ существует такое поле $\mathbb{F} \supset \Bbbk$, что f разлагается в $\mathbb{F}[x]$ в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\Bbbk$ и для всех многочленов степени $< n$ из $\Bbbk[x]$ мы умеем строить такое поле[1]. Если f приводим: $f = gh$, где $\deg g < n$ и $\deg h < n$, мы можем построить поле $\mathbb{L} \supset \Bbbk$ над которым g полностью разложится на линейные множители, а затем поле $\mathbb{F} \supset \mathbb{L}$ над которым разложится h, а тем самым, и f. Если f неприводим, рассмотрим поле $\mathbb{L} = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ в качестве классов констант, и многочлен f делится в $\mathbb{L}[x]$ 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 $\mathbb{F} \supset \mathbb{L}$. Тогда и f разложится над $\mathbb{F}$. □

Теорема 3.2 (китайская теорема об остатках)
Пусть $\Bbbk$ — произвольное поле, и многочлен $f \in \Bbbk[x]$ является произведением m попарно взаимно простых сомножителей: $f = f_1 f_2 \cdots f_m$, нод$(f_i, f_j) = 1$. Отображение

$$\varphi : \Bbbk[x]/(f) \to \Bbbk[x]/(f_1) \times \Bbbk[x]/(f_2) \times \cdots \times \Bbbk[x]/(f_m)$$
$$\varphi : [g]_f \longmapsto \left([g]_{f_1}, [g]_{f_2}, \ldots, [g]_{f_m}\right)$$

является корректно определённым изоморфизмом колец.

Доказательство. Проверки того, что φ корректно определён[2], является гомоморфизмом и имеет нулевое ядро, дословно повторяют рассуждения из n° 2.7, и мы оставляем их читателю. Покажем, что φ сюръективен. Для этого, как и в n° 2.7, построим для любого заданного набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f_i)$ такой многочлен $g \in \Bbbk[x]$, что $g \equiv r_i \pmod{f_i}$ при всех i. Для каждого i обозначим через $F_i = \prod_{\nu \neq i} f_\nu$ произведение всех многочленов f_ν кроме i-того. Так как f_i взаимно прост с каждым из f_ν с $\nu \neq i$, он по лем. 2.3 взаимно прост с F_i. Поэтому существует такой многочлен[3] $h_i \in \Bbbk[x]$, что $F_i \cdot h_i \equiv 1 \pmod{f_i}$. Так как многочлен $g_i = F_i \cdot h_i$ при этом делится на все f_ν с $\nu \neq i$, многочлен $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m \equiv r_i \pmod{f_i}$ при всех i. □

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 $x, y \in \mathbb{R}$, а класс $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2 = -1$. $\mathbb{C}$ является полем, так как для $x + yi \neq 0$

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

Комплексное число $z = x + yi$ удобно изображать на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат (x, y) *радиус-вектором* $0z$, ведущим из начала координат в точку $z = (x, y)$, как на рис. 3◇1 на стр. 43 ниже. Координаты (x, y) называются при этом *действительной* и *мнимой* частями числа $z \in \mathbb{C}$ и обозначаются через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ соответственно, а длина $|z| = \sqrt{x^2 + y^2}$ радиус вектора $0z$ называется *модулем* (или *абсолютной величиной*)

[1] Заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \Bbbk$.

[2] Т. е. $\varphi\left([g]_f\right)$ не зависит от выбора представителя $g \in \Bbbk[x]$ в классе $[g]_f \subset \Bbbk[x]$.

[3] Чтобы найти его явно, можно, например, взять остаток R_i от деления F_i на f_i и применить алгоритм Евклида к паре $E_0 = f_i$, $E_1 = R_i$.

комплексного числа z. Множество всех таких $\vartheta \in \mathbb{R}$, что поворот плоскости $\mathbb{C}$ вокруг нуля на угол ϑ совмещает координатный луч $0x$ с лучом $0z$, называется *аргументом* числа z и обозначается $\operatorname{Arg}(z) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}$, где α — ориентированная длина какой-нибудь дуги[1], идущей по единичной окружности из точки $(1, 0)$ в точку $z/|z|$.

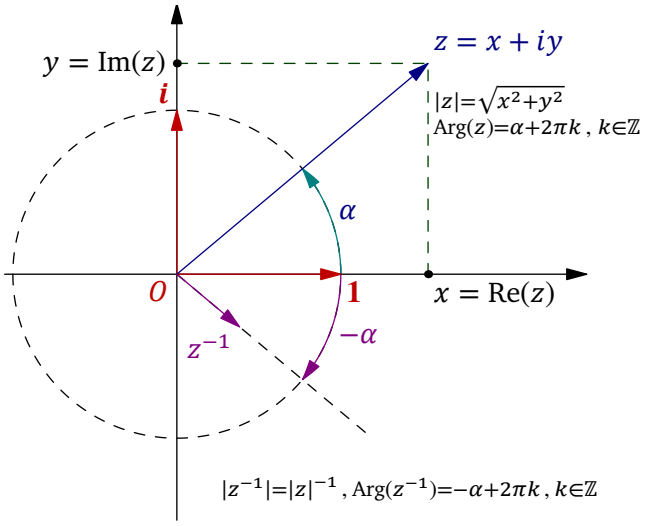

Рис. 3◇1.

Таким образом, $z = x + yi \in \mathbb{C}$ имеет $\operatorname{Re}(z) = |z| \cdot \cos\alpha$, $\operatorname{Im}(z) = |z| \cdot \sin\alpha$ и может быть записан как $z = |z| \cdot (\cos\alpha + i \cdot \sin\alpha)$, где $\alpha \in \operatorname{Arg}(z)$.

Лемма 3.1
Множество радиус-векторов точек z евклидовой координатной плоскости $\mathbb{R}^2$ с операцией сложения векторов и операцией умножения, заключающейся в перемножении модулей и сложении аргументов:

$$|z_1 z_2| \stackrel{\text{def}}{=} |z_1| \cdot |z_2| \tag{3-15}$$

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

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

Упражнение 3.17. 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 $0x$, а обратным к ненулевому вектору z является вектор z^{-1} с

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

[1]Любые две таких дуги отличаются друг от друга на целое число оборотов, а «ориентированность» означает, что длину дуги следует брать со знаком «+», если движение вдоль этой дуги происходит против часовой стрелки, и со знаком «−», если по часовой стрелке.

(см. рис. 3⋄1). Для проверки дистрибутивности заметим, что отображение $\lambda_a\colon z \mapsto az$ умножения на фиксированный ненулевой вектор a это *поворотная гомотетия*[1] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b+c) = ab + ac$ утверждает, что поворотная гомотетия перестановочна со сложением векторов: $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$. Это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы.

Таким образом, векторы на евклидовой координатной плоскости $\mathbb{R}^2$ образуют поле. Векторы, параллельные оси $0x$ образуют в этом поле подполе, изоморфное полю $\mathbb{R}$. Произвольный вектор $z = (x, y) \in \mathbb{R}^2$ записывается в виде $z = x + iy$, где i — единичный направляющий вектор оси $0y$, числа $x, y \in \mathbb{R}$ понимаются как векторы, параллельные оси 0, 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 $z_2 = x_2 + iy_2$ выполняются равенства

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$$
$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1)$$

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

3.4.1. Сопряжение. Числа$z = x + iy$ и $\overline{z} \stackrel{\text{def}}{=} x - iy$ называются *комплексно сопряжёнными*. В терминах комплексного сопряжения формулу для обратного числа можно записать в виде

$$z^{-1} = \overline{z}/|z|^2\,.$$

Геометрически, комплексное сопряжение $z \mapsto \overline{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси $0x$. С алгебраической точки зрения сопряжение является инволютивным[2] автоморфизмом поля $\mathbb{C}$, т. е. $\forall\, z \in \mathbb{C}\ \ \overline{\overline{z}} = z$ и $\forall\ z_1, z_2 \in \mathbb{C}$

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 \quad \text{и} \quad \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2\,.$$

3.4.2. Тригонометрия. Большая часть школьной тригонометрии является не самой удобной для восприятия записью заурядных вычислений с комплексными числами, 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 $\cos(\varphi_1+\varphi_2)+i\sin(\varphi_1+\varphi_2)$, а с другой стороны, пользуясь дистрибутивностью умножения, получаем $z_1 z_2 = \Big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2\Big) + i\Big(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2\Big)$, 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.

[1] *Поворотной гомотетией* относительно точки 0 на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки 0 и растяжения в ϱ раз относительно 0 (поскольку растяжения коммутируют с поворотами, всё равно, в каком порядке эта композиция выполняется).

[2] Отличный от тождественного эндоморфизм $\iota : X \to X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \mathrm{Id}_X$. По предл. 1.4 на стр. 13 всякая инволюция автоматически биективна.

Пример 3.4 (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 $(\cos\varphi + i\sin\varphi)^n$ скобки по форм. (1-9) на стр. 7, получаем равенство

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

заключающее в себе сразу *все* мыслимые формулы для кратных углов:

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

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

Упражнение 3.18. 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

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

имеется ровно n различных классов эквивалентности вещественных чисел по модулю добавления целых кратных 2π, 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 $0\leqslant k\leqslant n-1$. Таким образом, уравнение $z^n = 1$ имеет ровно n корней

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

расположенных в вершинах правильного n-угольника, вписанного в единичную окружность так, что вершина ζ_0 находится в точке 1 (см. рис. 3⋄2). Они образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-той степени из* единицы.

Корень $\zeta\in\boldsymbol{\mu}_n$ называются *первообразным корнем* степени n из единицы, если все остальные элементы группы $\boldsymbol{\mu}_n$ представляются в виде ζ^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 $\boldsymbol{\mu}_6$ на рис. 3⋄3 на стр. 46 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1}$.

Упражнение 3.19. Покажите, что корень $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ является первообразным тогда и только тогда, когда $\text{нод}(k,n) = 1$.

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

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

называется n-тым *круговым* (или *циклотомическим*) многочленом. Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z-z_1)(z-z_2)(z-z_3)(z-z_4) = z^4+z^3+z^2+z+1$$
$$\Phi_6(z) = (z-z_1)(z-z_4) = z^2 - z + 1\,.$$

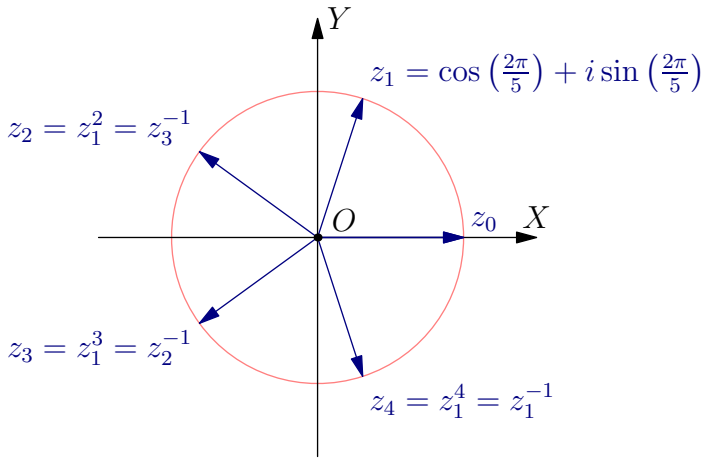

Рис. 3◇2. Корни уравнения $z^5 = 1$.

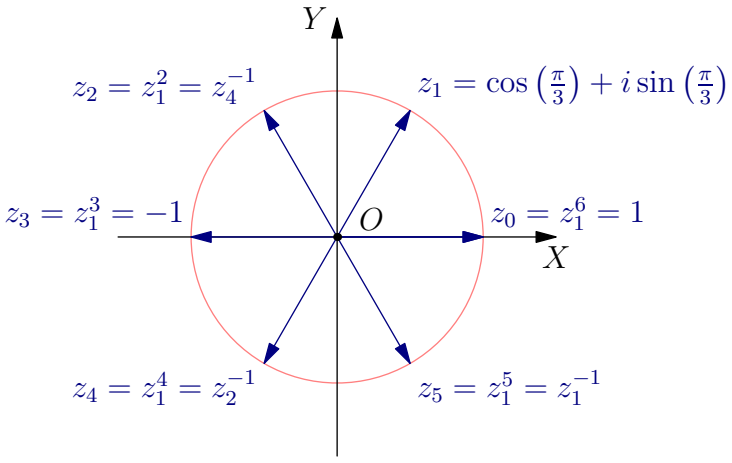

Рис. 3◇3. Корни уравнения $z^6 = 1$.

Упражнение 3.20*. Покажите, что при всех n многочлен Φ_n имеет целые коэффициенты и неприводим[1] в $\mathbb{Q}[x]$.

[1] Т. е. не являются произведениями многочленов строго меньшей степени.

Пример 3.5 (уравнение $z^n = a$)
Корни уравнения $z^n = a$ это числа $z = |z| \cdot (\cos\varphi + i\sin\varphi)$ с $|z|^n = |a|$, а $n\varphi \in \operatorname{Arg}(a)$. При $a = |a| \cdot (\cos\alpha + i\sin\alpha) \neq 0$ имеется ровно n таких чисел

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

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 α/n к оси $0x$.

Пример 3.6 (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 $n = z \cdot \overline{z}$. Из второго уравнения сразу же видно, что если числа m_1 и m_2 представляются в виде суммы двух квадратов

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

то их произведение $m = m_1m_2$ также является суммой двух квадратов:

$$m = z_1z_2 \cdot \overline{z_1z_2} = |z_1z_2|^2 = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2$$

(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 **??**, 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 **??** на стр. **??**.

Упражнение 3.21. Покажите, что обратимыми элементами кольца $\mathbb{Z}[i]$ являются четыре числа: ± 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

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

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[1]: 0, 1, $\omega = x \pmod{(x^2+x+1)}$ и $1 + \omega = \omega^2 = \omega^{-1}$.

Упражнение 3.22. Убедитесь, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

[1] 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 $\mathbb{R} \subset \mathbb{C}$, если понимать поле $\mathbb{C}$ как расширение $\mathbb{R}[\omega]$, где $\omega^2+\omega+1=0$, получающееся присоединением к полю $\mathbb{R}$ первообразного комплексного кубического корня из единицы[1]. Аналогом комплексного сопряжения $\mathbb{C} \to \mathbb{C}$, переводящего ω в $\overline{\omega} = \omega^2$, в поле $\mathbb{F}_4$ является гомоморфизм Фробениуса[2] $F_2 \colon \mathbb{F}_4 \to \mathbb{F}_4$, $a \mapsto a^2$, 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 $F_3 \colon a \mapsto a^3$ переводит элемент $a + bi$ в $a - bi$.

Упражнение 3.23. 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 $\boldsymbol{\mu}_8$.

Теорема 3.3
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 α, таких что $\alpha^q = \alpha$. Они образуют поле: если $\alpha^q = \alpha$, то $(-\alpha)^q = -\alpha$ и $\left(\alpha^{-1}\right)^q = \alpha^{-1}$, 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 $F_p \colon \mathbb{F} \to \mathbb{F}$, $x \mapsto x^p$, это гомоморфизм Фробениуса. □

Упражнение 3.24. 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 $\boldsymbol{\mu}_n \subset \mathbb{C}$, рассматривавшаяся нами в n° 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 $m \in \mathbb{N}$, такой что $b^m = 1$. Наименьший такой показатель называется *порядком* элемента b и обозначается $\operatorname{ord} b$.

Если $\operatorname{ord} b = n$, то элементы $b^0 = 1$, $b^1 = b$, b^2, …, 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 $b^m = (b^n)^q b^r = b^r$.

[1] Т. е. комплексного корня того же самого многочлена $x^2 + x + 1$.

[2] См. n° 2.8.2 на стр. 31.

Предложение 3.10
Любая конечная подгруппа A в мультипликативной группе $\Bbbk^*$ произвольного поля $\Bbbk$ является циклической.

Доказательство. Обозначим через m максимальный из порядков элементов группы A. Достаточно убедиться, что порядок каждого 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 нок(m_1, m_2).

Упражнение 3.25. Покажите, что при 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 нок(m_1, m_2) в виде произведения $\ell_1 \ell_2$ так, что

$$m_1 = k_1 \ell_1, \quad m_2 = k_2 \ell_2 \quad \text{и} \quad (\ell_1, \ell_2) = 1.$$

Упражнение 3.26. Убедитесь в этом.

Элементы $b_1' = b_1^{k_1}$ и $b_2' = b_2^{k_2}$ имеют взаимно простые порядки ℓ_1 и ℓ_2, а их произведение $b_1' b_2'$ по упр. 3.25 имеет порядок $\ell_1 \ell_2 =$ нок(m_1, m_2), что и требовалось. □

Теорема 3.4
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 3.3.

Доказательство. Если $\operatorname{char} \mathbb{F} = p$, то по упр. 3.24 поле $\mathbb{F}$ состоит из $q = p^n$ элементов для подходящего $n \in \mathbb{N}$, а ненулевые элементы поля $\mathbb{F}$ образуют согласно предл. 3.10 циклическую группу по умножению, порождённую некоторым элементом $\zeta \in \mathbb{F}^*$, так что

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

Мы построим сейчас ещё одно поле из q элементов, которое будет изоморфно как полю $\mathbb{F}$, так и полю $\mathbb{F}_q$ из теор. 3.3. Для этого обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен наименьшей степени, такой что $g(\zeta) = 0$.

Упражнение 3.27. 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, а правило

$$h(x) \pmod g \mapsto h(\zeta)$$

корректно задаёт гомоморфизм колец $\mathrm{ev}_\zeta \colon \mathbb{F}_p[x]/(g) \to \mathbb{F}$. Он инъективен, т. к. $\mathbb{F}_p[x]/(g)$ поле, и сюръективен, поскольку его образ содержит все степени ζ^m. Тем самым, $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$.

С другой стороны, т. к. ζ является корнем многочлена $f(x) = x^q - x$, из упр. 3.27 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. 3.3 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 $\mathrm{ev}_\xi \colon \mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

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 в $\mathbb{F}_p^*$ мультипликативную подгруппу — образ мультипликативного гомоморфизма возведения в квадрат $\mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$. 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 мультипликативного гомоморфизма возведения в степень $(p-1)/2$:

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

По малой теореме Ферма[1], каждый лежащий в образе этого гомоморфизма элемент $x = a^{(p-1)/2}$ удовлетворяет уравнению $x^2 = a^{p-1} = 1$ и стало быть равен ± 1. С другой стороны образ гомоморфизма (3-19) отличен от 1, поскольку уравнение $x^{(p-1)/2} = 1$ имеет не более $(p-1)/2$ корней в поле $\mathbb{F}_p$. Тем самым, ядро гомоморфизма (3-19) состоит ровно из $(p-1)/2$ элементов и совпадает с подгруппой квадратов, т. е. $a \in \mathbb{F}_p^*$ является квадратом если и только если $a^{(p-1)/2} = 1$. 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

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

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 3.28*. 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 3.5 (квадратичный закон взаимности Гаусса)
Для любых простых $p, q > 2$ выполняется равенство

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Два доказательства этой теоремы, предложенные, соответственно, Эйзенштейном и Золотарёвым, намечены в листке $3\frac{1}{2}$. Вот пример того, как эта теорема 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.

[1] См. сл. 2.1 на стр. 26.

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

Упр. 3.5. $\left(a_0 + a_1x + a_2x^2 + \ldots\right)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \cdots = a_0 + a_1x^p + a_2x^{2p} + \cdots$ (первое равенство справедливо, поскольку возведение в p-тую степень перестановочно со сложением, второе — по малой теореме Ферма).

Упр. 3.6. Если $f(x) = \sum a_k x^k$, то $f(x+t) = \sum\limits_{k,\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu}t^\nu = \sum\limits_\nu t^\nu \cdot f_\nu(x)$, где

$$f_\nu(x) = \sum_{k\geqslant\nu} a_k\binom{k}{\nu}\cdot x^{k-\nu} = \frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0} a_k x^k\,.$$

Упр. 3.8. Годятся 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 нод$(p, g) = p$, и тогда g делится на p, либо нод$(p, g) = 1$, и тогда g взаимно прост с p. Пусть в равенстве

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m$$

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 λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 3.11. Если многочлен степени $\leqslant 3$ приводим, то у него есть делитель степени один, корень которого будет корнем исходного многочлена.

Упр. 3.12. Единственность вытекает из сл. 3.3. Для отыскания такого многочлена заметим, что многочлен $\prod\limits_{\nu\neq i}(x - a_\nu)$ зануляется во всех точках a_ν кроме i-той, где он принимает ненулевое значение. Деля его на это значение, получаем такой многочлен $f_i(x) = \prod\limits_{\nu\neq i}(x-a_\nu)/\prod\limits_{\nu\neq i}(a_i-a_\nu)$, что

$$f_i(a_\nu) = \begin{cases} 1, \text{ при } \nu = i \\ 0, \text{ при } \nu \neq i\,. \end{cases}$$

Искомый многочлен равен $\sum\limits_{i=0}^n b_i\cdot f_i(x) = \sum\limits_{i=0}^n b_i \prod\limits_{\nu\neq i}(x-a_\nu)/(a_i-a_\nu)$.

Упр. 3.13. См. упр. 1.10 на стр. 10.

Упр. 3.14. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x-\alpha)$ в качестве констант сюръективно, поскольку число $\alpha \in \Bbbk$ переходит в класс $[x]$, и значит, для любого $g \in \Bbbk[x]$ число $g(\alpha)$ переходит в класс $[g]$.

Упр. 3.15. 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 $h_1 g + h_2 p = 1$; тем самым, $[h_1] = [g]^{-1}$.

Упр. 3.16. Указание: достаточно найти обратные ко всем элементам $\vartheta - a$, что делается по алгоритму Евклида[1] — 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 $g \in \mathbb{Q}[x]$. Поскольку остаток от деления x^2+x+1 на $x-a$ равен a^2+a+1, алгоритм Евклида остановится уже на втором шагу.

Упр. 3.18. 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. 3.19. 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 ξ встречаются те и только те степени первообразного корня ζ, которые делятся на нод(k,n), ибо равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$.

Упр. 3.20. См. листок № $3\frac{2}{3}$.

Упр. 3.21. Из равенства $z_1 z_2 = 1$ 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: ± 1 и $\pm i$, и все они обратимы.

Упр. 3.24. Это сразу следует из теоремы **??** на стр. **??** о существовании базиса в конечномерном векторном пространстве: если $\operatorname{char}\mathbb{F} = p$, то $\mathbb{F} \supset \mathbb{F}_p$ и является конечномерным векторным пространством над $\mathbb{F}_p$. Выбирая в нём базис $e_1, e_2, \ldots, e_n$, заключаем, что $\mathbb{F}$ состоит из p^n векторов $x_1e_1 + x_2e_2 + \cdots + x_ne_n$, где каждый коэффициент x_i независимо пробегает $\mathbb{F}_p$ (см. **??** на стр. **??**). 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 $\mathbb{L}$, такому что $\mathbb{F}_p \subset \mathbb{L} \subset \mathbb{F}$, какого-нибудь элемента $\zeta \in \mathbb{F} \smallsetminus \mathbb{L}$. Число элементов в получающемся поле $\mathbb{F}[\zeta] \supset \mathbb{L}$ является n-той степенью числа элементов в поле $\mathbb{L}$, откуда нужное утверждение следует по индукции.

Упр. 3.25. 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 $(b_1b_2)^{m_1m_2} = 1$, $\operatorname{ord}(b_1b_2) = m_1m_2$.

[1] См. n° 3.2.2 на стр. 38.

Упр. 3.26. Надо отправить в ℓ_1 все простые делители числа m_1, входящие в разложение числа m_1 в большей степени, чем в разложение числа m_2.

Упр. 3.27. 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. 3.28. Запишите элементы поля $\mathbb{F}_p$ в строку вида:

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

и покажите, что[1] $a \in \mathbb{F}_p^*$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» от умножения на a, чётно, после чего примените это к $a = 2$.

[1] Это утверждение известно как *лемма Гаусса о квадратичных вычетах*.