§3. Многочлены и алгебраические числа

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

3.1. Степенные ряды и многочлены. Бесконечное выражение вида

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

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

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

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

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

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

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

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

[1]формально говоря, мы определяем здесь операции над *последовательностями* (a_ν) и (b_ν) 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[1]. Напротив, подстановка в ряд $f(x)$ вместо x любого ряда без свободного члена $g(x) = b_1x + b_2x^2 + \cdots$ — это алгебраическая операция, дающая ряд

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

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 $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in K[[x]]$ 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 $f^{-1}(x) = b_0 + b_1x + b_2x^2 + \cdots$, 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. Приравнивая коэффициенты при одинаковых степенях x в правой и левой части равенства

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

мы получаем на коэффициенты b_i бесконечную систему уравнений

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

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

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

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

[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; но при произвольных α 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[1], 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. □

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

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

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

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

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:

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

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

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

Получаем хорошо известную формулу

$$f'(x) = \sum_{k \geqslant 1} k\, a_k x^{k-1} = a_1 + 2\, a_2 x + 3\, a_3 x^2 + \cdots \tag{3-6}$$

[1] 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 $\operatorname{char} K = 0$, 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

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

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

$$\exists\, g \in \Bbbk[[x]] \;:\; f(x) = g(x^p) = g(x)^p \tag{3-7}$$

(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

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

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 (3-6). 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 $g(x+t)$: $\;f\big(g(x+t)\big) = f\big(g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2)\big)$ 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

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

откуда $\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)$. 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 $\big(f^{-1}\big)' = -f'/f^2$. $\square$

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 $n \geqslant \deg u$. Если $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ и $u = b_0x^k + b_1x^{k-1} + \cdots + b_{k-1}x + b_k$, 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 $f, g \in \Bbbk[x]$ 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 любого многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 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 $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

Упражнение 3.6 (схема Горнера). Выполнив деление уголком, покажите, 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

$$f_1h_1 + f_2h_2 + \dots + f_nh_n\,, \quad \text{где} \quad h_i \in \Bbbk[x]\,. \tag{3-11}$$

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. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (3-11), через

$$(f_1, f_2, \dots, f_n) = \{f_1h_1 + f_2h_2 + \dots + f_nh_n \mid h_i \in \Bbbk[x]\}\,. \tag{3-12}$$

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 $(f_1, f_2, \dots, f_n)$. Поскольку остаток $r = g - qd$ от деления произвольного многочлена $g \in (f_1, f_2, \dots, f_n)$ на d лежит в кольце $(f_1, f_2, \dots, f_n)$, его степень $\deg r$ не может быть строго меньше, чем $\deg d$, откуда $r = 0$, т. е. что 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 $\text{нод}(f_1, f_2, \dots, f_n)$.

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 $1 = h_1f_1 + h_2f_2 + \dots + h_nf_n$, 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[1] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 3.7. 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 $p_1p_2 \cdots p_k = f = q_1q_2 \cdots q_m$ 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 3.8. 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

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

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

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

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

следующий шаг уже даёт наибольший общий делитель

$$\begin{aligned}
E_4 &= -16\,(x^2 + 3\,x + 4) = E_2 + 16\,(4\,x - 7)\,E_3 =\\
&= 16\left(x^2 - 3\right) E_0 - 16\left(x^4 - 2\,x^3 + 2\,x - 2\right) E_1
\end{aligned}$$

поскольку

$$\begin{aligned}
E_5 &= E_3 + \frac{x + 2}{256}\,E_4 =\\
&= \frac{x^3 + 2\,x^2 + x + 1}{16}\,E_0 - \frac{x^5 + x^2 + 1}{16}\,E_1 = 0\,.
\end{aligned}$$

Откуда,

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

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 3.6
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 $\prod\limits_i (x - \alpha_i)$. В частности, если $f \neq 0$, то $\deg(f) \geqslant s$.

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. □

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 $\Bbbk$ — поле, и $a_0, a_1, \dots, a_n \in \Bbbk$ — любые $n + 1$ различных его элементов. Покажите, что для произвольного набора значений $b_0, b_1, \dots, b_n \in \Bbbk$ существует единственный многочлен $f(x) \in \Bbbk[x]$ степени $\leqslant n$, 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 $\leqslant n$ и больше, чем n корней. □

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

3.3.1. Общие корни нескольких многочленов. Пусть $\Bbbk$ — поле. Число α тогда и только тогда является общим корнем многочленов $f_1, f_2, \dots, f_m \in \Bbbk[x]$, 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$(f_1, f_2, \dots, f_m)$, 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 нод$(f_1, f_2, \dots, f_m)$ обычно меньше степени любого f_i.

Если многочлены $f_1, f_2, \dots, f_m \in \Bbbk[x]$ 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 $f_1 h_1 + f_2 h_2 + \dots + f_m h_m = 1$, многочлены f_i не могут одновременно обратиться в нуль ни при каком значении x.

3.3.2. Кратные корни. Пусть $\Bbbk$ — 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
Для того, чтобы $\alpha \in \Bbbk$ был кратным корнем $f \in \Bbbk[x]$ необходимо и достаточно, чтобы $f(\alpha) = f'(\alpha) = 0$.

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 $f'(\alpha) = g(\alpha) \neq 0$. □

Предложение 3.8
Если 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 $f(x) = (x-\alpha)^m \cdot g(x)$ то $f'(x) = (x-\alpha)^{m-1} \cdot \big(m \cdot g(x) + (x-\alpha) \cdot g'(x)\big)$. 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'. □

Предложение 3.9
Если char$(\Bbbk) = p > 0$, то $f' = 0$ тогда и только тогда, когда $f = g^p$ для некоторого $g \in \Bbbk[x]$.

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

Следствие 3.4
Для произвольного поля $\Bbbk$ неприводимый многочлен $f \in \Bbbk[x]$ не имеет кратных корней ни в каком кольце $K \supset \Bbbk$.

Доказательство. Согласно предл. 3.9 производная неприводимого многочлена отлична от нуля над любым полем. Поскольку f неприводим, он взаимно прост с f'. В силу n° 3.3.1 у взаимно простых многочленов нет общих корней ни в каком кольце $K \supset \Bbbk$. □

3.4. Алгебраические расширения полей. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу $\mathbb{Z}/(n)$. 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

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

Упражнение 3.12. Проверьте корректность[1] этого определения, а также выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулевым элементом кольца $\Bbbk[x]/(f)$ 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 $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$

[1] т. е. независимость классов $[g+h]$ и $[gh]$ от выбора представителей $g \in [g]$ и $h \in [h]$

гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому для классов чисел $c \in \Bbbk$ мы всюду далее пишем c вместо $[c]_f$.

Упражнение 3.13. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Так как любой многочлен $g \in \Bbbk[x]$ 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

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

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

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

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 $\Bbbk[\vartheta] : f(\vartheta) = 0$ и называют *расширением* поля $\Bbbk$ посредством *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$. Выражения (3-14) в таком контексте называются *алгебраическими числами*[1].

Например, кольцо $\mathbb{Q}[x]/(x^2-2)$ можно воспринимать как множество формальных записей вида $a + b\sqrt{2}$, где $\sqrt{2} \overset{\text{def}}{=} [x]$. 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 3.14. 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) $\vartheta^3 + 2 = 0$.

Предложение 3.10
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 $g \notin (f)$ 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 3.15. Напишите явную формулу для вычисления обратного элемента к числу $a_0 + a_1\vartheta$ в поле $\mathbb{Q}(\vartheta)$ с $\vartheta^2 + \vartheta + 1 = 0$.

[1] в классической терминологии *алгебраическим числом* называется элемент поля $\mathbb{Q}[x]/(f)$, где $f \in \mathbb{Q}[x]$ — неприводимый многочлен (см. предложение (предл. 3.10) ниже); обсуждаемая нами ситуация отличается от классической тем, что во-первых, вместо $\mathbb{Q}$ мы рассматриваем произвольное поле $\Bbbk$, а во-вторых, не требуем, чтобы соотношение на ϑ было неприводимо

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 $\mathbb{F}' \supset \Bbbk$ 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 $\mathbb{F}' = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ 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 $\mathbb{F}'$. $\square$

3.5. Поле комплексных чисел $\mathbb{C} \overset{\text{def}}{=} \mathbb{R}[t]/(t^2+1)$ 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 $i \overset{\text{def}}{=} [t]$ 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).

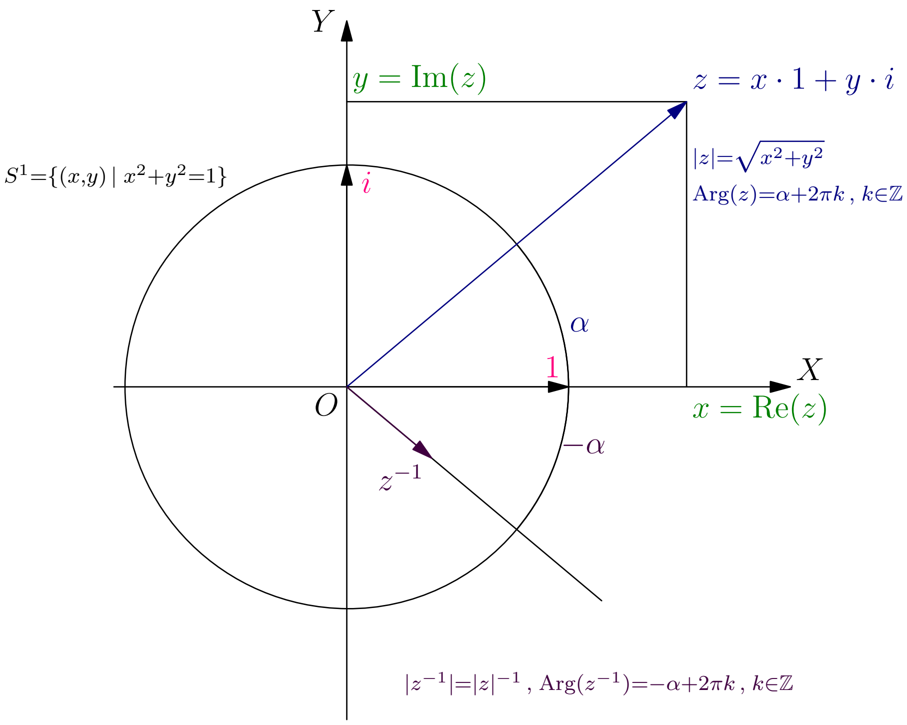

Рис. 3⋄1.

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

Координаты (x, y) называются при этом *действительной* и *мнимой* частями числа комплексного числа $z \in \mathbb{C}$ и обозначаются через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ 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 ϑ совмещает координатный луч OX с лучом, идущим в направлении радиус вектора z, называется *аргументом* числа z и обозначается

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

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

Лемма 3.1
Множество радиус-векторов точек z декартовой координатной плоскости $\mathbb{R}^2$ с операцией сложения векторов и операцией умножения, заданной правилами[2]

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

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

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

Упражнение 3.16. 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

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

(см. рис. 3◇1). Для проверки дистрибутивности заметим, что отображение $\lambda_a : z \mapsto az$ умножения на фиксированный вектор a представляет собою *поворотную гомотетию*[3] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\mathrm{Arg}\,(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b + c) = ab + ac$ означает, 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 образуют поле. Векторы, параллельные прямой OX образут в нём подполе, изоморфное полю $\mathbb{R}$. Произвольный вектор $z = (x, y)$ записывается в виде

[1]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

[2]иначе говоря, при умножении комплексных чисел их модули перемножаются, а аргументы складываются

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

$z = x + iy$, 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 $z_2 = x_2 + iy_2$

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

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

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

3.5.2. 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,

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

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.

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 $(\cos\varphi + i\sin\varphi)^n$ 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:

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

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

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

[1]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

3.5.3. 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 $n\mathrm{Arg}\,(z) = \mathrm{Arg}\,(1) = \{2\pi k \mid k \in \mathbb{Z}\}$. Поскольку

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

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

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

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[1].

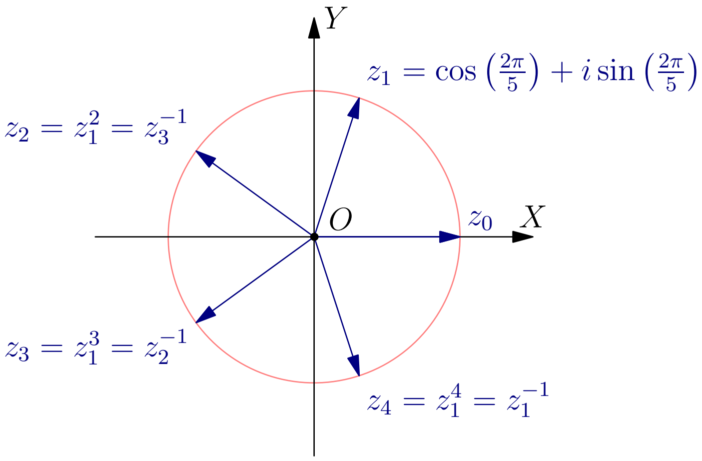

Рис. 3◇2. Корни уравнения $z^5 = 1$.

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. 43 первообразными являются только ζ_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 нод$(k, n) = 1$.

[1]фактически мы уже встречались с ней в n° 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

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

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

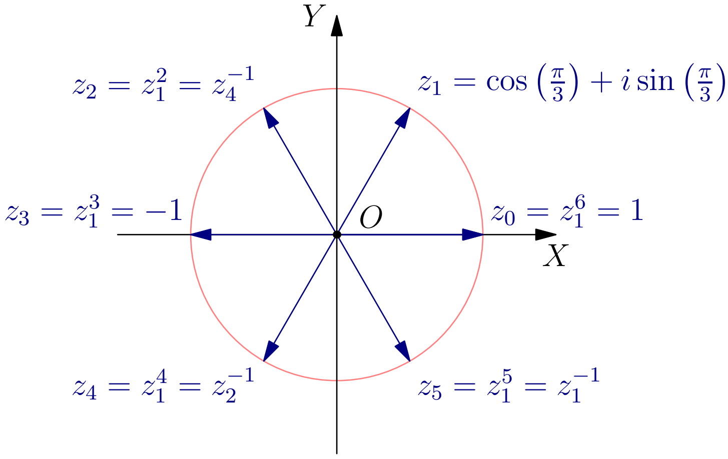

Рис. 3◇3. Корни уравнения $z^6 = 1$.

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*[1] в $\mathbb{Q}[x]$.

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 $n\varphi \in \operatorname{Arg}(a)$. 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 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

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

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 через некоторое время докажем, тождество Эйлера сводит вопрос о представимости произвольного натурального числа в виде суммы двух квадратов к анализу представимости простых чисел.

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

3.6. 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

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

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

Упражнение 3.21. Убедитесь, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

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[2]. Аналогом комплексного сопряжения, переводящего ω в $\overline{\omega} = \omega^2$, в поле $\mathbb{F}_4$ является гомоморфизм Фробениуса[3] $F_2 : \mathbb{F}_4\to\mathbb{F}_4\,,\ a\mapsto a^2$, 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 $F_3 : a\mapsto a^3$ 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 $\boldsymbol{\mu}_8$.

[1] отметим, что в силу равенства $-1 = 1$ в поле $\mathbb{F}_2$ можно обходиться без «минусов»

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

[3] см. n° 2.8.2 на стр. 28

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

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

3.6.1. 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° 3.5.3, 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 $b^0 = 1\,,\ b^1 = b\,,\ b^2\,,\ \dots\,,\ b^{n-1}$ 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 $b^m = (b^n)^q b^r = b^r$.

Предложение 3.11
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 нок(m_1, m_2).

Упражнение 3.24. 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 $m_1 = k_1\ell_1$, $m_2 = k_2\ell_2$ и 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 ℓ_1 и ℓ_2, а их произведение $b_1'b_2'$ по упр. 3.24 имеет порядок $\ell_1\ell_2 =$ нок(m_1, m_2), что и требовалось. □

Теорема 3.3
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 3.2.

Доказательство. Если $\operatorname{char}\mathbb{F} = p$, 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. 3.11 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 сюрьективный гомоморфизм колец $\mathrm{ev}_\zeta : \mathbb{F}_p[x]/(g) \twoheadrightarrow \mathbb{F}$.

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 ev_ζ инъективен и $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$.

С другой стороны, поскольку ζ 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 $\mathrm{ev}_\xi : \mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюрьективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

3.6.2. 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 $\mathbb{F}_p^* \to \mathbb{F}_p^*$ 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[1], 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

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

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

[1]см. сл. 2.1 на стр. 22

$x^2 = 1$, он состоит в точности из двух элементов ± 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

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

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 3.27*. 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, впервые доказанной Гауссом.

Теорема 3.4 (квадратичный закон взаимности)
Для любых простых $p, q > 2$

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

□

Два доказательства этой теоремы, предложенные Эйзенштейном и Золотарёвым, намечены в задачах из необязательного листка № $3\frac{1}{2}$. 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.

Ответы и указания к некоторым упражнениям

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

Упр. 3.5. 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. 3.7. 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

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

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 λ — 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_ν кроме i-той, есть $\prod\limits_{\nu \neq i}(x - a_\nu)$. Деля этот многочлен на его значение в точке a_i, получаем многочлен $f_i(x) = \prod\limits_{\nu \neq i}(x - a_\nu) / \prod\limits_{\nu \neq i}(a_i - a_\nu)$, такой что

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

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

Упр. 3.12. См. упр. 1.9 на стр. 10.

Упр. 3.13. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x - \alpha)$ в качестве констант сюрьективно, 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. 3.14. 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 $h_1 g + h_2 p = 1$; 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. n° 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 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. 3.19. См. листок № $3\frac{2}{3}$.

Упр. 3.20. 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. 3.23. Это сразу следует из теоремы 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 $e_1, e_2, \dots, e_n$, заключаем, что $\mathbb{F}$ состоит из p^n векторов $x_1e_1 + x_2e_2 + \dots + x_ne_n$, где каждый коэффициент x_i независимо пробегает $\mathbb{F}_p$.

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

Упр. 3.25. Надо отправить в ℓ_1 все простые делители числа m_1, входящие в разложение числа m_1 в бо́льшей 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[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*