Б. М. Верников, Д. В. Скоков

МНОГОЧЛЕНЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Учебное пособие

Екатеринбург

В пособии излагается одна из стандартных тем университетского курса алгебры — теория многочленов от одной переменной. Приводятся примеры решения типовых задач, имеется подборка задач для самостоятельного решения.

Для студентов и преподавателей математических и компьютерно-информационных направлений подготовки и специальностей.

Оглавление

Предисловие

Данное пособие предназначено для студентов первого курса бакалавриата и специалитета, обучающихся по математическим и компьютерно-информационным направлениям подготовки и специальностям. В пособии излагается одна из стандартных тем университетского курса алгебры — теория многочленов от одной переменной.

Пособие содержит четыре главы. В главе I собрана необходимая для дальнейшего информация из других разделов алгебры. Глава II посвящена первоначальным сведениям о многочленах и теории делимости многочленов, глава III — исследованию корней многочленов, а глава IV — разложению многочленов на неприводимые множители. Кроме того, в главе III затрагивается вопрос об аппроксимации функций многочленами, а в главе IV изучаются рациональные дроби. Главы II–IV завершаются примерами решения типовых задач. После главы IV приводится раздел «Задачи для самостоятельного решения», в котором, помимо самих задач, имеются ответы и указания к ним. Заканчивается пособие списком литературы, списком обозначений и предметным указателем.

Главы делятся на параграфы, имеющие сквозную нумерацию. Утверждения, алгоритмы, примеры, формулы, рисунки и таблицы нумеруются двумя числами, первое из которых — это номер параграфа, в котором они приводятся. При этом утверждения всех типов, алгоритмы и примеры нумеруются совместно. Задачи в разделах «Решение типовых задач» в главах II–IV также нумеруются двумя числами, первое из которых на этот раз означает номер соответствующей главы. Символом $\square$ обозначается конец или отсутствие доказательства утверждения или обоснования алгоритма.

Авторы благодарны С. В. Гусеву и А. Я. Овсянникову, которые прочли рукопись пособия и сделали ряд ценных замечаний, способствовавших ее существенному улучшению, а также М. В. Волкову и А. Г. Гейну за полезные советы.

Глава I

Начальные сведения об алгебрах некоторых типов и комплексных числах

Данная глава является вспомогательной и содержит первоначальную информацию об универсальных алгебрах некоторых типов (группах, кольцах и полях) и о комплексных числах. Мы не ставим себе целью систематически изложить здесь основы общей алгебры и теории комплексных чисел, а ограничиваемся исключительно теми понятиями и результатами, которые необходимы для понимания основного материала пособия.

§ 1. Группы, кольца, поля

Пусть S — непустое множество. Множество всевозможных упорядоченных пар элементов из S называется *декартовым квадратом* множества S и обозначается через S^2. *Бинарной операцией* на S называется произвольное отображение из S^2 в S. Никакие операции, кроме бинарных, в данном пособии появляться не будут, поэтому

мы часто будем называть бинарные операции просто *операциями*. В общем случае мы будем записывать бинарную операцию на некотором множестве в виде $f(x,y)$. Множество S с заданной на нем бинарной операцией f будем обозначать через $\langle S; f\rangle$. Часто бинарную операцию называют *умножением* и обозначают так же, как умножение чисел: точкой или отсутствием символа, т. е. $x \cdot y$ или xy.

Бинарная операция f, заданная на множестве S, называется *ассоциативной*, если $f\big(f(x,y),z\big) = f\big(x,f(y,z)\big)$ для любых $x,y,z \in S$. Если писать xy вместо $f(x,y)$, то ассоциативность операции означает, что $(xy)z = x(yz)$ для любых $x,y,z \in S$. Если операция ассоциативна, то в записях вида $x_1x_2\cdots x_n$ скобки можно не ставить, так как результат операции от их расстановки не зависит.

Пусть S — множество, на котором задана бинарная операция f. Элемент $e \in S$ называется *нейтральным* относительно f, если $f(x,e) = f(e,x) = x$ для любого $x \in S$. Если писать xy вместо $f(x,y)$, то нейтральность элемента e означает, что $xe = ex = x$ для любого $x \in S$. Легко проверяется, что множество с бинарной операцией не может содержать два различных нейтральных элемента.

Пусть S — множество с бинарной операцией f и нейтральным элементом e. Элемент $y \in S$ называется *обратным к элементу* $x \in S$, если $f(x,y) = f(y,x) = e$ или, в более компактной записи, $xy = yx = e$. Элемент, обратный к x, обозначается через x^{-1}. Элемент $x \in S$ называется *обратимым*, если существует элемент, обратный к x. Легко проверяется, что если элемент x множества с ассоциативной бинарной операцией и нейтральным элементом обратим, то обратный к x элемент определен однозначно. Из определения обратного элемента легко вытекают также следующие два утверждения: если элемент x обратим, то элемент x^{-1} также обратим и $(x^{-1})^{-1} = x$; если элементы x и y обратимы и бинарная операция ассоциативна, то элемент xy также обратим и $(xy)^{-1} = y^{-1}x^{-1}$.

Группой называется множество с заданной на нем ассоциативной бинарной операцией, в котором есть нейтральный элемент относительно этой операции и все элементы обратимы. Нейтральный элемент произвольной группы называется *единицей группы* и часто обозначается символом 1.

Бинарная операция f, заданная на множестве S, называется *коммутативной*, если $f(x,y) = f(y,x)$ для любых $x,y \in S$. Ес-

ли писать xy вместо $f(x,y)$, то коммутативность операции означает, что $xy = yx$ для любых $x, y \in S$. Группа G называется *абелевой*, если ее бинарная операция коммутативна (т. е. если $xy = yx$ для любых $x, y \in G$). Бинарную операцию в абелевой группе часто называют *сложением* и обозначают символом $+$. Нейтральный элемент относительно такой операции обычно называется *нулем* и обозначается символом 0, а элемент, обратный к x относительно сложения, как правило, называется *противоположным к* x и обозначается через $-x$.

Пусть f и g — бинарные операции на множестве S. Операция g называется *дистрибутивной относительно* f, если для любых $x, y, z \in S$ выполнены равенства

$$g\big(f(x,y),z\big) = f\big(g(x,z),g(y,z)\big) \text{ и } g\big(x,f(y,z)\big) = f\big(g(x,y),g(x,z)\big).$$

Если в этих равенствах писать $x+y$ вместо $f(x,y)$ и xy вместо $g(x,y)$, а также договориться о том, что, как обычно, умножение имеет приоритет перед сложением, то равенства из определения примут знакомый и привычный вид: $(x+y)z = xz+yz$ и $x(y+z) = xy+xz$.

Кольцом называется множество R, на котором заданы две бинарные операции (одну из которых мы будем называть *сложением* и обозначать через $x+y$, другую — *умножением* и обозначать через $x \cdot y$ или xy) такие, что $\langle R; + \rangle$ — абелева группа и умножение дистрибутивно относительно сложения. Нейтральный элемент кольца по сложению называется *нулем* кольца и обозначается через 0, а элемент, обратный по сложению к элементу $x \in R$, называется *противоположным* к x и обозначается через $-x$. Если умножение ассоциативно [коммутативно], то кольцо называется *ассоциативным* [соответственно *коммутативным*]. Если в кольце есть нейтральный элемент по умножению, то этот элемент называется *единицей* и обозначается (как правило) через 1, а кольцо называется *кольцом с* 1. Кольцо R с операциями сложения $+$ и умножения $\cdot$ будем обозначать через $\langle R; +, \cdot \rangle$.

Приведем примеры колец, которые будут встречаться в дальнейшем. Напомним, что буквами $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ обозначаются соответственно множества всех натуральных, целых, рациональных и действительных чисел. Ясно, что множества $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ с обычными

операциями сложения и умножения чисел являются ассоциативно-коммутативными кольцами с 1. Пусть $n \in \mathbb{N}$ и $n > 1$. Положим $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ и определим на множестве $\mathbb{Z}_n$ операции сложения $\oplus$ и умножения $\otimes$ следующим образом: если $x, y \in \mathbb{Z}_n$, то $x \oplus y$ [соответственно $x \otimes y$] — это остаток от деления числа $x + y$ [соответственно xy] на n (здесь $x + y$ и xy — обычные сумма и произведение чисел x и y). Очевидно, что $\langle \mathbb{Z}_n; \oplus, \otimes \rangle$ — ассоциативно-коммутативное кольцо с 1 (противоположным к x является число $n - x$, если $x \neq 0$, и 0, если $x = 0$). Оно называется *кольцом вычетов по модулю* n.

Легко понять, что если R — кольцо, то $x \cdot 0 = 0 \cdot x = 0$ для всякого $x \in R$. Элемент x кольца R называется *делителем нуля*, если $x \neq 0$ и существуют ненулевые элементы $y, z \in R$ такие, что $xy = 0$ и $zx = 0$. Делители нуля есть, например, в кольце $\mathbb{Z}_n$ при условии, что n — составное число: если $n = km$, где $1 < k, m < n$, то k и m — делители нуля, так как $k \otimes m = m \otimes k = 0$. Существуют кольца, в которых всякий ненулевой элемент является делителем нуля. Таковым является, например, кольцо векторов трехмерного физического пространства с операциями сложения и векторного произведения векторов (поскольку, как известно, $\vec{x} \times \vec{x} = \vec{0}$ для любого вектора $\vec{x}$). Но для дальнейшего основной интерес представляет противоположная «крайность» — кольца, не содержащие делителей нуля. Ассоциативно-коммутативное кольцо с 1, не содержащее делителей нуля, называется *областью целостности* или *целостным кольцом*. Примерами областей целостности являются кольца $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$.

Введем новое понятие, которое будет играть очень важную роль в этом пособии. *Полем* называется неодноэлементное ассоциативно-коммутативное кольцо с 1, в котором все ненулевые элементы обратимы относительно умножения. Следующее утверждение показывает, что всякое поле является областью целостности (обратное утверждение неверно: очевидным контрпримером является кольцо $\mathbb{Z}$).

Замечание 1.1. *Поле не содержит делителей нуля.*

Доказательство. Поскольку в поле все ненулевые элементы обратимы, достаточно доказать, что обратимый элемент кольца не может быть делителем нуля. В самом деле, если элемент x обратим и

$xy = 0$, то

$$y = 1 \cdot y = \bigl(x^{-1}x\bigr)y = x^{-1}(xy) = x^{-1} \cdot 0 = 0.$$

Следовательно, x не является делителем нуля. □

Примерами полей являются кольца $\mathbb{Q}$ и $\mathbb{R}$ с обычными операциями сложения и умножения. Следующее утверждение показывает, что полем является также кольцо вычетов по простому модулю.

Лемма 1.2. *Кольцо вычетов по модулю n является полем тогда и только тогда, когда n — простое число.*

Доказательство. Необходимость. Как уже отмечалось выше, кольцо $\mathbb{Z}_n$ при составном n содержит делители нуля, а в силу замечания 1.1 в поле делителей нуля нет.

Достаточность. Пусть p — простое число. Достаточно проверить, что каждый ненулевой элемент кольца $\mathbb{Z}_p$ имеет обратный элемент по умножению. Пусть $s \in \mathbb{Z}_p \setminus \{0\}$, т. е. $1 \leqslant s \leqslant p-1$. Рассмотрим числа $1 \otimes s$, $2 \otimes s$, …, $(p-1) \otimes s$. Требуется доказать, что одно из них равно 1. Пусть $k \in \{1, 2, \ldots, p-1\}$. Очевидно, $0 \leqslant k \otimes s \leqslant p-1$. Из того что $k, s < p$, а p — простое число, вытекает, что p не$+ks$. Следовательно, $k \otimes s \neq 0$ и потому $1 \leqslant k \otimes s \leqslant p-1$. Далее, если $k \otimes s = \ell \otimes s$ для некоторых $1 \leqslant k < \ell \leqslant p-1$, то $(\ell - k) \otimes s = \ell \otimes s - k \otimes s = 0$ вопреки сказанному выше. Следовательно, все числа $1 \otimes s, 2 \otimes s, \ldots, (p-1) \otimes s$ попарно различны. Иными словами, $\{1 \otimes s, 2 \otimes s, \ldots, (p-1) \otimes s\} = \{1, 2, \ldots, p-1\}$. Следовательно, одно из чисел $1 \otimes s$, $2 \otimes s$, …, $(p-1) \otimes s$ равно 1, что и требовалось доказать. □

Если p — простое число, то поле $\mathbb{Z}_p$ называется *полем вычетов по модулю p*.

Пусть R — произвольное кольцо, $x \in R$, а n — натуральное число. Положим по определению

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ раз}}.$$

Заметим, что если $x, y \in R$, а $n \in \mathbb{N}$, то справедливо равенство

$$n(xy) = (nx)y, \tag{1.1}$$

которое пригодится нам в § 13. В самом деле,

$$n(xy) = \underbrace{xy + xy + \cdots + xy}_{n \text{ раз}} = (\underbrace{x + x + \cdots + x}_{n \text{ раз}})y = (nx)y.$$

Отметим одно существенное различие между свойствами полей $\mathbb{Q}$ и $\mathbb{R}$ с одной стороны и поля вычетов по простому модулю — с другой. Очевидно, что если F — одно из полей $\mathbb{Q}$ и $\mathbb{R}$, то не существует натурального числа n такого, что $nx = 0$ для всех $x \in F$. В то же время если p — простое число, то $px = 0$ для всякого $x \in \mathbb{Z}_p$. Это различие делает естественным следующее определение. Пусть F — произвольное поле. Если существует натуральное число n такое, что $nx = 0$ для всякого $x \in F$, то минимальное число n с таким свойством называется *характеристикой* поля F; если такого n не существует, то характеристика F по определению равна 0. Характеристика поля F обозначается через $\operatorname{char} F$. Очевидно, что $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = 0$, а $\operatorname{char}\mathbb{Z}_p = p$. Несложно проверяется, что характеристика любого поля равна либо 0, либо простому числу. Мы опускаем доказательство этого факта, поскольку в дальнейшем он нам не понадобится.

Замечание 1.3. *Пусть F — поле, а n — натуральное число. Если $na = 0$ для некоторого $a \in F \setminus \{0\}$, то $nx = 0$ для всякого $x \in F$.*

Доказательство. Обозначим единицу поля F через e. Пусть $x \in F$. Поскольку $a \neq 0$, элемент a обратим. Используя (1.1), имеем

$$nx = n(ex) = n(aa^{-1}x) = (na)(a^{-1}x) = 0 \cdot a^{-1}x = 0.$$

Замечание доказано. □

Непустое подмножество A кольца R называется *подкольцом* кольца R, если для любых двух элементов $x, y \in A$ имеют место включения $x+y \in A$ и $xy \in A$. Иллюстрацией к этому определению служит рис. 1.1, на котором, как и на рис. 1.2, пунктирные линии обозначают сложение, а штрихпунктирные — умножение. В качестве примеров отметим, что кольцо $\mathbb{Z}$ является подкольцом кольца $\mathbb{Q}$, а кольцо $\mathbb{Q}$ — подкольцом кольца $\mathbb{R}$.

Говорят, что кольцо A *изоморфно вложимо* или просто *вложимо* в кольцо B, если существует взаимно однозначное отображение

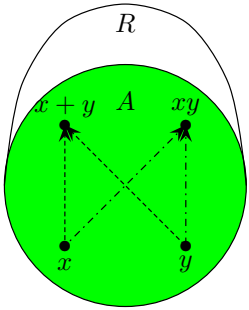

Рис. 1.1. Подкольцо

φ из A в B такое, что $\varphi(x+y) = \varphi(x) + \varphi(y)$ и $\varphi(xy) = \varphi(x) \cdot \varphi(y)$. Иллюстрацией к этому определению служит рис. 1.2. Отображение φ называется при этом *изоморфным вложением* или просто *вложением* A в B. Примером вложения является отображение φ из $\mathbb{Z}$ в $\mathbb{Q}$, задаваемое правилом: $\varphi(n) = \frac{n}{1}$ для всякого $n \in \mathbb{N}$.

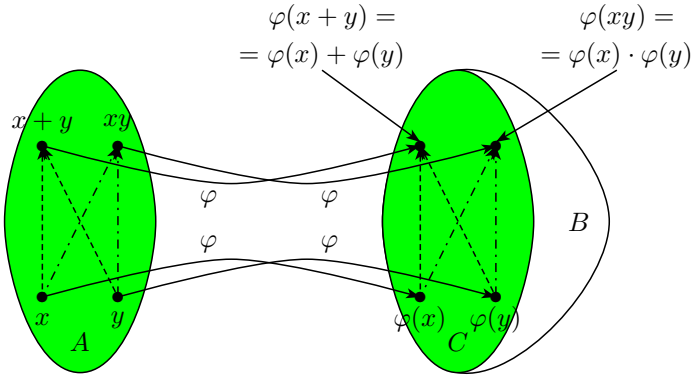

Рис. 1.2. Вложение A в B

Если изоморфное вложение φ из A в B *сюръективно* (т. е. для любого $y \in B$ существует $x \in A$ такой, что $f(x) = y$), то оно называется *изоморфизмом*, а кольца A и B называются *изоморфны-*

ми. Если φ — вложение из A в B, то множество $C = \{\varphi(x) \mid x \in \in A\}$ образует подкольцо в B, изоморфное A. Говоря неформально, изоморфность колец A и B означает, что эти кольца идентичны по своим алгебраическим свойствам: их элементы складываются и перемножаются по одним и тем же правилам, но под «разными именами» (если φ — изоморфизм из A на B, то элемент $x \in A$ «действует» в B «под именем» $\varphi(x)$). Поэтому изоморфные кольца часто отождествляют и считают одним и тем же кольцом (или двумя «реализациями» одного и того же кольца).

§ 2. Комплексные числа

Комплексным числом называется упорядоченная пара (a, b) действительных чисел a и b. *Суммой* комплексных чисел (a, b) и (c, d) называется число $(a + c, b + d)$, а их *произведением* — число $(ac - bd, ad + bc)$. Множество всех комплексных чисел обозначается через $\mathbb{C}$.

Тот факт, что некие «новые» числа вводятся как пары «старых», не должен удивлять. Ведь и рациональное число $\frac{m}{n}$ при желании можно определить как упорядоченную пару целых чисел (m, n). На языке пар можно определить и операции над рациональными числами:

$$(m, n) + (k, \ell) = (m\ell + kn, n\ell) \quad \text{и} \quad (m, n) \cdot (k, \ell) = (mk, n\ell).$$

Но действовать с рациональными числами в таком виде неудобно, поэтому лучше перейти к традиционной их записи в виде дроби. Для комплексных чисел также существует более удобный способ их записи, называемый алгебраической формой комплексных чисел, к которому мы перейдем чуть ниже.

Легко проверяется, что множество $\mathbb{C}$ с операциями сложения и умножения является ассоциативно-коммутативным кольцом с 1; роль нейтрального элемента по умножению играет число $(1, 0)$.

Определим отображение φ из $\mathbb{R}$ в $\mathbb{C}$ правилом: $\varphi(a) = (a, 0)$ для всякого $a \in \mathbb{R}$. Легко понять, что это отображение является изоморфным вложением $\mathbb{R}$ в $\mathbb{C}$. Это позволяет нам отождествить комплексное число $(a, 0)$ с действительным числом a и считать, что

$\mathbb{R} \subseteq \mathbb{C}$. Отметим, что аналогичным образом мы отождествляем рациональное число $\frac{n}{1}$ с целым числом n, и именно это позволяет нам считать, что $\mathbb{Z} \subseteq \mathbb{Q}$.

Комплексное число $(0,1)$ называется *мнимой единицей* и обозначается через i. По определению умножения комплексных чисел $i^2 = (0,1)\cdot(0,1) = (-1,0)$. Как мы уже договорились, мы не различаем комплексное число $(-1,0)$ и действительное число -1. Таким образом, $i^2 = -1$. Мы видим, что в кольце $\mathbb{C}$ разрешимо уравнение $x^2 + 1 = 0$, неразрешимое в кольце $\mathbb{R}$.

Заметим, что

$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)\cdot(0,1) = a + bi.$$

Выражение $a+bi$ называется *алгебраической формой* комплексного числа (a,b).

Лемма 2.1. *Множество $\mathbb{C}$ с операциями сложения и умножения является полем.*

Доказательство. Как уже отмечалось выше, $\langle \mathbb{C}; +, \cdot \rangle$ — ассоциативно-коммутативное кольцо с 1. Остается проверить, что для всякого ненулевого комплексного числа существует обратное к нему число по умножению. Пусть $v = a + bi$ и $v \neq 0$, т. е. $a^2 + b^2 \neq 0$. Положим $w = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\cdot i$. Тогда

$$vw = (a+bi)\left(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\cdot i\right) = \frac{a^2+b^2}{a^2+b^2} + \frac{-ab+ab}{a^2+b^2}\cdot i = 1.$$

Учитывая еще, что $wv = vw$, получаем, что w обратно к v. □

Отметим, что $\operatorname{char}\mathbb{C} = 0$.

Если $x = a+bi$ — комплексное число, то число $a-bi$ называется *комплексно сопряженным к x* и обозначается через $\overline{x}$. Если x и y — произвольные комплексные числа, то $x = \overline{x}$ тогда и только тогда, когда $x \in \mathbb{R}$, $x + \overline{x}$ и $x\cdot\overline{x}$ — действительные числа, $\overline{x+y} = \overline{x} + \overline{y}$ и $\overline{xy} = \overline{x}\cdot\overline{y}$. Проверку этих фактов мы оставляем читателю.

Из школьного курса математики известна геометрическая интерпретация множества всех действительных чисел как множества точек числовой прямой. Обобщая это построение, рассмотрим плоскость, на которой зафиксирована прямоугольная декартова система координат. Комплексное число $a + bi$ будем изображать точкой

плоскости с координатами (a, b). Это задает взаимно однозначное соответствие между множеством всех комплексных чисел и множеством всех точек плоскости.

Пусть комплексное число $z = a + bi$ изображается на плоскости точкой M. Тогда длина отрезка OM называется *модулем* числа z. Модуль комплексного числа z обозначается через $|z|$. На рис. 2.1 $r = |z|$.

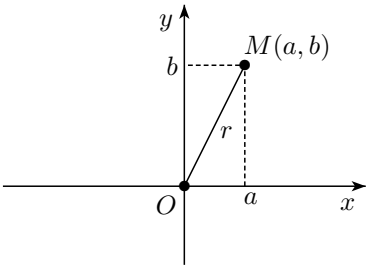

Рис. 2.1. Модуль комплексного числа

Очевидно, что если $z = a + bi$, то $|z| = \sqrt{a^2 + b^2}$. Отметим, что для действительных чисел, рассматриваемых как комплексные, введенное только что понятие модуля совпадает с понятием модуля (абсолютной величины), известным из школьного курса математики.

Лемма 2.2. *Если x и y — произвольные комплексные числа, то $|xy| = |x| \cdot |y|$ и $|x + y| \leqslant |x| + |y|$.*

Доказательство. Равенство $|xy| = |x| \cdot |y|$ проверяется непосредственными вычислениями, которые мы оставляем читателю. Чтобы доказать неравенство $|x + y| \leqslant |x| + |y|$, зафиксируем на плоскости прямоугольную декартову систему координат и обозначим через A, B и C точки на плоскости, отвечающие числам x, y и $x + y$ соответственно при геометрической интерпретации комплексных чисел. Предположим, что точки A и B не лежат на одной прямой. Этот случай проиллюстрирован на рис. 2.2. Поскольку длина стороны

треугольника меньше суммы длин двух других его сторон, имеем

$$|x+y| = |OC| < |OA| + |AC| = |OA| + |OB| = |x| + |y|.$$

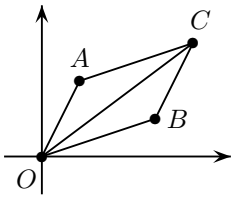

Рис. 2.2. Модуль суммы комплексных чисел

Случай же, когда точки A и B лежат на одной прямой, разбирается очень просто, и мы оставляем его читателю. Отметим только, что здесь возможно выполнение равенства $|x+y| = |x| + |y|$. □

Глава II

Многочлены как последовательности. Делимость многочленов

Эта глава содержит три параграфа. В § 3 дается определение многочленов и доказываются их простейшие свойства. Параграфы 4 и 5 посвящены соответственно вопросам, связанным с делимостью многочлена на многочлен (с остатком или без него) и с понятием наибольшего общего делителя многочленов.

§ 3. Кольцо многочленов

Изучение многочленов естественно начать с их определения. Пусть R — произвольное ассоциативно-коммутативное кольцо с 1. *Многочленом* над кольцом R называется произвольная бесконечная последовательность вида

$$(\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$$

такая, что все элементы этой последовательности принадлежат R и существует число $m \in \mathbb{N} \cup \{0\}$ такое, что $\alpha_n = 0$ для всех $n \geqslant m$. Множество всех многочленов над кольцом R обозначается

через $R[x]$. Определим сумму и произведение последовательностей из $R[x]$ следующим образом: если $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ и $g = (\beta_0, \beta_1, \dots, \beta_n, \dots)$, то $f+g = (\gamma_0, \gamma_1, \dots, \gamma_n, \dots)$ и $fg = (\delta_0, \delta_1, \dots, \delta_n, \dots)$, где $\gamma_k = \alpha_k + \beta_k$ и $\delta_k = \sum_{i=0}^{k} \alpha_i \beta_{k-i}$ для всякого $k \in \mathbb{N} \cup \{0\}$. Последовательность из $R[x]$, все элементы которой равны 0, обозначается через o и называется *нулевым* многочленом.

Как мы увидим ниже, многочлены в смысле данного только что определения суть то же самое, что многочлены от одной переменной в привычном смысле этого слова. Разница состоит только в том, что коэффициенты у них могут лежать не в поле $\mathbb{R}$, а в произвольном ассоциативно-коммутативном кольце R с 1. Отметим еще, что *мы часто для краткости будем опускать упоминание о том, что кольцо R ассоциативно-коммутативно и содержит* 1.

Докажем некоторые простейшие свойства многочленов.

Замечание 3.1. *Сумма и произведение многочленов над кольцом R являются многочленами над R.*

Доказательство. Пусть $f, g \in R[x]$, причем

$$f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots) \text{ и } g = (\beta_0, \beta_1, \dots, \beta_n, \dots).$$

Существуют такие числа q и r, что $\alpha_n = 0$ для всех $n \geqslant q$ и $\beta_n = 0$ для всех $n \geqslant r$. Положим $f + g = (\gamma_0, \gamma_1, \dots, \gamma_n, \dots)$ и $fg = (\delta_0, \delta_1, \dots, \delta_n, \dots)$. Тогда, очевидно, $\gamma_n = 0$ для всех $n \geqslant \max\{q, r\}$ и $\delta_n = 0$ для всех $n \geqslant q + r$. Следовательно, $f + g, fg \in R[x]$. □

Лемма 3.2. *Множество всех многочленов над кольцом R относительно операций сложения и умножения многочленов является ассоциативно-коммутативным кольцом с* 1.

Доказательство. В силу замечания 3.1 сложение и умножение многочленов над кольцом R являются бинарными операциями на множестве $R[x]$. Поскольку $\langle R; + \rangle$ — абелева группа, из определения суммы многочленов вытекает, что $\langle R[x]; + \rangle$ также является абелевой группой (нейтральным элементом этой группы является нулевой многочлен). Из определения произведения многочленов непосредственно следует, что умножение многочленов коммутативно, а многочлен $(1, 0, \dots, 0, \dots)$ является нейтральным элементом

по умножению. Проверим ассоциативность умножения. Пусть $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$, $g = (\beta_0, \beta_1, \dots, \beta_n, \dots)$ и $h = (\gamma_0, \gamma_1, \dots, \gamma_n, \dots)$. Тогда $fg = (\delta_0, \delta_1, \dots, \delta_n, \dots)$ и $gh = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_n, \dots)$, где

$$\delta_m = \sum_{k+\ell=m} \alpha_k \beta_\ell \quad \text{и} \quad \varepsilon_r = \sum_{s+t=r} \beta_s \gamma_t.$$

Следовательно, $(fg)h = (\mu_0, \mu_1, \dots, \mu_n, \dots)$, где

$$\mu_d = \sum_{m+t=d} \delta_m \gamma_t = \sum_{m+t=d} \left(\sum_{k+\ell=m} \alpha_k \beta_\ell \right) \gamma_t = \sum_{k+\ell+t=d} \alpha_k \beta_\ell \gamma_t.$$

Аналогично $f(gh) = (\nu_0, \nu_1, \dots, \nu_n, \dots)$, где

$$\nu_d = \sum_{k+r=d} \alpha_k \varepsilon_r = \sum_{k+r=d} \alpha_k \left(\sum_{s+t=r} \beta_s \gamma_t \right) = \sum_{k+s+t=d} \alpha_k \beta_s \gamma_t.$$

Сравнивая полученные выражения для μ_d и ν_d, получаем требуемое равенство $f(gh) = (fg)h$.

Осталось проверить дистрибутивность умножения относительно сложения. В силу коммутативности умножения достаточно доказать равенство $(f + g)h = fh + gh$. Ясно, что

$$(f + g)h = (\rho_0, \rho_1, \dots, \rho_n, \dots), \text{ где } \rho_d = \sum_{k+\ell=d} (\alpha_k + \beta_k) \gamma_\ell.$$

С другой стороны, $fh = (\sigma_0, \sigma_1, \dots, \sigma_n, \dots)$, а $gh = (\tau_0, \tau_1, \dots, \tau_n, \dots)$, где

$$\sigma_m = \sum_{s+t=m} \alpha_s \gamma_t, \quad \text{а} \quad \tau_m = \sum_{s+t=m} \beta_s \gamma_t.$$

Следовательно, $fh + gh = (\xi_0, \xi_1, \dots, \xi_n, \dots)$, где

$$\xi_d = \sigma_d + \tau_d = \sum_{s+t=d} (\alpha_s \gamma_t + \beta_s \gamma_t) = \sum_{s+t=d} (\alpha_s + \beta_s) \gamma_t.$$

Сравнивая полученные выражения для ρ_d и ξ_d, получаем требуемое равенство $(f + g)h = fh + gh$. □

Кольцо $R[x]$ называется *кольцом многочленов над кольцом* R.

Пусть $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ — произвольный многочлен. Если $f \neq o$, то существует $m \in \mathbb{N} \cup \{0\}$ такое, что $\alpha_m \neq 0$ и $\alpha_k = 0$ для любого $k > m$. Число m называется *степенью* многочлена f. Степень нулевого многочлена по определению равна $-\infty$, причем мы будем считать, что $-\infty < m$ и $m + (-\infty) = -\infty + m = -\infty$ для любого целого m. Степень многочлена f обозначается через $\deg f$.

Следующее утверждение показывает, что кольцо R изоморфно вложимо в кольцо $R[x]$.

Лемма 3.3. *Совокупность всех многочленов из кольца $R[x]$ степени $\leqslant 0$ образует подкольцо этого кольца, изоморфное кольцу R.*

Доказательство. Многочлены степени 0 — это последовательности вида $(\alpha, 0, \dots, 0, \dots)$, где $\alpha \in R \setminus \{0\}$, и только они, а единственный многочлен степени < 0 — это нулевой многочлен. Таким образом, многочлены степени $\leqslant 0$ — это последовательности вида $(\alpha, 0, \dots, 0, \dots)$, где $\alpha \in R$, и только они. Очевидно, что для всех $\alpha, \beta \in R$ выполнены равенства

$$(\alpha, 0, \dots, 0, \dots) + (\beta, 0, \dots, 0, \dots) = (\alpha + \beta, 0, \dots, 0, \dots)$$
$$\text{и } (\alpha, 0, \dots, 0, \dots) \cdot (\beta, 0, \dots, 0, \dots) = (\alpha\beta, 0, \dots, 0, \dots).$$

Следовательно, совокупность всех многочленов из кольца $R[x]$ степени $\leqslant 0$ образует подкольцо этого кольца, а отображение $\varphi\colon R \longrightarrow R[x]$, заданное правилом

$$\varphi(\alpha) = (\alpha, 0, \dots, 0, \dots),$$

является изоморфизмом из R на это подкольцо. □

Перейдем к привычной записи многочленов. Обозначим последовательность $(0, 1, 0, \dots, 0, \dots)$ через x. По индукции положим $x^m = x^{m-1}x$ для всякого натурального $m > 1$. С помощью индукции по m легко проверить, что

$$x^m = (\underbrace{0, 0, \dots, 0}_{m \text{ чисел}}, 1, 0, \dots, 0, \dots).$$

Отсюда вытекает, что

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0 = (\alpha_0, \alpha_1, \dots, \alpha_n, 0, \dots, 0, \dots)$$

для любых $\alpha_0, \alpha_1, \ldots, \alpha_n \in R$. Это позволяет нам всюду в дальнейшем вместо исходной записи многочлена в виде

$$(\alpha_0, \alpha_1, \ldots, \alpha_n, 0, \ldots, 0, \ldots)$$

использовать его более привычную запись:

$$f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0. \tag{3.1}$$

В дальнейшем, при рассмотрении многочленов над некоторым кольцом R, мы иногда будем называть R *кольцом скаляров*, а элементы этого кольца — *скалярами*. Скаляры α_0, α_1, ..., α_n называются *коэффициентами* многочлена (3.1). Если f имеет вид (3.1) и $\alpha_n \neq 0$, то $\deg f = n$, одночлен $\alpha_n x^n$ называется *старшим членом* многочлена f и обозначается через $\ell m(f)$, скаляр α_n называется *старшим коэффициентом* многочлена f и обозначается через $\ell c(f)$, а скаляр α_0 называется *свободным членом* многочлена f.

Всюду далее в этом пособии, кроме тех случаев, когда явно оговорено противное, предполагается, что кольцо скаляров является областью целостности. Более того, почти все основные результаты, которые будут доказаны в этом пособии, относятся к многочленам над полем.

Следующее утверждение показывает, как связаны степени суммы и произведения многочленов со степенями самих этих многочленов. В дальнейшем мы часто будем пользоваться данной леммой, как правило, не оговаривая этого в явном виде.

Лемма 3.4. *Пусть f и g — многочлены над кольцом R. Тогда:*

1) *если R — область целостности, то* $\deg(fg) = \deg f + \deg g$;
2) *если* $\deg f \neq \deg g$, *то* $\deg(f+g) = \max\{\deg f, \deg g\}$;
3) *если* $\deg f = \deg g$, *то* $\deg(f+g) \leqslant \deg f$.

Доказательство. Пусть $\ell m(f) = ax^n$, а $\ell m(g) = bx^m$. В частности, $a, b \neq 0$.

1) Очевидно, что в многочлене fg все коэффициенты при x^k, где $k > n+m$, равны 0, а коэффициент при x^{n+m} равен ab. Поскольку R не содержит делителей нуля, $ab \neq 0$. Следовательно, $\deg(fg) = n+m = \deg f + \deg g$.

2) Положим $r = \max\{n, m\}$. Очевидно, что в многочлене $f + g$ все коэффициенты при x^k, где $k > r$, равны 0, а коэффициент при x^r равен либо a, либо b. В частности, последний коэффициент отличен от 0. Следовательно, $\deg(f + g) = r = \max\{\deg f, \deg g\}$.

3) Очевидно, что в данном случае в многочлене $f + g$ все коэффициенты при x^k, где $k > n$, равны 0. Отсюда вытекает требуемое заключение. □

Отметим, что если $\deg f = \deg g = n$, то $\deg(f + g) < \deg f$ тогда и только тогда, когда $\ell c(f) = -\ell c(g)$ (так как в этом и только этом случае коэффициент при x^n в $f + g$ равен 0).

Следующее несложно проверяемое утверждение показывает, какие многочлены обратимы (относительно умножения) в кольце многочленов над полем. Эта информация будет полезна в дальнейшем.

Лемма 3.5. *Многочлен f над полем F обратим (относительно умножения) в кольце $F[x]$ тогда и только тогда, когда* $\deg f = 0$.

Доказательство. Необходимость. Предположим, что f обратим. Тогда $fg = 1$ для некоторого $g \in F[x]$. В силу п. 1) леммы 3.4 $\deg f + \deg g = \deg(fg) = \deg 1 = 0$, откуда $\deg f \leqslant 0$. Если $\deg f < 0$, то $f = o$. Но нулевой многочлен очевидным образом необратим. Следовательно, $\deg f = 0$.

Достаточность. Если $\deg f = 0$, то $f \in F \setminus \{0\}$. Учитывая, что F — поле, получаем, что многочлен f обратим. □

§ 4. Деление многочлена на многочлен с остатком

В арифметике важную роль играет тот факт, что числа можно делить друг на друга с остатком. Докажем, что то же самое можно делать и с многочленами.

Теорема 4.1. *Пусть F — поле и $f, g \in F[x]$, причем $g \neq o$. Тогда существуют однозначно определенные многочлены $q, r \in F[x]$ такие, что*

$$f = qg + r \ \text{ и } \ \deg r < \deg g. \tag{4.1}$$

Доказательство. Существование. По условию $\deg g \geqslant 0$. Если $\deg g = 0$, то $g \in F$. При этом $g \neq 0$. Следовательно, существует многочлен g^{-1}. Имеем $f = f \cdot 1 = f(g^{-1}g) = (fg^{-1})g$, и соотношения (4.1) выполнены при $q = fg^{-1}$ и $r = o$.

Предположим теперь, что $\deg g > 0$. При $\deg f < \deg g$ достаточно положить $q = o$ и $r = f$. Пусть теперь $\deg f \geqslant \deg g$, $\deg f = k$, $\deg g = m$, $\ell c(f) = \alpha$ и $\ell c(g) = \beta$. В частности, $k \geqslant m$. Положим $q_1 = \frac{\alpha}{\beta}x^{k-m}$ и $r_1 = f - q_1 g$. Тогда $\ell m(q_1 g) = \alpha x^k = \ell m(f)$ и потому $\deg r_1 < \deg f$. Итак, существуют многочлены q_1 и r_1 такие, что $f = q_1 g + r_1$ и $\deg r_1 < \deg f$. Если $\deg r_1 < \deg g$, то требуемое утверждение выполнено при $q = q_1$ и $r = r_1$.

Пусть теперь $\deg r_1 \geqslant \deg g$. Тогда можно подобрать такой одночлен q_2, что $\ell m(q_2 g) = \ell m(r_1)$. Положим $r_2 = r_1 - q_2 g$. Тогда $\deg r_2 < \deg r_1$, $r_1 = q_2 g + r_2$ и

$$f = q_1 g + r_1 = q_1 g + q_2 g + r_2 = (q_1 + q_2)g + r_2.$$

Если $\deg r_2 < \deg g$, то соотношения (4.1) выполнены при $q = q_1 + q_2$ и $r = r_2$.

Если $\deg r_2 \geqslant \deg g$, продолжим описанный процесс. На каждом шаге будут строиться одночлен q_k и многочлен r_k такие, что $\deg r_k < \deg r_{k-1}$ и $f = (q_1 + q_2 + \cdots + q_k)g + r_k$. Поскольку $\deg r_1 > \deg r_2 > \cdots$, при некотором k будет выполнено неравенство $\deg r_k < \deg g$. Тогда соотношения (4.1) выполнены при $q = q_1 + q_2 + \cdots + q_k$ и $r = r_k$.

Единственность. Предположим, что $f = q_1 g + r_1$ и $f = q_2 g + r_2$ для некоторых многочленов q_1, q_2, r_1 и r_2 таких, что $\deg r_1, \deg r_2 < \deg g$. Из равенства $q_1 g + r_1 = q_2 g + r_2$ получаем, что $(q_1 - q_2)g = r_2 - r_1$. Но если $q_1 - q_2 \neq o$, то это невозможно, так как $\deg\big((q_1 - q_2)g\big) \geqslant \deg g$, а $\deg(r_2 - r_1) < \deg g$. Следовательно, $q_1 - q_2 = o$, откуда $q_1 = q_2$. Но тогда $r_2 - r_1 = o \cdot g = o$, и, значит, $r_1 = r_2$. □

Если выполнены соотношения (4.1), то многочлен q называется *частным*, а многочлен r — *остатком* от деления f на g (с остатком).

Если $f = qg$, то говорят, что многочлен f *делится* на многочлен g, или что g *делит* f; этот факт будет обозначаться через

$g \mid f$. В дальнейшем мы многократно будем использовать следующие два простых свойства отношения делимости многочленов, не всегда упоминая их в явном виде.

Замечание 4.2. *Пусть f, g, g_1, g_2 и h — многочлены над произвольным ассоциативно-коммутативным кольцом R с 1. Тогда:*

1) *если $f \mid g$, то $f \mid gh$;*
2) *если $f \mid g_1$ и $f \mid g_2$, то $f \mid (g_1 + g_2)$.*

Доказательство. 1) По условию $g = fa$ для некоторого многочлена $a \in R[x]$. Следовательно, $gh = (fa)h = f(ah)$ и потому $f \mid gh$.

2) По условию $g_1 = fa_1$ и $g_2 = fa_2$ для некоторых многочленов $a_1, a_2 \in R[x]$. Следовательно, $g_1 + g_2 = fa_1 + fa_2 = f(a_1 + a_2)$ и потому $f \mid (g_1 + g_2)$. □

Многочлены f и g из $R[x]$ называются *ассоциированными*, если $f \mid g$ и $g \mid f$. Оказывается, что ассоциированные многочлены над полем могут отличаться друг от друга только скалярным множителем. Более точно, справедлива следующая лемма.

Лемма 4.3. *Ненулевые многочлены f и g над полем F ассоциированы тогда и только тогда, когда $f = \alpha g$ для некоторого $\alpha \in \in F \setminus \{0\}$.*

Доказательство. Необходимость. Если f и g ассоциированы, то $f = \alpha g$ и $g = \beta f$ для некоторых $\alpha, \beta \in F[x]$. Следовательно, $\deg f = \deg g + \deg \alpha$ и $\deg g = \deg f + \deg \beta$, откуда $\deg f = \deg f + \deg \alpha + \deg \beta$. Следовательно, $\deg \alpha \leqslant 0$, т. е. $\alpha \in F$. Кроме того, $\alpha \neq 0$, так как в противном случае $f = \alpha g = o$.

Достаточность. Если $f = \alpha g$ и $\alpha \in F \setminus \{0\}$, то $g = \alpha^{-1} f$. Из первого равенства вытекает, что $f \mid g$, а из второго — что $g \mid f$. □

§ 5. Наибольший общий делитель многочленов

По аналогии с понятием наибольшего общего делителя целых чисел можно определить наибольший общий делитель двух многочленов. Пусть F — поле и $f, g \in F[x]$. Многочлен $h \in F[x]$ называется *наибольшим общим делителем* многочленов f и g, если $h \mid f$,

$h \mid g$ и для любого многочлена $p \in F[x]$ из того, что $p \mid f$ и $p \mid g$ следует, что $p \mid h$.

Из определения наибольшего общего делителя двух многочленов не вытекает, что он существует. Мы докажем существование наибольшего общего делителя двух многочленов над полем чуть ниже (см. теорему 5.2). А пока отметим, что если наибольший общий делитель двух многочленов существует, то он определен не однозначно, а с точностью до ассоциированности. Сформулируем это утверждение более точно.

Лемма 5.1. *Пусть f и g — многочлены над полем F и d — наибольший общий делитель f и g. Многочлен $e \in F[x]$ также является наибольшим общим делителем многочленов f и g тогда и только тогда, когда он ассоциирован с d.*

Доказательство. Необходимость. Пусть d и e — наибольшие общие делители многочленов f и g. Тогда каждый из многочленов d и e делит как f, так и g. По определению наибольшего общего делителя это означает, что многочлены d и e делят друг друга, т. е. ассоциированы.

Достаточность. Пусть d — наибольший общий делитель f и g, а многочлен e ассоциирован с d. Из того что d делит f и g, а $e \mid d$, вытекает, что e делит f и g. Далее, если h делит f и g, то $h \mid d$, а поскольку $d \mid e$, то и $h \mid e$. Следовательно, e — наибольший общий делитель f и g. □

Следующий результат не только доказывает, что наибольший общий делитель двух многочленов над полем существует, но и устанавливает, что он обладает некоторым свойством, аналог которого справедлив и для наибольшего общего делителя целых чисел.

Теорема 5.2. *Для любых ненулевых многочленов f и g над полем F существует их наибольший общий делитель d и существуют многочлены $u, v \in F[x]$ такие, что*

$$d = uf + vg. \tag{5.1}$$

Доказательство. Без ограничения общности предположим, что $\deg f \geqslant \deg g$. Применяя теорему 4.1, разделим f на g с остатком: $f = q_1 g + r_1$, где $\deg r_1 < \deg g$. Если $r_1 \neq o$, разделим g на r_1 с

остатком: $g = q_2 r_1 + r_2$, где $\deg r_2 < \deg r_1$. Если $r_2 \neq o$, разделим r_1 на r_2 с остатком: $r_1 = q_3 r_2 + r_3$, где $\deg r_3 < \deg r_2$. Будем продолжать этот процесс, деля теперь на каждом шаге предпоследний остаток на последний, при условии, что последний остаток отличен от o. Поскольку $\deg g > \deg r_1 > \deg r_2 > \cdots$, на каком-то шаге степень остатка окажется $\leqslant 0$. Если сам остаток при этом будет отличен от o, он станет равным o на следующем шаге. Таким образом, описанный выше процесс оборвется. В результате мы получим следующие равенства:

$$\begin{cases} f = q_1 g + r_1, \ r_1 \neq o, \ \deg r_1 < \deg g; \\ g = q_2 r_1 + r_2, \ r_2 \neq o, \ \deg r_2 < \deg r_1; \\ r_1 = q_3 r_2 + r_3, \ r_3 \neq o, \ \deg r_3 < \deg r_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{k-1} = q_{k+1} r_k + r_{k+1}, \ r_{k+1} \neq o, \ \deg r_{k+1} < \deg r_k; \\ r_k = q_{k+2} r_{k+1}. \end{cases} \tag{5.2}$$

Докажем, что r_{k+1} — наибольший общий делитель f и g. Поднимаясь по цепочке равенств (5.2) снизу вверх, покажем, что $r_{k+1} \mid f$ и $r_{k+1} \mid g$. Из последнего равенства получаем, что $r_{k+1} \mid r_k$, из предпоследнего в силу п. 2) замечания 4.2 — что $r_{k+1} \mid r_{k-1}$. Аналогичным образом на каждом следующем шаге, переходя к очередному равенству вида $r_s = q_{s+2} r_{s+1} + r_{s+2}$ и используя уже доказанные к этому моменту соотношения $r_{k+1} \mid r_{s+1}$ и $r_{k+1} \mid r_{s+2}$, мы получаем, что $r_{k+1} \mid r_s$. Дойдя до второго и первого равенств, получим $r_{k+1} \mid g$ и $r_{k+1} \mid f$ соответственно.

Опускаясь по цепочке равенств (5.2) сверху вниз, покажем, что если $h \mid f$ и $h \mid g$, то $h \mid r_{k+1}$. Пусть $h \mid f$ и $h \mid g$. Из первого равенства получаем, что $r_1 = f - q_1 g$ и потому в силу п. 2) замечания 4.2 $h \mid r_1$. Рассматривая следующее равенство, получаем, что $r_2 = g - q_2 r_1$, откуда в силу п. 2) замечания 4.2 $h \mid r_2$. Опускаясь по цепочке равенств (5.2) сверху вниз, получим, что $h \mid r_s$ при $s = 3, \ldots, k+1$.

Итак, $r_{k+1} \mid f$, $r_{k+1} \mid g$ и если $h \mid f$ и $h \mid g$, то $h \mid r_{k+1}$. Следовательно, r_{k+1} — наибольший общий делитель f и g.

Осталось доказать, что $r_{k+1} = uf + vg$ для некоторых многочленов u и v. Из предпоследнего равенства в системе (5.2) вытекает, что $r_{k+1} = r_{k-1} - q_{k+1} r_k$. Подставим в это равенство выражение

$r_k = r_{k-2} - q_k r_{k-1}$, полученное из предыдущего равенства системы (5.2). Получим

$$r_{k+1} = r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) = -q_{k+1} r_{k-2} + (q_{k+1} q_k + 1) r_{k-1}.$$

Итак, $r_{k+1} = u_2 r_{k-2} + v_2 r_{k-1}$ для некоторых многочленов u_2 и v_2. Подставляя в это равенство выражение $r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}$, полученное из соответствующего равенства системы (5.2), получим

$$r_{k+1} = u_2 r_{k-2} + v_2(r_{k-3} - q_{k-1} r_{k-2}) = v_2 r_{k-3} + (u_2 - v_2 q_{k-1}) r_{k-2}.$$

Следовательно, $r_{k+1} = u_3 r_{k-3} + v_3 r_{k-2}$ для некоторых многочленов u_3 и v_3. Продолжая движение снизу вверх по системе (5.2), на каждом шаге будем получать равенство $r_{k+1} = u_s r_{k-s} + v_s r_{k-s+1}$ для некоторых u_s и v_s, где $s = 4, \ldots, k-1$. При $s = k-1$ получаем $r_{k+1} = u_{k-1} r_1 + v_{k-1} r_2$. Подставляя в это равенство выражение $r_2 = g - q_2 r_1$, полученное из второго равенства системы (5.2), получаем

$$r_{k+1} = u_{k-1} r_1 + v_{k-1}(g - q_2 r_1) = v_{k-1} g + (u_{k-1} - v_{k-1} q_2) r_1,$$

т. е. $r_{k+1} = u_k g + v_k r_1$ для некоторых u_k и v_k. Подставляя в это равенство выражение $r_1 = f - q_1 g$, полученное из первого равенства системы (5.2), окончательно имеем

$$r_{k+1} = u_k g + v_k(f - q_1 g) = v_k f + (u_k - v_k q_1) g,$$

т. е. $r_{k+1} = uf + vg$ для некоторых u и v. □

Правая часть равенства (5.1) называется *линейной формой* наибольшего общего делителя.

В доказательстве теоремы 5.2 содержится алгоритм построения наибольшего общего делителя двух многочленов, который называется *алгоритмом Евклида*. Сформулируем его в явном виде.

Алгоритм 5.3 (алгоритм Евклида)**.** Даны ненулевые многочлены f и g над полем такие, что $\deg f \geqslant \deg g$. Требуется найти наибольший общий делитель d многочленов f и g. Полагаем $r_{-1} = f$, $r_0 = g$ и $k = 0$. Если $r_k \neq o$, делим r_{k-1} на r_k, остаток от деления обозначаем через r_{k+1} и увеличиваем значение k на 1. Если $r_k \neq o$, повторяем указанные действия. Если $r_k = o$, полагаем $d = r_{k-1}$ и завершаем работу алгоритма. □

Поскольку $\deg r_{k+1} < \deg r_k$ для всякого k, существует k такое, что $\deg r_k \leqslant 0$. При этом если $r_k \neq o$, то $r_{k+1} = o$. Следовательно, алгоритм завершит работу через конечное число шагов.

Многочлены f и g над полем F называются *взаимно простыми*, если одним из наибольших общих делителей f и g является скаляр 1. Учитывая леммы 4.3 и 5.1, мы видим, что *если многочлены f и g над полем F взаимно просты, то любой ненулевой элемент из F является их наибольшим общим делителем.* Из теоремы 5.2 вытекает следующий факт.

Следствие 5.4. *Многочлены f и g над полем F взаимно просты тогда и только тогда, когда существуют многочлены $u, v \in F[x]$ такие, что*

$$uf + vg = 1. \tag{5.3}$$

Доказательство. Необходимость вытекает из теоремы 5.2.

Достаточность. Пусть выполнено равенство (5.3). Предположим, что h — общий делитель многочленов f и g, т. е. $f = hp$ и $g = hq$ для некоторых многочленов p и q. Тогда

$$1 = uf + vg = uph + vqh = (up + vq)h,$$

т. е. $h \mid 1$. Поскольку, очевидно, $1 \mid f$ и $1 \mid g$, получаем, что 1 — наибольший общий делитель f и g. □

Укажем некоторые свойства взаимно простых многочленов. Отметим, что все они являются аналогами свойств взаимно простых чисел.

Предложение 5.5. *Пусть f, g и h — многочлены над полем F. Тогда:*

1) *если f и g взаимно просты, $f \mid h$ и $g \mid h$, то $fg \mid h$;*
2) *если f и g взаимно просты и $f \mid gh$, то $f \mid h$;*
3) *если h взаимно прост и с f, и с g, то h взаимно прост с fg.*

Доказательство. 1) Пусть $h = fp$ и $h = gq$ для некоторых многочленов p и q. В силу следствия 5.4 существуют многочлены u и v такие, что выполняется равенство (5.3). Умножая обе части этого равенства на h, получим, что $h = huf + hvg$, откуда $h = gquf + fpvg = fg(qu + pv)$. Следовательно, $fg \mid h$.

2) По условию $gh = fp$ для некоторого многочлена p. В силу следствия 5.4 существуют многочлены u и v такие, что выполняется равенство (5.3). Следовательно, $huf + hvg = h$, откуда $h = huf + fpv = f(hu + pv)$. Следовательно, $f \mid h$.

3) В силу следствия 5.4 существуют многочлены u и v такие, что $uf + vh = 1$. Следовательно, $ufg + vhg = g$. Предположим, что многочлены h и fg не взаимно просты. Обозначим наибольший общий делитель этих многочленов через p. Используя п. 1) замечания 4.2, получаем, что, с одной стороны, p делит h, а значит, и vhg, а с другой — p делит fg, а значит, и ufg. Из п. 2) замечания 4.2 теперь вытекает, что p делит $vgh + ufg = g$. Но это противоречит взаимной простоте g и h. Следовательно, h и fg взаимно просты. □

Решение типовых задач

Основными типами задач по теме данной главы являются следующие:

1) найти частное и остаток от деления одного многочлена на другой;

2) найти наибольший общий делитель двух многочленов и его линейную форму.

Приведем примеры решения задач первого типа.

Задача II.1. Разделить многочлен $f(x) = x^5 + 2x^3 - 2x^2 + x - 2$ на многочлен $g(x) = x^3 - x^2 + 2x - 3$ с остатком.

Решение. Требуется найти многочлены $q(x)$ и $r(x)$ такие, что $f = qg + r$ и $\deg r < \deg g$. Заметим, что $\deg f \geqslant \deg g$. Поэтому, в соответствии с алгоритмом деления многочлена на многочлен с остатком, надо начать с нахождения многочлена $q_1(x)$ такого, чтобы выполнялось равенство $\ell m(f) = \ell m(q_1 g)$. Очевидно, что $q_1(x) = x^2$. После этого вычисляем многочлен $f_1 = f - q_1 g$:

$$f_1(x) = f(x) - x^2 g(x) = (x^5 + 2x^3 - 2x^2 + x - 2) - \\ - (x^5 - x^4 + 2x^3 - 3x^2) = x^4 + x^2 + x - 2.$$

Поскольку $\deg f_1 \geqslant \deg g$, находим многочлен $q_2(x)$ такой, чтобы выполнялось равенство $\ell m(f_1) = \ell m(q_2 g)$. Очевидно, что $q_2(x) = x$. Вычисляем многочлен $f_2 = f_1 - q_2 g$:

$$f_2(x) = f_1(x) - xg(x) = (x^4 + x^2 + x - 2) - (x^4 - x^3 + 2x^2 - 3x) = \\ = x^3 - x^2 + 4x - 2.$$

Поскольку $\deg f_2 \geqslant \deg g$, находим многочлен $q_3(x)$ такой, чтобы выполнялось равенство $\ell m(f_2) = \ell m(q_3 g)$. Очевидно, что $q_3(x) = 1$. Вычисляем многочлен $f_3 = f_2 - q_3 g$:

$$f_3(x) = f_2(x) - g(x) = (x^3 - x^2 + 4x - 2) - (x^3 - x^2 + 2x - 3) = \\ = 2x + 1.$$

Поскольку $\deg f_3 < \deg g$, работа алгоритма завершена. Остается выписать частное $q(x)$ и остаток $r(x)$:

$$q(x) = q_1(x) + q_2(x) + q_3(x) = x^2 + x + 1 \text{ и } r(x) = f_3(x) = 2x + 1.$$

Описанный выше процесс нахождения многочленов $q(x)$ и $r(x)$ можно оформить как деление столбиком (по аналогии с делением чисел) следующим образом:

$$\begin{array}{r|l} x^5 + 2x^3 - 2x^2 + x - 2 & x^3 - x^2 + 2x - 3 \\ \cline{2-2} \quad x^5 - x^4 + 2x^3 - 3x^2 & x^2 + x + 1 \\ \cline{1-1} \quad\; x^4 + x^2 + x \\ \quad\; x^4 - x^3 + 2x^2 - 3x \\ \cline{1-1} \quad\quad x^3 - x^2 + 4x - 2 \\ \quad\quad x^3 - x^2 + 2x - 3 \\ \cline{1-1} \quad\quad 2x + 1 \end{array}$$

Ответ. $q(x) = x^2 + x + 1$, $r(x) = 2x + 1$.

В качестве еще одного примера задачи первого типа рассмотрим задачу, в которой требуется разделить многочлен $f(x)$ на двучлен вида $x - \alpha$. В разделе «Решение типовых задач» в главе III будет указан более компактный способ записи решения таких задач (см. задачу III.3).

Задача II.2. Разделить многочлен $f(x) = x^4 - x^3 - 3x^2 + 3x - 2$ на многочлен $g(x) = x - 3$ с остатком.

Решение. Разделим $f(x)$ на $g(x)$ столбиком:

$$\begin{array}{r|l}
x^4 - x^3 - 3x^2 + 3x - 2 & x - 3 \\
\cline{2-2}
-\,(x^4 - 3x^3) & x^3 + 2x^2 + 3x + 12 \\
\cline{1-1}
2x^3 - 3x^2 & \\
-\,(2x^3 - 6x^2) & \\
\cline{1-1}
3x^2 + 3x & \\
-\,(3x^2 - 9x) & \\
\cline{1-1}
12x - 2 & \\
-\,(12x - 36) & \\
\cline{1-1}
34 &
\end{array}$$

Ответ. $q(x) = x^3 + 2x^2 + 3x + 12$, $r(x) = 34$.

В дальнейшем необходимость деления одного многочлена на другой будет многократно возникать как промежуточный шаг при решении более сложных задач. Во всех таких случаях мы будем пропускать вычисления, оставляя проверку выкладок читателю, и сразу приводить результат деления.

Перейдем к задачам второго типа.

Задача II.3. Найти наибольший общий делитель $d(x)$ многочленов $f(x) = x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$ и $g(x) = x^3 - 6x - 9$ и многочлены $u(x)$ и $v(x)$ такие, что $d = uf + vg$.

Решение. Будем решать задачу в соответствии с алгоритмом Евклида. Разделив $f(x)$ на $g(x)$ с остатком, найдем частное $q_1(x) = x^2 + x$ и остаток $r_1(x) = x^2 - 2x - 3$. Поскольку $r_1(x) \neq o$, разделим $g(x)$ на $r_1(x)$. Получим частное $q_2(x) = x + 2$ и остаток $r_2(x) = x - 3$. Поскольку $r_2(x) \neq o$, разделим $r_1(x)$ на $r_2(x)$. Получим частное $q_3(x) = x + 1$ и остаток $r_3(x) = o$. Поскольку последний остаток нулевой, работа алгоритма Евклида завершена. Наибольшим общим делителем многочленов $f(x)$ и $g(x)$ является последний ненулевой остаток. Таким образом, $d(x) = r_2(x) = x - 3$. Из равенств $f = q_1 g + r_1$ и $g = q_2 r_1 + r_2$ получаем, что

$$d = r_2 = g - q_2 r_1 = g - q_2(f - q_1 g) = -q_2 f + (1 + q_1 q_2) g.$$

Следовательно, $u(x) = -q_2(x) = -x - 2$ и

$$v(x) = 1 + q_1(x)q_2(x) = 1 + (x^2 + x)(x + 2) = x^3 + 3x^2 + 2x + 1.$$

Ответ. $d(x) = x - 3$, $u(x) = -x - 2$, $v(x) = x^3 + 3x^2 + 2x + 1$.

Отметим, что и в доказательстве теоремы 5.2, и в формулировке алгоритма Евклида предполагается, что $\deg f \geqslant \deg g$. Поэтому, если требуется найти наибольший общий делитель многочленов f и g таких, что $\deg f < \deg g$, надо «поменять ролями» f и g и начать с деления g на f.

Другой способ нахождения наибольшего общего делителя двух многочленов будет указан в разделе «Решение типовых задач» в главе IV (см. задачу IV.3).

Разновидностью задач второго типа являются задачи, в которых требуется доказать, что данные многочлены взаимно просты. Приведем пример решения такой задачи.

Задача II.4. Доказать, что многочлены $f(x) = 6x^4 - 2x^3 + 3x^2 + 5x + 2$ и $g(x) = 6x^5 - 14x^4 + 7x^3 + 5x^2 - 4x - 3$ взаимно просты и найти многочлены $u(x)$ и $v(x)$ такие, что $uf + vg = 1$.

Решение. Поскольку $\deg f < \deg g$, алгоритм Евклида начинает свою работу не с деления f на g, а с деления g на f. Разделив g на f с остатком, находим частное $q_1(x) = x - 2$ и остаток $r_1(x) = 6x^2 + 4x + 1$. Поскольку $r_1 \neq o$, разделим f на r_1. Получим частное $q_2(x) = x^2 - x + 1$ и остаток $r_2(x) = 2x + 1$. Поскольку $r_2 \neq o$, делим r_1 на r_2. Получаем частное $q_3(x) = 3x + \frac{1}{2}$ и остаток $r_3(x) = \frac{1}{2}$. Поскольку $r_3 \neq o$, делим r_2 на r_3. На этот раз получаем частное $q_4(x) = 4x + 2$ и остаток $r_4(x) = o$. Получение нулевого остатка означает, что работа алгоритма Евклида завершена. Наибольший общий делитель многочленов f и g равен последнему ненулевому остатку, т. е. $\frac{1}{2}$. Поскольку наибольший общий делитель многочленов f и g является скаляром, эти многочлены взаимно просты. Учитывая, что $g = q_1 f + r_1$, $f = q_2 r_1 + r_2$ и $r_1 = q_3 r_2 + r_3$, имеем

$$\begin{aligned} r_3 &= r_1 - q_3 r_2 = g - q_1 f - q_3(f - q_2 r_1) = \\ &= g - q_1 f - q_3\big(f - q_2(g - q_1 f)\big) = \\ &= -(q_1 + q_3 + q_1 q_2 q_3) f + (1 + q_2 q_3) g. \end{aligned}$$

Но $r_3 = \frac{1}{2}$, и потому

$$1 = 2r_3 = -2(q_1 + q_3 + q_1q_2q_3)f + 2(1 + q_2q_3)g.$$

Подсчитаем коэффициенты при f и g в правой части полученного равенства:

$$\begin{aligned} -2(q_1 + q_3 + q_1q_2q_3) &= -2x + 4 - 6x - 1 - \\ &\quad - (x-2)(x^2 - x + 1)(6x + 1) = \\ &= -8x + 3 - (x^3 - 3x^2 + 3x - 2)(6x + 1) = \\ &= -8x + 3 - 6x^4 + 17x^3 - 15x^2 + 9x + 2 = \\ &= -6x^4 + 17x^3 - 15x^2 + x + 5 \\ \text{и} \quad 2(1 + q_2q_3) &= 2 + (x^2 - x + 1)(6x + 1) = \\ &= 6x^3 - 5x^2 + 5x + 3. \end{aligned}$$

Следовательно, $1 = uf + vg$, где $u(x) = -6x^4 + 17x^3 - 15x^2 + x + 5$, а $v(x) = 6x^3 - 5x^2 + 5x + 3$.

Ответ. $u(x) = -6x^4 + 17x^3 - 15x^2 + x + 5$, $v(x) = 6x^3 - 5x^2 + 5x + 3$.

Глава III

Многочлены как функции. Корни многочленов

Многочлен $f(x)$ над кольцом R естественно рассматривать как функцию из R в R. Изучению многочленов с этой точки зрения и посвящена данная глава.

§ 6. Аппроксимация функций многочленами

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ — многочлен над кольцом R. Его можно рассматривать как отображение из кольца R в себя, сопоставляющее каждому элементу $\xi \in R$ элемент $f(\xi) \in R$, определяемый равенством

$$f(\xi) = \alpha_n \xi^n + \alpha_{n-1} \xi^{n-1} + \cdots + \alpha_1 \xi + \alpha_0.$$

Элемент $f(\xi)$ кольца R называется *значением многочлена* $f(x)$ в кольце R при $x = \xi$ (или в точке x).

В различных приложениях математики часто возникает следующая задача. Исследуется некоторая функция (отображение) $f(x)$ из поля F в себя. Известны значения функции $f(x)$ в точках x_0, x_1, ..., x_n: $f(x_0) = y_0$, $f(x_1) = y_1$, ..., $f(x_n) = y_n$. Требуется аппроксимировать (приблизить) эту функцию многочленом, т. е. найти многочлен $p(x)$ наименьшей возможной степени над полем F такой, что $p(x_0) = y_0$, $p(x_1) = y_1$, ..., $p(x_n) = y_n$. Любой многочлен с указанным свойством называется *интерполяционным многочленом Лагранжа*, соответствующим набору пар

$$(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n). \tag{6.1}$$

Следующая теорема показывает, что интерполяционный многочлен Лагранжа, соответствующий любому набору пар (6.1), существует и определен однозначно. Кроме того, она показывает, что всякий многочлен степени $\leqslant n$ над данным полем однозначно определяется своими значениями в $(n+1)$-й точке.

Теорема 6.1. *Пусть F — поле, содержащее более n элементов, $\xi_0, \xi_1, \ldots, \xi_n$ — попарно различные элементы поля F, а α_0, α_1, ..., α_n — его произвольные элементы. Тогда существует, и притом только один, многочлен $p(x)$ степени $\leqslant n$ над полем F такой, что $p(\xi_i) = \alpha_i$ для всех $i = 0, 1, \ldots, n$.*

Доказательство. Пусть $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ — произвольный многочлен над полем F. Если $p(\xi_i) = \alpha_i$ для всех $i = 0, 1, \ldots, n$, то выполнены равенства

$$\begin{cases} a_n\xi_0^n + a_{n-1}\xi_0^{n-1} + \cdots + a_0 = \alpha_0, \\ a_n\xi_1^n + a_{n-1}\xi_1^{n-1} + \cdots + a_0 = \alpha_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_n\xi_n^n + a_{n-1}\xi_n^{n-1} + \cdots + a_0 = \alpha_n. \end{cases}$$

Это означает, что набор скаляров $(a_0, a_1, \ldots, a_n)$ является решением системы линейных уравнений

$$\begin{cases} x_0 + \xi_0 x_1 + \xi_0^2 x_2 + \cdots + \xi_0^n x_n = \alpha_0, \\ x_0 + \xi_1 x_1 + \xi_1^2 x_2 + \cdots + \xi_1^n x_n = \alpha_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_0 + \xi_n x_1 + \xi_n^2 x_2 + \cdots + \xi_n^n x_n = \alpha_n. \end{cases} \tag{6.2}$$

Таким образом, доказываемое утверждение равносильно тому, что система (6.2) имеет решение и притом только одно. Эта система является крамеровской (так как число уравнений в ней равно числу неизвестных), а ее определитель имеет вид

$$\begin{vmatrix} 1 & \xi_0 & \xi_0^2 & \dots & \xi_0^n \\ 1 & \xi_1 & \xi_1^2 & \dots & \xi_1^n \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \xi_n & \xi_n^2 & \dots & \xi_n^n \end{vmatrix}.$$

Напомним, что этот определитель называется *определителем Вандермонда*, обозначается через $V(\xi_0, \xi_1, \dots, \xi_n)$ и, как доказывается в общем курсе алгебры, вычисляется по формуле

$$V(\xi_0, \xi_1, \dots, \xi_n) = \prod_{0 \leqslant i < j \leqslant n} (\xi_j - \xi_i).$$

Поскольку по условию скаляры $\xi_0, \xi_1, \dots, \xi_n$ попарно различны, получаем, что $V(\xi_0, \xi_1, \dots, \xi_n) \neq 0$. Остается сослаться на известную из общего курса алгебры теорему Крамера, которая утверждает, что если определитель крамеровской системы линейных уравнений отличен от 0, то система имеет решение, причем ровно одно. □

Из доказательства теоремы 6.1 видно, как построить интерполяционный многочлен Лагранжа, соответствующий набору пар (6.1): для того, чтобы найти его коэффициенты, достаточно решить систему (6.2). Покажем, как это сделать по-другому. Для всякого $i = 0, 1, \dots, n$ положим

$$p_i(x) = \frac{x - x_0}{x_i - x_0} \cdot \dots \cdot \frac{x - x_{i-1}}{x_i - x_{i-1}} \cdot \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdot \dots \cdot \frac{x - x_n}{x_i - x_n}. \tag{6.3}$$

Очевидно, что $\deg p_i(x) = n$, $p_i(x_i) = 1$ и $p_i(x_j) = 0$ при $j = 0, 1, \dots, n$, $j \neq i$. Далее, положим

$$p(x) = y_0 p_0(x) + y_1 p_1(x) + \dots + y_n p_n(x). \tag{6.4}$$

Тогда для всякого $i = 0, 1, \dots, n$ выполнены равенства

$$\begin{aligned} p(x_i) &= y_0 p_0(x_i) + y_1 p_1(x_i) + \dots + y_{i-1} p_{i-1}(x_i) + \\ &\quad + y_i p_i(x_i) + y_{i+1} p_{i+1}(x_i) + \dots + y_n p_n(x_i) = \\ &= y_0 \cdot 0 + y_1 \cdot 0 + \dots + y_{i-1} \cdot 0 + y_i \cdot 1 + \\ &\quad + y_{i+1} \cdot 0 + \dots + y_n \cdot 0 = y_i. \end{aligned}$$

Таким образом, $p(x)$ — интерполяционный многочлен Лагранжа, соответствующий набору пар (6.1). При этом ясно, что $\deg p(x) \leqslant \leqslant n$.

В нашем курсе интерполяционные многочлены Лагранжа будут упоминаться в § 7 и 15.

§ 7. Два понятия равенства многочленов

Всюду ранее мы, не оговаривая этого в явном виде, имели в виду, что многочлены f и g равны, если у них равны коэффициенты при x^k для всех натуральных k и равны свободные члены. Если вернуться к исходному определению многочлена как бесконечной последовательности элементов некоторого кольца, то это определение равенства многочленов можно сформулировать так: многочлены $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ и $g = (\beta_0, \beta_1, \ldots, \beta_n, \ldots)$ над одним и тем же кольцом R равны, если $\alpha_i = \beta_i$ для всех $i \geqslant 0$. В этом случае говорят, что многочлены f и g *равны как последовательности*. Во избежание недоразумений отметим, что *всюду в данном пособии знак равенства в выражениях вида $f = g$ означает, что многочлены f и g равны в указанном только что смысле.*

Если же рассматривать многочлены как функции, то можно ввести другое понятие равенства многочленов. Говорят, что многочлены f и g над одним и тем же кольцом R *равны как функции*, если $f(\xi) = g(\xi)$ для любого $\xi \in R$. Возникает естественный вопрос: эквивалентны ли два введенных понятия равенства многочленов?

Замечание 7.1. *Если многочлены f и g над одним и тем же ассоциативно-коммутативным кольцом R с 1 равны как последовательности, то они равны и как функции.*

Доказательство. По условию $f = g = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ для некоторых $\alpha_0, \alpha_1, \ldots, \alpha_n \in R$, и потому $f(\xi) = g(\xi) = \alpha_n \xi^n + \alpha_{n-1} \xi^{n-1} + \cdots + \alpha_0$ для любого $\xi \in R$. □

Но, как показывает следующий пример, обратная импликация в общем случае неверна.

Пример 7.2 (пример многочленов, равных как функции, но не равных как последовательности)**.** Очевидно, что если x — произвольный элемент поля $\mathbb{Z}_2 = \{0, 1\}$, то выполнено равенство $x^2 = x$. Следовательно, многочлены x^2 и x над полем $\mathbb{Z}_2$ равны как функции. В то же время очевидно, что они не равны как последовательности.

Аналогичный пример можно построить для многочленов над произвольным конечным полем. Но, как показывает следующее утверждение, для многочленов над бесконечным полем примеров такого рода не существует.

Предложение 7.3. *Многочлены f и g над бесконечным полем F равны как последовательности тогда и только тогда, когда они равны как функции.*

Доказательство. Необходимость вытекает из замечания 7.1.

Достаточность. Положим $n = \max\{\deg f, \deg g\}$. Поскольку поле F бесконечно, существуют попарно различные скаляры ξ_0, ξ_1, …, $\xi_n \in F$. При этом $f(\xi_i) = g(\xi_i)$ для всех $i = 0, 1, \ldots, n$, поскольку многочлены f и g равны как функции. Для всякого $i = 0, 1, \ldots, n$ положим $f(\xi_i) = g(\xi_i) = \alpha_i$. Тогда f и g — интерполяционные многочлены Лагранжа, соответствующие набору пар (ξ_0, α_0), (ξ_1, α_1), …, (ξ_n, α_n) и $\deg f, \deg g \leqslant n$. Но по теореме 6.1 существует только один многочлен с такими свойствами. Следовательно, $f = g$. □

§ 8. Корни многочленов над произвольным полем

Следующее утверждение будет часто использоваться в дальнейшем.

Теорема 8.1 (теорема Безу)**.** *Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \\ + \cdots + a_0$ — многочлен степени > 0 над полем F, $\alpha \in F$, а $q(x)$ и $r(x)$ — частное и остаток от деления многочлена $f(x)$ на $x - \alpha$ соответственно. Тогда:*

1) $r(x) = f(\alpha)$;
2) $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$, *где* $b_{n-1} = a_n$ *и* $b_k = \\ = a_{k+1} + \alpha b_{k+1}$ *для всех* $k = 0, 1, \ldots, n-2$.

Доказательство. 1) По условию $f(x) = q(x)(x-\alpha) + r(x)$, где $\deg r < \deg(x-\alpha)$. Поскольку $\deg(x-\alpha) = 1$, получаем, что $\deg r(x) \leqslant 0$, т. е. $r(x) \in F$. Таким образом, $r(x)$ — скаляр, не зависящий от x. Поэтому далее вместо $r(x)$ будем писать r. Подставив α вместо x в равенство $f(x) = q(x)(x-\alpha)+r$, имеем $f(\alpha) = q(\alpha)\cdot 0 + r$, откуда $r = f(\alpha)$.

2) Ясно, что $\deg\bigl(q(x)(x-\alpha)\bigr) \geqslant \deg(x-\alpha) = 1 > \deg r$. Учитывая лемму 3.4, имеем

$$\begin{aligned}\deg f(x) &= \deg\bigl(q(x)(x-\alpha)+r\bigr) = \deg\bigl(q(x)(x-\alpha)\bigr) = \\ &= \deg q(x) + \deg(x-\alpha) = \deg q(x) + 1,\end{aligned}$$

откуда $\deg q(x) = \deg f(x) - 1 = n-1$. Следовательно, $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0$ для некоторых $b_0, b_1, \dots, b_{n-1} \in F$. Учитывая, что $r = f(\alpha)$ в силу п. 1), имеем

$$\begin{aligned}&a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = \\ &= (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1 x + b_0)(x-\alpha) + f(\alpha) = \\ &= b_{n-1}x^n + (-\alpha b_{n-1} + b_{n-2})x^{n-1} + \dots + (-\alpha b_1 + b_0)x + \\ &\quad + \bigl(-\alpha b_0 + f(\alpha)\bigr).\end{aligned}$$

Следовательно, $b_{n-1} = a_n$, $-\alpha b_{n-1} + b_{n-2} = a_{n-1}$, …, $-\alpha b_1 + b_0 = a_1$, $-\alpha b_0 + f(\alpha) = a_0$, откуда вытекают требуемые равенства. □

Понятно, что многочлен $f(x)$ можно разделить на двучлен $x-\alpha$ «напрямую», т. е. столбиком. Но теорема Безу позволяет указать более компактный и удобный способ решения этой задачи. Этот способ известен как *схема Горнера*. Он состоит в следующем. Требуется найти частное $q(x)$ и остаток $r(x)$ от деления многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ на двучлен $x-\alpha$. Составим таблицу из двух строк. В первой строке запишем коэффициенты многочлена $f(x)$ в порядке убывания их индексов: a_n, a_{n-1}, …, a_1, a_0. В первую клетку второй строки перенесем число из первой клетки первой строки. Каждое последующее число второй строки будем вычислять путем умножения предыдущего (только что найденного) числа из второй строки на α и сложения результата с числом из первой строки, стоящим над заполняемой клеткой второй строки. Согласно теореме Безу в результате указанных действий

во всех клетках второй строки, кроме последней, слева направо будут выписаны коэффициенты многочлена $q(x)$ в порядке убывания индексов, а в ее последней клетке будет стоять скаляр, равный $r(x)$. Обычно для удобства проведения вычислений скаляр α записывают во второй строке слева от ее первого элемента.

Пусть $f(x)$ — многочлен над кольцом R. Элемент $\alpha \in R$ называется *корнем* многочлена $f(x)$, если $f(\alpha) = 0$ (другими словами, если α — корень уравнения $f(x) = 0$). Из теоремы Безу вытекает следующее важное для дальнейшего утверждение.

Следствие 8.2 (следствие из теоремы Безу). *Пусть $f(x)$ — многочлен над полем F и $\alpha \in F$. Элемент α является корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = q(x)(x - \alpha)$ для некоторого многочлена $q(x) \in F[x]$.*

Доказательство. Необходимость. В силу п. 1) теоремы Безу $f(x) = q(x)(x - \alpha) + f(\alpha)$ для некоторого многочлена $q(x)$. Если α — корень многочлена $f(x)$, то $f(\alpha) = 0$ и потому $f(x) = q(x)(x - \alpha)$. Из п. 2) теоремы Безу вытекает, что $q(x) \in F[x]$.

Достаточность. Пусть $f(x) = q(x)(x - \alpha)$. Тогда

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0.$$

Следствие доказано. □

Натуральное число k называется *кратностью* корня α многочлена $f(x)$, если $f(x) = g(x)(x - \alpha)^k$ для некоторого многочлена $g(x)$ такого, что $g(\alpha) \neq 0$. С учетом следствия из теоремы Безу это определение можно переформулировать так: *α — корень кратности k многочлена $f(x)$, если $f(x)$ делится на $(x - \alpha)^k$, но не делится на $(x-\alpha)^{k+1}$*. Корень многочлена называется *кратным*, если его кратность > 1, и *простым*, если она равна 1. Чтобы упростить рассуждения, нам будет иногда удобно рассматривать скаляр, не являющийся корнем многочлена f, как корень f *кратности* 0.

Пусть $f(x)$ — многочлен степени > 0 над полем F, а α_1, α_2, $\ldots$, α_m — его попарно различные корни в этом поле. Для всякого $i = 1, 2, \ldots, m$ обозначим через k_i кратность корня α_i. Тогда $f(x)$ делится на $(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_m)^{k_m}$, и потому $k_1 + k_2 + \cdots + k_m \leqslant \deg f$. Учитывая еще, что число корней многочлена

не превосходит суммы их кратностей, получаем, что справедливо следующее утверждение.

Следствие 8.3. *Пусть f — многочлен степени $n > 0$ над полем F. Сумма кратностей всех корней многочлена f, а значит и число его корней, не превосходит n. В частности, число корней многочлена f конечно.* □

§ 9. Корни многочленов над полем $\mathbb{C}$

В оставшейся части главы изучаются корни многочленов над тремя основными числовыми полями: $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$. Начнем с самого большого из них — поля комплексных чисел. Здесь ключевую роль играет следующий фундаментальный факт.

Теорема 9.1 (основная теорема алгебры)**.** *Если $f(x)$ — многочлен степени > 0 над полем $\mathbb{C}$, то $f(x)$ имеет по крайней мере один комплексный корень.* □

Известно несколько доказательств этой теоремы, но все они выходят за рамки курса алгебры и используют идеи и результаты из топологии и/или теории функций комплексного переменного. Поэтому мы не будем ее доказывать. Отметим, что основная теорема алгебры — пример «чистой теоремы существования»: ни сама эта теорема, ни ее доказательство не дают никакой информации о том, как искать корни многочленов над полем $\mathbb{C}$.

Отметим еще, что свой громкий титул («основная теорема алгебры») эта теорема получила в конце XVIII в., когда она была доказана Гауссом. В то время он соответствовал действительности, поскольку решение *алгебраических уравнений*, т. е. уравнений вида $f(x) = 0$, где $f(x)$ — многочлен, рассматривалось тогда как основная задача алгебры. Сейчас это название следует воспринимать только как традиционное и историческое.

Из основной теоремы алгебры вытекает несколько важных для дальнейшего следствий. Пусть f — многочлен над полем $\mathbb{C}$ и $\deg f = n > 0$. По основной теореме алгебры многочлен f имеет некоторый корень α_1. Но тогда, по следствию из теоремы Безу,

$f(x) = (x-\alpha_1)g(x)$ для некоторого многочлена g. Ясно, что $\deg g = n-1$. Если $n-1>0$, то по основной теореме алгебры многочлен g имеет некоторый корень α_2 и потому

$$f(x) = (x-\alpha_1)g(x) = (x-\alpha_1)(x-\alpha_2)h(x)$$

для некоторого многочлена h степени $n-2$. Продолжая этот процесс, мы через n шагов представим f в виде произведения n линейных множителей и многочлена степени 0 (т. е. элемента поля $\mathbb{C}$). Иными словами,

$$\begin{aligned} f(x) &= a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = \\ &= (ax-a\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \end{aligned}$$

где $a, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Мы доказали следующее утверждение.

Следствие 9.2. *Любой многочлен степени $n>0$ над полем $\mathbb{C}$ разлагается в произведение n линейных многочленов над этим полем.* □

Из следствия 9.2 вытекает следующий факт.

Следствие 9.3. *Любой многочлен степени $n>0$ над полем $\mathbb{C}$ имеет ровно n комплексных корней, если каждый корень считать столько раз, какова его кратность.* □

Это утверждение можно переформулировать следующим образом: *сумма кратностей корней произвольного многочлена степени >0 над полем $\mathbb{C}$ равна степени этого многочлена.*

Для дальнейшего нам понадобится следующее несложное наблюдение.

Лемма 9.4 (лемма о модуле старшего члена)**.** *Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ — многочлен степени >0 над полем $\mathbb{C}$, а k — произвольное положительное действительное число. Положим $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. Если $\xi \in \mathbb{C}$ и $|\xi| \geqslant \frac{kA}{|a_n|} + 1$, то*

$$|a_n\xi^n| > k\cdot|a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0|. \tag{9.1}$$

Доказательство. Используя лемму 2.2, формулу вычисления суммы первых n членов геометрической прогрессии и неравенство $|\xi| - 1 \geqslant \frac{kA}{|a_n|}$, имеем

$$
\begin{aligned}
&|a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0| \leqslant \\
&\leqslant |a_{n-1}\xi^{n-1}| + \cdots + |a_1\xi| + |a_0| = \\
&= |a_{n-1}| \cdot |\xi|^{n-1} + \cdots + |a_1| \cdot |\xi| + |a_0| \leqslant \\
&\leqslant A\big(|\xi|^{n-1} + \cdots + |\xi| + 1\big) = \\
&= A \cdot \frac{|\xi|^n - 1}{|\xi| - 1} \leqslant A \cdot \frac{(|\xi|^n - 1) \cdot |a_n|}{kA} = \\
&= \frac{|a_n| \cdot (|\xi|^n - 1)}{k} < \frac{|a_n| \cdot |\xi|^n}{k} = \frac{|a_n\xi^n|}{k}.
\end{aligned}
$$

Таким образом, $|a_{n-1}\xi^{n-1}+\cdots+a_1\xi+a_0| < \frac{|a_n\xi^n|}{k}$. Поскольку $k > 0$, это равносильно неравенству (9.1). □

Для произвольного многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ степени > 0над полем $\mathbb{C}$ положим

$$
R_f = \frac{\max\big\{|a_0|, |a_1|, \ldots, |a_{n-1}|\big\}}{|a_n|} + 1.
$$

Предложение 9.5. *Если ξ — корень многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ степени > 0 над полем $\mathbb{C}$, то $|\xi| < R_f$.*

Доказательство. Если $\xi \in \mathbb{C}$ и $|\xi| \geqslant R_f$, то, применяя неравенство (9.1) при $k = 1$, получаем, что

$$
|a_n\xi^n| > |a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0|
$$

и потому $f(\xi) = a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0 \neq 0$. Следовательно, если ξ — корень многочлена $f(x)$, то $|\xi| < R_f$. □

В терминах геометрической интерпретации комплексных чисел (см. § 2) предложение 9.5 можно переформулировать следующим образом: корень ξ многочлена f над полем $\mathbb{C}$ располагается на комплексной плоскости внутри круга радиуса R_f с центром в начале координат. Этот факт проиллюстрирован на рис. 9.1. Окружность, ограничивающая упомянутый круг, изображена пунктирной линией, поскольку ξ не может лежать на ней.

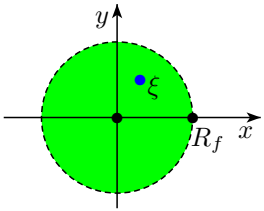

Рис. 9.1. Корень ξ многочлена f на комплексной плоскости

Отметим, что верхняя оценка модуля корня многочлена, даваемая предложением 9.5, во многих случаях является довольно грубой, т. е. сильно завышенной. Существуют значительно более точные оценки такого рода, но они выходят за рамки нашего курса.

Завершая изучение корней многочленов над полем $\mathbb{C}$, докажем следующую лемму, которая будет использоваться в дальнейшем.

Лемма 9.6. *Пусть $f(x)$ — многочлен над полем $\mathbb{C}$, все коэффициенты которого являются действительными числами, а γ — корень этого многочлена. Тогда число $\overline{\gamma}$ является корнем многочлена $f(x)$ той же кратности, что и γ.*

Доказательство. Пусть $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$. Тогда $\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0 = 0$. Используя свойства операции сопряжения комплексных чисел и тот факт, что $\overline{\alpha} = \alpha$ для всякого $\alpha \in \mathbb{R}$, имеем:

$$\begin{aligned} f(\overline{\gamma}) &= \alpha_n \overline{\gamma}^{\,n} + \alpha_{n-1} \overline{\gamma}^{\,n-1} + \cdots + \alpha_1 \overline{\gamma} + \alpha_0 = \\ &= \overline{\alpha_n} \cdot \overline{\gamma}^{\,n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma}^{\,n-1} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} = \\ &= \overline{\alpha_n} \cdot \overline{\gamma^n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma^{n-1}} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} = \\ &= \overline{\alpha_n \gamma^n} + \overline{\alpha_{n-1} \gamma^{n-1}} + \cdots + \overline{\alpha_1 \gamma} + \overline{\alpha_0} = \\ &= \overline{\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0} = \overline{0} = 0. \end{aligned}$$

Мы доказали, что $\overline{\gamma}$ — корень многочлена $f(x)$.

Осталось проверить, что γ и $\overline{\gamma}$ — корни многочлена $f(x)$ одной и той же кратности. В самом деле, предположим, что γ — корень

$f(x)$ кратности k, $\overline{\gamma}$ — корень $f(x)$ кратности m и $k \neq m$. Для определенности будем считать, что $k > m$. Положим

$$g(x) = (x - \gamma)(x - \overline{\gamma}) = x^2 - (\gamma + \overline{\gamma})x + \gamma\overline{\gamma}.$$

Поскольку $\gamma + \overline{\gamma}, \gamma\overline{\gamma} \in \mathbb{R}$ для любого $\gamma \in \mathbb{C}$, получаем, что $g(x)$ — многочлен с действительными коэффициентами. Ясно, что $g^m \mid f$. Иными словами, $f = g^m h$ для некоторого многочлена h. Как частное многочленов с действительными коэффициентами, многочлен h также имеет действительные коэффициенты. При этом ясно, что h делится на $(x - \gamma)^{k-m}$, поскольку f делится на $(x - \gamma)^k$. Следовательно, γ — корень многочлена h. В силу сказанного выше число $\overline{\gamma}$ также является корнем h. Но тогда $\overline{\gamma}$ — корень многочлена f кратности $> m$. Полученное противоречие завершает доказательство. □

§ 10. Действительные корни многочленов над полем $\mathbb{R}$

Перейдем к рассмотрению действительных корней многочленов над полем $\mathbb{R}$. Прежде всего, отметим, что аналог основной теоремы алгебры в данном случае места не имеет: действительные корни есть не у всех многочленов из $\mathbb{R}[x]$. Очевидным примером, подтверждающим это, является многочлен $x^2 + 1$. Заметим, что он имеет четную степень. Это не случайно, поскольку справедливо следующее утверждение.

Предложение 10.1. *Любой многочлен нечетной степени над полем $\mathbb{R}$ имеет по крайней мере один действительный корень.*

Доказательство. Мы приведем два принципиально различных доказательства этого утверждения. Первое из них опирается на факты из математического анализа, второе является чисто алгебраическим.

Аналитическое доказательство. Как известно из математического анализа, многочлены над $\mathbb{R}$ являются непрерывными функциями из $\mathbb{R}$ в $\mathbb{R}$. Это позволяет нам в дальнейшем использовать

следующую теорему Больцано–Коши: если функция g из $\mathbb{R}$ в $\mathbb{R}$ непрерывна на отрезке $[c, d]$ и числа $g(c)$ и $g(d)$ имеют разные знаки, то $g(\xi) = 0$ для некоторого $\xi \in (c, d)$ (иллюстрацией к этому утверждению служит рис. 10.1).

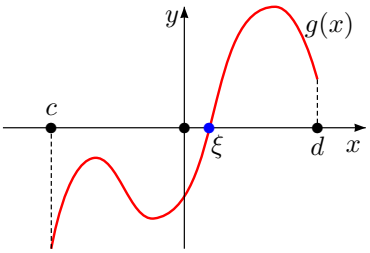

Рис. 10.1. Корень ξ на отрезке $[c, d]$

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ — многочлен нечетной степени над полем $\mathbb{R}$. Можно считать, что $a_n > 0$, так как в противном случае можно умножить $f(x)$ на -1 (понятно, что при этом корни многочлена не изменятся). Пусть c и d — действительные числа такие, что $c < -R_f$ и $d > R_f$. Применяя неравенство (9.1) при $k = 1$, получаем, что $f(c) \neq 0$ и знак числа $f(c)$ совпадает со знаком числа $a_n c^n$. Учитывая, что $a_n > 0$, $c < 0$, а число n нечетно, получаем, что $f(c) < 0$. Аналогично проверяется справедливость неравенства $f(d) > 0$. Из упомянутой в предыдущем абзаце теоремы Больцано–Коши вытекает, что $f(\xi) = 0$ для некоторого $\xi \in (c, d)$. □

Алгебраическое доказательство. Пусть f — многочлен над полем $\mathbb{R}$. В силу следствия 9.3 степень многочлена f равна числу его корней, подсчитываемых с учетом их кратностей. А из леммы 9.6 вытекает, что корни, не являющиеся действительными числами, можно разбить на пары комплексно сопряженных друг к другу чисел, и потому число таких корней четно. Следовательно, если степень многочлена f нечетна, то среди его корней должны быть действительные числа. □

Возникает естественный вопрос о том, как искать действительные корни уравнений вида $f(x) = 0$, где $f(x) \in \mathbb{R}[x]$. Если $\deg f = 1$,

то ответ на него очевиден: уравнение $ax + b = 0$, где $a \neq 0$, решается по формуле $x = -\frac{b}{a}$. Из школьного курса математики хорошо известна формула для вычисления корней квадратного уравнения, которая дает ответ на поставленный вопрос в случае, когда $\deg f = 2$. В XVI в. были найдены формулы для вычисления корней уравнений степени 3 и 4. Однако в начале XIX в. было показано, что аналогичных формул для уравнений степени $\geqslant 5$ не существует.

Таким образом, не существует способа найти все действительные корни произвольного многочлена над полем $\mathbb{R}$. Оказывается, однако, что можно получить существенную информацию о корнях многочлена $f(x) \in \mathbb{R}[x]$, не находя их. В частности, из предложения 9.5 немедленно вытекает следующий факт.

Следствие 10.2. *Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ — многочлен степени > 0 над полем $\mathbb{R}$. Если ξ — действительный корень многочлена $f(x)$, то $-R_f < \xi < R_f$.* □

Верхняя и нижняя оценки границ интервала, содержащего корни многочлена, даваемые следствием 10.2, во многих случаях являются довольно грубыми. Известны значительно более точные оценки, но они выходят за рамки нашего курса.

Кроме того, для произвольного многочлена над полем $\mathbb{R}$ можно найти число всех действительных корней этого многочлена и число его корней, принадлежащих произвольному, наперед заданному отрезку числовой прямой. Как мы увидим в конце данного параграфа, это открывает путь к приближенному вычислению действительных корней многочленов над полем $\mathbb{R}$ с любой наперед заданной степенью точности. Чтобы доказать соответствующие результаты, нам понадобятся некоторые новые понятия и вспомогательные утверждения.

Всякий многочлен над полем $\mathbb{R}$ является функцией из $\mathbb{R}$ в $\mathbb{R}$. Это позволяет рассматривать производную таких многочленов в том смысле, какой это понятие имеет в математическом анализе. Как обычно, производная многочлена f обозначается через f'. Следующая лемма будет усилена в § 13 (см. предложение 13.5).

Лемма 10.3. *Пусть f — многочлен над полем $\mathbb{R}$, а ξ — действительный корень кратности k многочлена f. Если $k = 1$, то ξ не является корнем многочлена f'. Если $k > 1$, то ξ является корнем кратности $k - 1$ многочлена f'.*

Доказательство. По условию многочлен f делится на $(x-\xi)^k$, т. е. $f=(x-\xi)^k g$ для некоторого многочлена g, но f не делится на $(x-\xi)^{k+1}$. Заметим, что g не делится на $x-\xi$, так как в противном случае f делился бы на $(x-\xi)^{k+1}$.

Если $k=1$, то $f=(x-\xi)g$. Тогда $f'=g+(x-\xi)g'$. Если ξ — корень многочлена f', то в силу следствия из теоремы Безу f' делится на $x-\xi$. Но тогда из равенства $f'=g+(x-\xi)g'$ вытекает, что g делится на $x-\xi$ вопреки сказанному выше. Итак, если $k=1$, то ξ не является корнем многочлена f'.

Пусть теперь $k>1$. Тогда

$$f'=k(x-\xi)^{k-1}g+(x-\xi)^k g'=(x-\xi)^{k-1}\bigl(kg+(x-\xi)g'\bigr).$$

Чтобы завершить доказательство, осталось убедиться в том, что многочлен $kg+(x-\xi)g'$ не делится на $x-\xi$. В самом деле, если $kg+(x-\xi)g'$ делится на $x-\xi$, то $(x-\xi)\mid kg$, т. е. $kg=(x-\xi)h$ для некоторого многочлена h. Но тогда $g=\frac{h}{k}(x-\xi)$, т. е. g делится на $x-\xi$, что вновь противоречит сказанному выше. □

Следствие 10.4. *Пусть f — произвольный многочлен степени >0 над полем $\mathbb{R}$, а d — наибольший общий делитель многочленов f и f'. Многочлены f и $g=\frac{f}{d}$ имеют одни и те же корни, причем второй из них не имеет кратных корней.*

Доказательство. Очевидно, что все корни многочлена g являются корнями многочлена f. А в силу леммы 10.3 все корни многочлена f являются простыми корнями многочлена g. □

Следуя обозначениям, принятым в математическом анализе, для всякого натурального $k\geqslant 4$ будем обозначать k-ю производную многочлена f через $f^{(k)}$. Отметим еще одно полезное следствие леммы 10.3.

Следствие 10.5. *Действительное число ξ является корнем кратности k многочлена f над полем $\mathbb{R}$ тогда и только тогда, когда оно является корнем многочленов f, f', f'', …, $f^{(k-1)}$, но не является корнем многочлена $f^{(k)}$.* □

Пусть $f(x)$ — многочлен степени >0 над полем $\mathbb{R}$. Положим $f_0=f$ и $f_1=f'$. Разделим f_0 на f_1 с остатком и обозначим через f_2

остаток от деления, умноженный на -1. Ясно, что $\deg f_2 < \deg f_1$. Если $f_2 \neq o$, разделим f_1 на f_2 с остатком и обозначим через f_3 остаток от деления, умноженный на -1. Ясно, что $\deg f_3 < \deg f_2$. Если $f_3 \neq o$, продолжим этот процесс. Поскольку $\deg f_1 > \deg f_2 > \deg f_3 > \cdots$, через конечное число шагов степень очередного остатка окажется $\leqslant 0$. Если сам остаток при этом будет отличен от o, то он станет равным o на следующем шаге. Мы получим следующую систему равенств:

$$\begin{cases} f_0 = q_1 f_1 - f_2,\ f_2 \neq o,\ \deg f_2 < \deg f_1; \\ f_1 = q_2 f_2 - f_3,\ f_3 \neq o,\ \deg f_3 < \deg f_2; \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_{m-2} = q_{m-1} f_{m-1} - f_m,\ f_m \neq o,\ \deg f_m < \deg f_{m-1}; \\ f_{m-1} = q_m f_m, \end{cases}$$

где q_i — частное от деления f_{i-1} на f_i для $i = 1, 2, \dots, m$. Упорядоченная последовательность многочленов f_0, f_1, …, f_m называется *системой многочленов Штурма* для многочлена f.

Лемма 10.6. *Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$, а f_0, f_1, …, f_m — система многочленов Штурма для многочлена f. Тогда:*

1) *f_m — наибольший общий делитель многочленов f и f';*
2) *многочлен f не имеет кратных корней тогда и только тогда, когда f_m не имеет действительных корней.*

Если f не имеет кратных корней, то, кроме того:

3) *для всякого $i = 0, 1, \dots, m-1$ многочлены f_i и f_{i+1} не имеют общих действительных корней;*
4) *если $f_k(\xi) = 0$ для некоторого $\xi \in \mathbb{R}$ и некоторого $0 < k < m$, то числа $f_{k-1}(\xi)$ и $f_{k+1}(\xi)$ отличны от 0 и имеют разные знаки.*

Доказательство. 1) Процесс построения системы многочленов Штурма очень близок к процессу нахождения наибольшего общего делителя двух многочленов по алгоритму Евклида. Отличие состоит лишь в том, что при построении системы многочленов Штурма мы на каждом шаге умножаем остаток от деления на -1. Но умножение на ненулевой скаляр никак не влияет на делимость

многочленов. Следовательно, f_m — наибольший общий делитель многочленов f и f'. Отметим, что этот факт можно доказать и непосредственно, дословно повторив соответствующую часть доказательства теоремы 5.2.

2) *Необходимость.* Если многочлен f_m имеет действительный корень ξ, то в силу следствия из теоремы Безу $(x-\xi) \mid f_m$. Поскольку в силу п. 1) f_m — наибольший общий делитель f и f', это означает, что $x-\xi$ делит и f, и f' и потому ξ является корнем обоих этих многочленов. Но тогда в силу леммы 10.3 ξ является кратным корнем многочлена f, что противоречит условию.

Достаточность. Если многочлен f имеет кратный корень ξ, то в силу леммы 10.3 ξ является корнем и многочлена f'. Тогда в силу следствия из теоремы Безу многочлен $x-\xi$ делит и f, и f'. Следовательно, $x-\xi$ делит наибольший общий делитель многочленов f и f'. В силу п. 1) это означает, что $(x-\xi) \mid f_m$. Но тогда f_m имеет действительный корень ξ вопреки условию.

3) Если многочлены $f_0 = f$ и $f_1 = f'$ имеют общий действительный корень, то в силу леммы 10.3 этот корень является кратным корнем многочлена f. Следовательно, f_0 и f_1 не имеют общих действительных корней. Из равенства $f_0 = q_1 f_1 - f_2$ вытекает, что если бы многочлены f_1 и f_2 имели общий корень, то этот корень был бы и корнем многочлена f_0. Следовательно, он был бы общим корнем многочленов f_0 и f_1, что противоречит сказанному выше. Таким образом, f_1 и f_2 общих корней не имеют. Аналогично из равенства $f_1 = q_2 f_2 - f_3$ и отсутствия общих корней у многочленов f_1 и f_2 вытекает их отсутствие у многочленов f_2 и f_3. Продолжая эти рассуждения, мы в конце концов докажем, что общие корни отсутствуют у многочленов f_i и f_{i+1} для всякого $i = 0, 1, \ldots, m-1$.

4) Если $f_k(\xi) = 0$ для некоторого $\xi \in \mathbb{R}$ и некоторого $0 < k < m$, то, полагая $x = \xi$ в равенстве $f_{k-1}(x) = q_k(x) f_k(x) - f_{k+1}(x)$, имеем $f_{k-1}(\xi) = q_k(\xi) \cdot 0 - f_{k+1}(\xi) = -f_{k+1}(\xi)$. При этом $f_{k-1}(\xi), f_{k+1}(\xi) \neq \neq 0$ в силу п. 3). Следовательно, числа $f_{k-1}(\xi)$ и $f_{k+1}(\xi)$ равны по модулю и имеют противоположные знаки. □

Пусть α_1, α_2, …, α_k — произвольный упорядоченный набор ненулевых действительных чисел. *Переменой знака* в этом наборе

чисел будем называть ситуацию, когда для некоторого $1 \leqslant i \leqslant k-1$ числа α_i и α_{i+1} имеют разные знаки.

Пусть $f(x) \in \mathbb{R}[x]$, $f_0, f_1, \ldots, f_m$ — система многочленов Штурма для многочлена f, а ξ — произвольное действительное число. Рассмотрим упорядоченный набор чисел $f_0(\xi)$, $f_1(\xi)$, $\ldots$, $f_m(\xi)$. Вычеркнем из него все нули. Обозначим через $W_f(\xi)$ число перемен знака в оставшемся наборе чисел.

Теорема 10.7 (теорема Штурма). *Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$, не имеющий кратных корней, $a, b \in \mathbb{R}$, $a < b$ и числа a и b не являются корнями многочлена $f(x)$. Тогда $W_f(a) \geqslant W_f(b)$ и число корней многочлена $f(x)$ на отрезке $[a, b]$ равно $W_f(a) - W_f(b)$.*

Доказательство. Как и в доказательстве предложения 10.1, мы будем пользоваться непрерывностью многочленов над $\mathbb{R}$ как функций из $\mathbb{R}$ в $\mathbb{R}$.

Договоримся для краткости говорить о знаках многочленов вместо знаков значений многочленов в тех или иных точках. Посмотрим, как меняется число $W_f(x)$, когда x движется, возрастая, от a к b. Пусть f_0, f_1, $\ldots$, f_m — система многочленов Штурма для многочлена f. Предположим сначала, что ни один из многочленов f_0, f_1, $\ldots$, f_m при этом ни разу не меняет знак. Ясно, что в этом случае $W_f(a) = W_f(b)$. С другой стороны, в этом случае многочлен $f_0 = f$ сохраняет знак в интервале (a, b). Кроме того, в этом интервале сохраняет знак многочлен $f_1 = f'$, а это значит, что f является монотонной функцией на (a, b). Ясно, что в этом случае f не имеет корней в интервале (a, b). Таким образом, как число корней многочлена $f(x)$ на отрезке $[a, b]$, так и число $W_f(a) - W_f(b)$ равны 0. В частности, они равны между собой.

Предположим теперь, что при движении x от a к b по крайней мере один из многочленов f_0, f_1, $\ldots$, f_m хотя бы один раз изменил знак. Ясно, что если многочлен f_i изменил знак при переходе x через точку $\xi \in (a, b)$, то ξ — корень многочлена f_i. В силу следствия 8.3 число точек интервала (a, b), в которых меняется знак хотя бы одного из многочленов f_0, f_1, $\ldots$, f_m, конечно. Обозначим эти точки через $c_1, c_2, \ldots, c_s$ и будем считать без ограничения общности, что $c_1 < c_2 < \cdots < c_s$. Кроме того, для удобства обозначений положим $c_0 = a$ и $c_{s+1} = b$.

Пока x проходит любой из интервалов (c_i, c_{i+1}), где $i = 0, 1, \ldots, s$, знаки многочленов f_0, f_1, $\ldots$, f_m, а значит и число перемен знаков в последовательности чисел $f_0(x)$, $f_1(x)$, $\ldots$, $f_m(x)$, не меняются. Посмотрим, как меняется число перемен знаков в этой последовательности, когда x проходит через точку c_k для некоторого $1 \leqslant k \leqslant s$. В силу выбора точек $c_1, c_2, \ldots, c_s$ при переходе x через c_k по крайней мере один из многочленов f_0, f_1, $\ldots$, f_m меняет знак. Пусть f_i, где $0 \leqslant i \leqslant m$, — произвольный многочлен, изменивший знак при переходе x через c_k. В частности, это означает, что $f_i(c_k) = 0$. Согласно п. 2) леммы 10.6 $i < m$. Дальнейшие рассмотрения распадаются на два случая.

Случай 1: $i > 0$. Из п. 3) леммы 10.6 вытекает, что числа $f_{i-1}(c_k)$ и $f_{i+1}(c_k)$ отличны от 0. Следовательно, существует $\varepsilon > 0$ такое, что каждый из многочленов f_{i-1} и f_{i+1} сохраняет знак в интервале $(c_k - \varepsilon, c_k + \varepsilon)$, а многочлен f_i сохраняет знак в каждом из интервалов $(c_k - \varepsilon, c_k)$ и $(c_k, c_k + \varepsilon)$. В силу п. 4) леммы 10.6 знаки многочленов f_{i-1} и f_{i+1} в интервале $(c_k - \varepsilon, c_k + \varepsilon)$ различны. Предположим сначала, что $f_i(x) > 0$ при $x \in (c_k - \varepsilon, c_k)$ и $f_i(x) < 0$ при $x \in (c_k, c_k + \varepsilon)$. Если $f_{i-1}(x) > 0$ и $f_{i+1}(x) < 0$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, то имеет место ситуация, указанная в строках 1 и 2 табл. 10.1, а если $f_{i-1}(x) < 0$ и $f_{i+1}(x) > 0$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, — ситуация, указанная в строках 3 и 4 той же таблицы (во всех строках табл. 10.1, как и в табл. 10.2 ниже, красным цветом указаны ситуации, в которых возникает перемена знака). Если же $f_i(x) < 0$ при $x \in (c_k - \varepsilon, c_k)$ и $f_i(x) > 0$ при $x \in (c_k, c_k + \varepsilon)$, то, в зависимости от знаков чисел $f_{i-1}(x)$ и $f_{i+1}(x)$ при $x \in (c_k - \varepsilon, c_k + \varepsilon)$, имеет место ситуация, указанная либо в строках 5 и 6 табл. 10.1, либо в строках 7 и 8 этой таблицы.

Мы видим, что если в интервале $(c_k - \varepsilon, c_k)$ перемена знака в последовательности чисел $f_0(x)$, $f_1(x)$, $\ldots$, $f_m(x)$ происходила при переходе от многочлена f_i к f_{i+1}, то в интервале $(c_k, c_k + \varepsilon)$ она будет происходить при переходе от f_{i-1} к f_i (см. строки 1, 2, 7 и 8 табл. 10.1). И наоборот, если в интервале $(c_k - \varepsilon, c_k)$ перемена знака происходила при переходе от f_{i-1} к f_i, то в интервале $(c_k, c_k + \varepsilon)$ она будет происходить при переходе от f_i к f_{i+1} (см. строки 3–6 табл. 10.1). Таким образом, за счет того, что многочлен f_i при $0 < i < m$ меняет знак в точке c_k, перемена знака в после-

Таблица 10.1. Перемена знака «сдвигается»

	x принадлежит интервалу	$f_{i-1}(x)$	$f_i(x)$	$f_{i+1}(x)$
1	$(c_k-\varepsilon, c_k)$	>0	>0	<0
2	$(c_k, c_k+\varepsilon)$	>0	<0	<0
3	$(c_k-\varepsilon, c_k)$	<0	>0	>0
4	$(c_k, c_k+\varepsilon)$	<0	<0	>0
5	$(c_k-\varepsilon, c_k)$	>0	<0	<0
6	$(c_k, c_k+\varepsilon)$	>0	>0	<0
7	$(c_k-\varepsilon, c_k)$	<0	<0	>0
8	$(c_k, c_k+\varepsilon)$	<0	>0	>0

довательности чисел $f_0(x)$, $f_1(x)$, …, $f_m(x)$ может «сдвинуться на одну позицию» влево или вправо, но число перемен знаков в этой последовательности измениться не может.

Случай 2: $i=0$. Это означает, что c_k — корень многочлена f_0. Из п. 3) леммы 10.6 вытекает, что c_k не является корнем многочлена f_1. Следовательно, существует $\varepsilon>0$ такое, что многочлен f_1 сохраняет знак в интервале $(c_k-\varepsilon, c_k+\varepsilon)$, а многочлен f_0 сохраняет знак в каждом из интервалов $(c_k-\varepsilon, c_k)$ и $(c_k, c_k+\varepsilon)$. Напомним, что $f=f_0$ и $f_1=f'$. Если $f_1(\xi)>0$ для всех $\xi\in(c_k-\varepsilon, c_k+\varepsilon)$, то многочлен $f=f_0$ монотонно возрастает в интервале $(c_k-\varepsilon, c_k+\varepsilon)$, и потому $f_0(\xi)<0$ при $\xi\in(c_k-\varepsilon, c_k)$ и $f_0(\xi)>0$ при $\xi\in(c_k, c_k+\varepsilon)$. Если же $f_1(\xi)<0$ для всех $\xi\in(c_k-\varepsilon, c_k+\varepsilon)$, то многочлен $f=f_0$ монотонно убывает в интервале $(c_k-\varepsilon, c_k+\varepsilon)$, и потому $f_0(\xi)>0$ при $\xi\in(c_k-\varepsilon, c_k)$ и $f_0(\xi)<0$ при $\xi\in(c_k, c_k+\varepsilon)$. Таким образом, имеет место ситуация, указанная либо в строках 1 и 2 табл. 10.2, либо в строках 3 и 4 той же таблицы.

Мы видим, что знаки чисел $f_0(x)$ и $f_1(x)$ различаются в интервале $(c_k-\varepsilon, c_k)$ и совпадают в интервале $(c_k, c_k+\varepsilon)$. Иными словами, в интервале $(c_k-\varepsilon, c_k)$ в последовательности чисел $f_0(x)$, $f_1(x)$, …, $f_m(x)$ происходит перемена знака при переходе от многочлена f_0 к f_1, а в интервале $(c_k, c_k+\varepsilon)$ эта перемена знака отсутствует. Таким образом, за счет того, что многочлен f_0 меняет знак в точке c_k, число перемен знаков в последовательности чисел $f_0(x)$, $f_1(x)$, …,

Таблица 10.2. Перемена знака исчезает

	x принадлежит интервалу	$f_0(x)$	$f_1(x)$
1	$(c_k - \varepsilon, c_k)$	< 0	> 0
2	$(c_k, c_k + \varepsilon)$	> 0	> 0
3	$(c_k - \varepsilon, c_k)$	> 0	< 0
4	$(c_k, c_k + \varepsilon)$	< 0	< 0

$f_m(x)$ уменьшается на 1.

Итак, при движении x от a к b число перемен знаков в последовательности чисел $f_0(x), f_1(x), \ldots, f_m(x)$ меняется только в случае, когда x проходит через точку, в которой многочлен $f_0 = f$ меняет знак, причем в этом случае оно уменьшается на 1. Следовательно, разность $W_f(a) - W_f(b)$ равна числу таких точек. Ясно, все числа, при переходе через которые многочлен f меняет знак, являются его корнями. Осталось проверить, что других корней у многочлена f на интервале (a, b) нет. В самом деле, пусть ξ — корень многочлена f, принадлежащий интервалу (a, b), и этот многочлен при переходе x через ξ не меняет знак. В силу следствия из теоремы Безу $f(x) = (x - \xi)g(x)$ для некоторого многочлена $g(x)$. Ясно, что двучлен $x - \xi$ меняет знак при переходе x через ξ. Поскольку $f(x)$ при этом знака не меняет, мы получаем, что многочлен $g(x)$ должен изменить знак при переходе x через ξ. Это означает, что число ξ является корнем многочлена $g(x)$, а значит, кратным корнем многочлена $f(x)$. Но по условию многочлен f не имеет кратных корней. □

Построение системы многочленов Штурма для данного многочлена f может привести к громоздким вычислениям. Чтобы упростить их, часто бывает полезным следующий факт: *в процессе построения многочленов $f_0(x)$, $f_1(x)$, …, $f_m(x)$ каждый из них можно умножать на произвольную положительную константу*, поскольку после такого умножения все свойства этой системы многочленов, перечисленные в лемме 10.6, сохранятся. В то же время умножать какие-то из многочленов $f_0(x)$, $f_1(x)$, …, $f_m(x)$ на отрицательные константы нельзя, так как для полученных при этом многочленов может не выполняться заключение п. 4) леммы 10.6.

Из теоремы Штурма и следствия 10.2 вытекает следующий факт.

Следствие 10.8. *Пусть $f(x)$ — многочлен степени > 0 над полем $\mathbb{R}$, не имеющий кратных корней. Число действительных корней многочлена $f(x)$ равно $W_f(-R_f) - W_f(R_f)$.* □

Теорема Штурма и следствие 10.8 доказаны в предположении, что многочлен не имеет кратных корней. Пусть теперь f — произвольный многочлен степени > 0 над полем $\mathbb{R}$. Положим $g = \frac{f}{d}$, где d — наибольший общий делитель многочленов f и f'. В силу следствия 10.4 многочлены f и g имеют одни и те же корни, причем второй из них не имеет кратных корней. Поэтому можно применить теорему Штурма или следствие 10.8 к многочлену g и найти соответственно число корней многочлена f на отрезке $[a, b]$ или число всех его действительных корней.

Начав с интервала $(-R_f, R_f)$, последовательно уменьшая размеры интервалов (например, методом половинного деления) и применяя к каждому из полученных интервалов теорему Штурма, можно для каждого корня многочлена $f \in \mathbb{R}[x]$ найти интервал числовой прямой, содержащий этот корень и не содержащий никаких других корней. Продолжая процесс половинного деления, можно сделать интервалы, содержащие корни, сколь угодно маленькими. Это означает, что мы можем приближенно найти все действительные корни многочлена f с любой наперед заданной степенью точности.

§ 11. Рациональные корни многочленов над полем $\mathbb{Q}$

В этом параграфе речь пойдет о способах нахождения рациональных корней многочленов над полем $\mathbb{Q}$. Очевидно, что многочлен из $\mathbb{Q}[x]$ может не иметь рациональных корней даже в том случае, когда у него есть действительные корни. В качестве примера, подтверждающего этот факт, можно взять многочлен $x^2 - 2$. Оказывается, однако, что с помощью несложных вычислений можно выяснить, есть ли у данного многочлена над полем $\mathbb{Q}$ рациональные корни, и если они есть, то найти их.

Если не все коэффициенты многочлена $f \in \mathbb{Q}[x]$ являются целыми числами, можно домножить его на наименьшее общее кратное знаменателей всех дробей, являющихся его коэффициентами. Полученный многочлен будет иметь те же корни, что и f, а все его коэффициенты будут целыми числами. Поэтому далее можно рассматривать только многочлены над $\mathbb{Q}$ с целыми коэффициентами.

Предложение 11.1. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен над полем* $\mathbb{Q}$ *с целыми коэффициентами, а* $\frac{p}{q}$ *— рациональное число и несократимая дробь. Если* $\frac{p}{q}$ *— корень многочлена* $f(x)$*, то* p *делит* a_0*,* a q *делит* a_n*.*

Доказательство. Поскольку $\frac{p}{q}$ — корень многочлена $f(x)$, имеем

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \cdot \frac{p}{q} + a_0 = 0. \tag{11.1}$$

Умножив обе части этого равенства на q^n, получим

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0,$$

откуда $a_0 q^n = p(-a_n p^{n-1} - a_{n-1}p^{n-2}q - \cdots - a_1 q^{n-1})$. Следовательно, $p \mid a_0 q^n$ (мы используем символ $\mid$ для обозначения делимости не только многочленов, но и целых чисел). Поскольку числа p и q взаимно просты, $p \mid a_0$. Аналогично из равенства $a_n p^n = q(-a_{n-1}p^{n-1} - \cdots - a_1 p q^{n-2} - a_0 q^{n-1})$ вытекает, что $q \mid a_n$. □

Многочлен, старший коэффициент которого равен 1, называется *унитарным*. Из предложения 11.1 непосредственно вытекает следующий факт.

Следствие 11.2. *Если* $f(x)$ *— унитарный многочлен над полем* $\mathbb{Q}$ *с целыми коэффициентами, то все рациональные корни многочлена* $f(x)$ *являются целыми числами и делят свободный член этого многочлена.* □

Поскольку число делителей старшего коэффициента и свободного члена многочлена над полем $\mathbb{R}$ с целыми коэффициентами конечно, предложение 11.1 сводит задачу нахождения рациональных

корней таких многочленов к несложному перебору, который, однако, может оказаться достаточно длинным, если старший коэффициент и свободный член многочлена имеют много делителей. Этот перебор можно существенно сократить, если использовать следующее утверждение (см. комментарий после его доказательства).

Предложение 11.3. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *— многочлен над полем* $\mathbb{Q}$ *с целыми коэффициентами,* $\frac{p}{q}$ *— рациональное число и несократимая дробь, а* k *— произвольное целое число. Если* $\frac{p}{q}$ *— корень многочлена* $f(x)$*, то* $p - kq$ *делит* $f(k)$*.*

Доказательство. Ясно, что

$$f(k) = a_n k^n + a_{n-1}k^{n-1} + \cdots + a_1 k + a_0.$$

Вычтем из этого равенства равенство (11.1). Получим

$$f(k) = a_n\left(k^n - \left(\frac{p}{q}\right)^n\right) + a_{n-1}\left(k^{n-1} - \left(\frac{p}{q}\right)^{n-1}\right) + \cdots + a_1\left(k - \frac{p}{q}\right).$$

Умножив это равенство на q^n, получим

$$\begin{aligned} q^n f(k) = {} & a_n(k^n q^n - p^n) + a_{n-1}q(k^{n-1}q^{n-1} - p^{n-1}) + \\ & + \cdots + a_1 q^{n-1}(kq - p). \end{aligned} \tag{11.2}$$

Учитывая, что для любого натурального s и для любых $a, b \in \mathbb{R}$ выполнено равенство

$$a^s - b^s = (a - b)(a^{s-1} + a^{s-2}b + \cdots + ab^{s-2} + b^{s-1}),$$

получаем, что $(kq - p) \mid (k^s q^s - p^s)$ для всех $s = 2, 3, \ldots, n$. Из равенства (11.2) вытекает теперь, что $(kq - p) \mid q^n f(k)$. Проверим, что $kq - p$ взаимно просто с q^n. Предположим, что это не так. Тогда существует простое число r, которое делит и $kq - p$, и q^n. Из того что r — простое число и $r \mid q^n$, вытекает, что $r \mid q$. Учитывая, что $r \mid (kq - p)$, получаем, что $r \mid p$. Но r не может одновременно делить и p, и q, поскольку числа p и q взаимно просты. Итак, $kq - p$ делит $q^n f(k)$ и взаимно просто с q^n. Следовательно, $(kq - p) \mid f(k)$. □

Предложение 11.3 позволяет существенно сократить перебор делителей старшего коэффициента и свободного члена многочлена

с целыми коэффициентами при поиске его рациональных корней, поскольку оно показывает, что можно рассматривать только такие пары (p, q), что $(p-q) \mid f(1)$, $(p+q) \mid f(-1)$, $(p-2q) \mid f(2)$ и т. д.

Отметим еще, что, поскольку $f(0) = a_0$, предложение 11.3 обобщает утверждение предложения 11.1 о том, что $p \mid a_0$.

Решение типовых задач

Основными типами задач по теме данной главы являются следующие:

1) задачи об аппроксимации функций многочленами (или, что то же самое, о нахождении многочлена по его значениям в заданных точках);
2) задачи, связанные с применением теоремы Безу;
3) задачи, связанные с выяснением кратности корней многочлена;
4) задачи о решении уравнений в поле $\mathbb{R}$ или поле $\mathbb{C}$;
5) задачи о нахождении числа действительных корней многочлена над полем $\mathbb{R}$ на всей числовой прямой или на некотором ее отрезке;
6) задачи о нахождении рациональных корней многочленов с целыми коэффициентами.

Решим две задачи первого типа.

Задача III.1. Найти многочлен наименьшей степени $p(x)$, принимающий в указанных ниже точках следующие значения:

x	-1	0	1	2
$p(x)$	-1	1	-3	-7

.

Решение. В силу теоремы 6.1 $\deg p(x) \leqslant 3$. Положим $p(x) = ax^3 + bx^2 + cx + d$. Подставив в это равенство вместо x значения, указанные в условии задачи, получим следующую систему линейных уравнений:

$$\begin{cases} -a + b - c + d = -1, \\ d = 1, \\ a + b + c + d = -3, \\ 8a + 4b + 2c + d = -7. \end{cases}$$

Согласно второму уравнению, $d = 1$. Подставив 1 вместо d в три других уравнения, получим систему

$$\begin{cases} -a + b - c = -2, \\ a + b + c = -4, \\ 8a + 4b + 2c = -8. \end{cases}$$

Решим ее методом Гаусса. Запишем расширенную матрицу системы и приведем ее к ступенчатому виду:

$$\left(\begin{array}{ccc|c} -1 & 1 & -1 & -2 \\ 1 & 1 & 1 & -4 \\ 8 & 4 & 2 & -8 \end{array}\right) \sim \left(\begin{array}{ccc|c} -1 & 1 & -1 & -2 \\ 0 & 2 & 0 & -6 \\ 0 & 12 & -6 & -24 \end{array}\right) \sim \left(\begin{array}{ccc|c} -1 & 1 & -1 & -2 \\ 0 & 2 & 0 & -6 \\ 0 & 0 & -6 & 12 \end{array}\right).$$

С помощью полученной матрицы последовательно находим, что $c = -2$, $b = -3$ и $a = 1$. Следовательно, $p(x) = x^3 - 3x^2 - 2x + 1$.

Ответ. $p(x) = x^3 - 3x^2 - 2x + 1$.

Задача III.2. Построить интерполяционный многочлен Лагранжа $p(x)$ для функции $f(x)$, принимающей следующие значения:

x	-2	-1	1	2
$f(x)$	1	-7	-5	-19

Решение. Решим задачу с помощью формул (6.3) и (6.4). Чтобы воспользоваться ими, перепишем условие задачи с помощью обозначений, используемых в этих формулах. В условии задачи указаны значения функции $f(x)$ в точках $x_0 = -2$, $x_1 = -1$, $x_2 = 1$ и $x_3 = 2$. А именно, $y_0 = f(x_0) = 1$, $y_1 = f(x_1) = -7$, $y_2 = f(x_2) = -5$ и $y_3 = f(x_3) = -19$. В соответствии с формулами (6.3) и (6.4) $p(x) = p_0(x) - 7p_1(x) - 5p_2(x) - 19p_3(x)$, где

$$p_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} \cdot \frac{x - x_3}{x_0 - x_3} = \frac{x+1}{-1} \cdot \frac{x-1}{-3} \cdot \frac{x-2}{-4} = \\ = \frac{x^3 - 2x^2 - x + 2}{-12},$$

$$p_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} = \frac{x+2}{1} \cdot \frac{x-1}{-2} \cdot \frac{x-2}{-3} = \\ = \frac{x^3 - x^2 - 4x + 4}{6},$$

$$p_2(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} = \frac{x+2}{3} \cdot \frac{x+1}{2} \cdot \frac{x-2}{-1} =$$

$$= \frac{x^3 + x^2 - 4x - 4}{-6},$$

$$p_3(x) = \frac{x - x_0}{x_3 - x_0} \cdot \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_3}{x_3 - x_2} = \frac{x+2}{4} \cdot \frac{x+1}{3} \cdot \frac{x-1}{1} =$$

$$= \frac{x^3 + 2x^2 - x - 2}{12}.$$

Следовательно,

$$p(x) = -\frac{x^3 - 2x^2 - x + 2}{12} - \frac{7(x^3 - x^2 - 4x + 4)}{6} +$$

$$+ \frac{5(x^3 + x^2 - 4x - 4)}{6} - \frac{19(x^3 + 2x^2 - x - 2)}{12} =$$

$$= -2x^3 - x^2 + 3x - 5.$$

Ответ. $p(x) = -2x^3 - x^2 + 3x - 5$.

Задачи второго типа чаще всего сводятся к тому, чтобы, используя схему Горнера, найти частное и остаток от деления многочлена $f(x)$ над полем $\mathbb{R}$ на двучлен $x - \alpha$, где $\alpha \in \mathbb{R}$. В разделе «Решение типовых задач» в главе II был приведен пример решения этой задачи с помощью деления многочлена на многочлен столбиком (см. задачу II.2). Решим ту же самую задачу с использованием схемы Горнера.

Задача III.3. Разделить многочлен $f(x) = x^4 - x^3 - 3x^2 + 3x - 2$ на многочлен $g(x) = x - 3$ с остатком.

Решение. Как обычно, обозначим частное от деления через $q(x)$, а остаток через $r(x)$. Составим таблицу, о которой говорится в описании схемы Горнера после доказательства теоремы Безу. Поскольку $3 \cdot 1 + (-1) = 2$, $3 \cdot 2 + (-3) = 3$, $3 \cdot 3 + 3 = 12$ и $3 \cdot 12 + (-2) = 34$, таблица будет выглядеть так:

	1	−1	−3	3	−2
3	1	2	3	12	34

.

Следовательно, $q(x) = x^3 + 2x^2 + 3x + 12$ и $r(x) = 34$.

Ответ. $q(x) = x^3 + 2x^2 + 3x + 12$, $r(x) = 34$.

Ответ, разумеется, совпал с ответом к задаче II.2.

Перейдем к задачам третьего типа.

Задача III.4. Выяснить, корнем какой кратности многочлена $f(x) = x^4 - 5x^3 + 9x^2 - 7x + 2$ является число 1.

Решение. Разделим $f(x)$ на $x - 1$ по схеме Горнера. Соответствующая таблица имеет вид:

	1	−5	9	−7	2
1	1	−4	5	−2	0

Следовательно, $f(x) = (x-1)f_1(x)$, где $f_1(x) = x^3 - 4x^2 + 5x - 2$. Разделим $f_1(x)$ на $x - 1$ по схеме Горнера. Соответствующая таблица имеет вид:

	1	−4	5	−2
1	1	−3	2	0

Следовательно, $f_1(x) = (x-1)f_2(x)$, и потому $f(x) = (x-1)^2 f_2(x)$, где $f_2(x) = x^2 - 3x + 2$. Разделим $f_2(x)$ на $x - 1$ по схеме Горнера. Соответствующая таблица имеет вид:

	1	−3	2
1	1	−2	0

Следовательно, $f_2(x) = (x-1)f_3(x)$, и потому $f(x) = (x-1)^3 f_3(x)$, где $f_3(x) = x - 2$. Очевидно, что $x - 2$ не делится на $x - 1$. Следовательно, $f(x)$ делится на $(x-1)^3$, но не делится на $(x-1)^4$, и потому 1 — корень кратности 3 многочлена $f(x)$.

Ответ. 3.

Способ решения задачи третьего типа, изложенный выше, является достаточно громоздким, так как требует многократного деления многочлена на многочлен. Укажем еще один способ решения этой задачи, при котором делить многочлен на многочлен не придется ни разу. Этот способ основан на следствии 10.5.

Задача III.5. Выяснить, корнем какой кратности многочлена $f(x) = x^6 + 9x^5 + 20x^4 - 30x^3 - 135x^2 - 27x + 162$ является число -3.

Решение. Проверим прежде всего, что -3 — корень многочлена $f(x)$. В самом деле,

$$f(-3) = 729 - 2187 + 1620 + 810 - 1215 + 81 + 162 = 0.$$

Будем теперь искать производные многочлена f и их значения при $x = -3$ до тех пор, пока значение очередной производной не окажется отличным от 0:

$$\begin{aligned}
f'(x) &= 6x^5 + 45x^4 + 80x^3 - 90x^2 - 270x - 27;\\
f'(-3) &= -1458 + 3645 - 2160 - 810 + 810 - 27 = 0;\\
f''(x) &= 30x^4 + 180x^3 + 240x^2 - 180x - 270;\\
f''(-3) &= 2430 - 4860 + 2160 + 540 - 270 = 0;\\
f'''(x) &= 120x^3 + 540x^2 + 480x - 180;\\
f'''(-3) &= -3240 + 4860 - 1440 - 180 = 0;\\
f^{\mathrm{iv}}(x) &= 360x^2 + 1080x + 480;\\
f^{\mathrm{iv}}(-3) &= 3240 - 3240 + 480 = 480 \neq 0.
\end{aligned}$$

Итак, число -3 является корнем многочленов f, f', f'' и f''', но не является корнем многочлена f^{iv}. В силу следствия 10.5 оно является корнем кратности 4 многочлена $f(x)$.

Ответ. 4.

Решим задачу четвертого типа.

Задача III.6. Решить уравнение $x^4 + x^3 + x^2 + 3x - 6 = 0$:

а) в поле $\mathbb{R}$;

б) в поле $\mathbb{C}$.

Решение. Проверим, имеет ли данное уравнение целые корни. В силу следствия 11.2 если они существуют, то являются делителями числа 6. Обозначим через $f(x)$ левую часть данного уравнения и найдем $f(1)$: $f(1) = 1 + 1 + 1 + 3 - 6 = 0$. Мы нашли первый корень данного уравнения в поле $\mathbb{R}$: $x_1 = 1$. Разделим $f(x)$ на $x - 1$ с помощью схемы Горнера. Соответствующая таблица имеет вид

	1	1	1	3	−6
1	1	2	3	6	0

.

Таким образом, $f(x) = (x - 1)(x^3 + 2x^2 + 3x + 6)$. Все остальные целые корни уравнения $f(x) = 0$, если они существуют, являются

корнями уравнения $g(x) = 0$, где $g(x) = x^3+2x^2+3x+6$. Перебирая дедители свободного члена многочлена $g(x)$, имеем:

$$\begin{aligned} g(1) &= 1+2+3+6 = 12 \neq 0; \\ g(-1) &= -1+2-3+6 = 4 \neq 0; \\ g(2) &= 8+8+6+6 = 26 \neq 0; \\ g(-2) &= -8+8-6+6 = 0. \end{aligned}$$

Мы нашли второй корень уравнения $f(x) = 0$ в поле $\mathbb{R}$: $x_2 = -2$. Разделим $g(x)$ на $x+2$ с помощью схемы Горнера. Соответствующая таблица имеет вид

	1	2	3	6
-2	1	0	3	0

Таким образом, $g(x) = (x+2)(x^2+3)$. Уравнение $x^2+3 = 0$ не имеет действительных корней и имеет два комплексных корня: $x_{3,4} = \pm\sqrt{3}i$. Следовательно, уравнение $f(x) = 0$ имеет в поле $\mathbb{R}$ два корня: $x_1 = 1$ и $x_2 = -2$, а в поле $\mathbb{C}$ четыре корня: $x_1 = 1$, $x_2 = -2$ и $x_{3,4} = \pm\sqrt{3}i$.

Ответ. а) $x_1 = 1$, $x_2 = -2$; б) $x_1 = 1$, $x_2 = -2$, $x_{3,4} = \pm\sqrt{3}i$.

Перейдем теперь к задачам пятого типа.

Задача III.7. Найти число действительных корней многочлена $f(x) = x^4 - 16x^2 - 16x - 4$:

а) на всей числовой прямой;

б) на отрезке $[-1, 1]$.

Решение. Построим систему многочленов Штурма для многочлена $f(x)$. Положим $f_0(x) = f(x) = x^4-16x^2-16x-4$. Если буквально следовать определению системы многочленов Штурма, в качестве многочлена $f_1(x)$ надо взять многочлен $f'(x) = 4x^3 - 32x - 16$. Но, как отмечалось выше (см. абзац после доказательства теоремы Штурма), в процессе построения системы многочленов Штурма любой многочлен можно умножить (а значит, и разделить) на любое положительное число. Чтобы упростить вычисления, разделим $f'(x)$ на 4 и положим $f_1(x) = x^3 - 8x - 4$. Разделим $f_0(x)$ на $f_1(x)$ с

остатком: $f_0(x) = xf_1(x) + (-8x^2 - 12x - 4)$. Если буквально следовать определению системы многочленов Штурма, в качестве многочлена $f_2(x)$ надо взять остаток, умноженный на -1, т. е. многочлен $8x^2 + 12x + 4$. Разделим его на 4 и положим $f_2(x) = 2x^2 + 3x + 1$. Теперь разделим $f_1(x)$ на $f_2(x)$ с остатком: $f_1(x) = (\frac{1}{2}x - \frac{3}{4})f_2(x) + + (-\frac{25}{4}x - \frac{13}{4}x)$. Умножим полученный остаток на -1. Чтобы сделать вычисления менее громоздкими, полученный многочлен умножим на 4. Получим, что $f_3(x) = 25x + 13$. Продолжим построение системы многочленов Штурма. Разделим $f_2(x)$ на $f_3(x)$ с остатком: $f_2(x) = (\frac{2}{25}x + \frac{49}{625})f_3(x) - \frac{12}{625}$. Остаток от деления, умноженный на -1, равен $\frac{12}{625}$. Это дает нам право считать, что $f_4(x) = 1$. Очевидно, что остаток от деления $f_3(x)$ на $f_4(x)$ равен 0. Поэтому система многочленов Штурма для многочлена $f(x)$ построена: она состоит из многочленов $f_0(x)$, $f_1(x)$, $f_2(x)$, $f_3(x)$ и $f_4(x)$. Многочлен $f_4(x)$ не имеет действительных корней. В силу п. 2) леммы 10.6 это означает, что многочлен $f(x)$ не имеет кратных корней и потому мы можем применить к нему теорему Штурма.

В силу следствия 10.2 все действительные корни многочлена $f(x)$ принадлежат интервалу $(-R_f, R_f)$, где

$$R_f = \frac{\max\{|-16|, |-16|, |-4|\}}{|1|} + 1 = 17.$$

Чтобы применить теорему Штурма, подсчитаем значения многочленов, входящих в систему многочленов Штурма, и число перемен знака в полученной последовательности чисел при $\xi = -17$ и $\xi = 17$. Результаты оформим в виде таблицы:

ξ	$f_0(\xi)$	$f_1(\xi)$	$f_2(\xi)$	$f_3(\xi)$	$f_4(\xi)$	$W_f(\xi)$
-17	79165	-4781	528	-412	1	4
17	78621	4773	630	438	1	0

В силу следствия 10.8 число действительных корней многочлена $f(x)$ равно $W_f(-17) - W_f(17) = 4 - 0 = 4$.

Чтобы найти число действительных корней многочлена $f(x)$ на отрезке $[-1, 1]$, проделаем вычисления, аналогичные проведенным выше, при $\xi = -1$ и $\xi = 1$. Результаты оформим в виде таблицы:

ξ	$f_0(\xi)$	$f_1(\xi)$	$f_2(\xi)$	$f_3(\xi)$	$f_4(\xi)$	$W_f(\xi)$
-1	-3	3	0	-12	1	3
1	-35	-11	6	38	1	1

В силу теоремы Штурма число действительных корней многочлена $f(x)$ на отрезке $[-1, 1]$ равно $W_f(-1) - W_f(1) = 3 - 1 = 2$.

Ответ. а) 4; б) 2.

Рассмотрим теперь случай, когда исходный многочлен имеет кратные корни.

Задача III.8. Найти число действительных корней многочлена $f(x) = x^3 - x^2 - 5x - 3$:

а) на всей числовой прямой;

б) на отрезке $[0, 3]$.

Решение. Как и в предыдущей задаче, начнем с построения системы многочленов Штурма для многочлена $f(x)$. Положим $f_0(x) = f(x) = x^3 - x^2 - 5x - 3$ и $f_1(x) = f'(x) = 3x^2 - 2x - 5$. Разделим $f_0(x)$ на $f_1(x)$ с остатком: $f_0(x) = (\frac{1}{3}x - \frac{1}{9})f_1(x) + (-\frac{32}{9}x - \frac{32}{9})$. Умножив остаток на $-\frac{9}{32}$, получаем, что $f_2(x) = x + 1$. Теперь разделим $f_1(x)$ на $f_2(x)$ с остатком: $f_1(x) = (3x - 5)f_2(x)$. Поскольку остаток равен 0, система многочленов Штурма для многочлена $f(x)$ построена: она состоит из многочленов $f_0(x)$, $f_1(x)$ и $f_2(x)$.

Многочлен $f_2(x)$ имеет действительный корень. В силу п. 2) леммы 10.6 это означает, что многочлен $f(x)$ имеет кратные корни. Поэтому напрямую к многочлену $f(x)$ теорема Штурма неприменима. Но в силу следствия 10.4 и п. 1) леммы 10.6 многочлен $g = \frac{f}{f_2}$ имеет те же корни, что и многочлен f, и не имеет кратных корней. Поэтому мы можем решить поставленную задачу, применив теорему Штурма к многочлену g.

Поскольку f_2 — многочлен степени 1, мы можем найти многочлен $g(x)$ с помощью схемы Горнера. Соответствующая таблица имеет вид

	1	−1	−5	−3
−1	1	−2	−3	0

.

Таким образом, $g(x) = x^2 - 2x - 3$. Построим систему многочленов Штурма для многочлена $g(x)$. Положим $g_0(x) = g(x) = x^2 - 2x - 3$. Поскольку $g'(x) = 2x - 2$, мы можем считать, что $g_1(x) = x - 1$. Разделим $g_0(x)$ на $g_1(x)$ с остатком: $g_0(x) = (x-1)g_1(x) - 4$. Поэтому можно считать, что $g_2(x) = 1$. Очевидно, что остаток от деления

$g_1(x)$ на $g_2(x)$ равен 0. Поэтому система многочленов Штурма для многочлена $g(x)$ построена: она состоит из многочленов $g_0(x)$, $g_1(x)$ и $g_2(x)$. Многочлен $g_2(x)$ не имеет действительных корней. В силу п. 2) леммы 10.6 это еще раз подтверждает, что многочлен $g(x)$ не имеет кратных корней и потому мы можем применить к нему теорему Штурма.

В силу следствия 10.2 все действительные корни многочлена $g(x)$ принадлежат интервалу $(-R_g, R_g)$, где

$$R_g = \frac{\max\{|-2|, |-3|\}}{|1|} + 1 = 4.$$

Чтобы применить теорему Штурма, подсчитаем значения многочленов, входящих в систему многочленов Штурма, и число перемен знака в полученной последовательности чисел при $\xi = -4$ и $\xi = 4$. Результаты оформим в виде таблицы:

ξ	$g_0(\xi)$	$g_1(\xi)$	$g_2(\xi)$	$W_g(\xi)$
-4	21	-5	1	2
4	5	3	1	0

В силу следствия 10.8 число действительных корней многочлена $g(x)$, а значит и многочлена $f(x)$, равно $W_g(-4) - W_g(4) = 2 - 0 = 2$.

Чтобы найти число действительных корней многочлена $g(x)$ на отрезке $[0, 3]$, проделаем вычисления, аналогичные проведенным выше, при $\xi = 0$ и $\xi = 3$. Результаты оформим в виде таблицы:

ξ	$g_0(\xi)$	$g_1(\xi)$	$g_2(\xi)$	$W_g(\xi)$
0	-3	-1	1	1
3	0	2	1	0

В силу теоремы Штурма число действительных корней многочлена $g(x)$, а значит и многочлена $f(x)$, на отрезке $[0, 3]$ равно $W_g(0) - W_g(3) = 1 - 0 = 1$.

Ответ. а) 2; б) 1.

Рассмотрим, наконец, задачи шестого типа.

Задача III.9. Найти все рациональные корни многочлена $f(x) = x^5 + 2x^4 - 7x^3 - 5x^2 + 12x - 3$.

Решение. В силу следствия 11.2 рациональными корнями многочлена $f(x)$ могут быть только числа ± 1 и ± 3. Найдем значения многочлена $f(x)$ от этих чисел. Пропуская вычисления, запишем их результаты: $f(1) = 0$, $f(-1) = -12 \neq 0$, $f(3) = 204 \neq 0$ и $f(-3) = 24 \neq 0$. Мы видим, что единственным рациональным корнем многочлена $f(x)$ является число 1.

Ответ. 1.

В качестве второго примера рассмотрим случай, когда не все коэффициенты многочлена являются целыми числами.

Задача III.10. Найти все рациональные корни многочлена $f(x) = x^5 + \frac{x^4}{2} + \frac{5x^3}{2} + \frac{x^2}{2} + x - 1$.

Решение. Чтобы избавиться от дробных коэффициентов, умножим многочлен $f(x)$ на 2. Понятно, что полученный многочлен $f_1(x) = 2x^5 + x^4 + 5x^3 + x^2 + 2x - 2$ имеет те же корни, что и $f(x)$. В силу предложения 11.1 рациональные корни многочлена $f_1(x)$ имеют вид $\frac{p}{q}$, где p и q делят число 2. При этом без ограничения общности можно считать, что $q > 0$ (если $q < 0$, мы можем умножить p и q на -1). Таким образом, $q \in \{1, 2\}$, а $p \in \{\pm 1, \pm 2\}$ и потому $\frac{p}{q} \in \{\pm 1, \pm 2, \pm\frac{1}{2}\}$. Найдем значения многочлена $f_1(x)$ от всех этих чисел: $f_1(1) = 9 \neq 0$, $f_1(-1) = -9 \neq 0$, $f_1(2) = 126 \neq 0$, $f_1(-2) = -90 \neq 0$, $f_1(\frac{1}{2}) = 0$ и $f_1(-\frac{1}{2}) = -\frac{27}{8} \neq 0$. Мы видим, что единственным рациональным корнем многочлена $f_1(x)$, а значит и многочлена $f(x)$, является число $\frac{1}{2}$.

Ответ. $\frac{1}{2}$.

В двух предыдущих задачах мы нашли рациональные корни многочлена полным перебором всех чисел, которые могут быть его корнями в силу предложения 11.1. Если старший коэффициент и/или свободный член многочлена имеют много делителей, такой способ решения является слишком громоздким. Следующие две задачи показывают, как можно сократить этот перебор.

Задача III.11. Найти все рациональные корни многочлена $f(x) = 3x^4 - 11x^3 + 9x^2 - 11x + 6$.

Решение. Пусть $\frac{p}{q}$ — корень многочлена $f(x)$, причем $q > 0$. В силу предложения 11.1 $q \in \{1, 3\}$, а $p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Предположим

сначала, что $q = 1$. Начнем рассматривать возможные значения $p = \frac{p}{q}$: $f(1) = -4 \neq 0$, $f(-1) = 40 \neq 0$, $f(2) = -20 \neq 0$, $f(-2) = 20 \neq \neq 0$, $f(3) = 0$. Мы видим, что число 3 является корнем многочлена $f(x)$. В силу следствия из теоремы Безу $f(x)$ делится на $x - 3$. Найдем частное $g(x)$ от деления $f(x)$ на $x - 3$ с помощью схемы Горнера. Соответствующая таблица имеет вид

	3	−11	9	−11	6
3	3	−2	3	−2	0

.

Итак, $g(x) = 3x^3 - 2x^2 + 3x - 2$. Все не найденные ранее корни многочлена $f(x)$ являются корнями многочлена $g(x)$. Вновь учитывая предложение 11.1, получаем, что если $\frac{p}{q}$ — корень многочлена $g(x)$ и $q > 0$, то $q \in \{1, 3\}$, а $p \in \{\pm 1, \pm 2\}$. Если $q = 1$, то $\frac{p}{q} \in \{\pm 1, \pm 2\}$. Ясно, что всякий корень многочлена $g(x)$ является корнем многочлена $f(x)$. Но, как мы видели выше, ни одно из чисел $\pm 1, \pm 2$ корнем многочлена $f(x)$ не является. Следовательно, при $q = 1$ корней многочлена $g(x)$ не существует. Поэтому можно считать, что $q = 3$ и потому $\frac{p}{q} \in \{\pm\frac{1}{3}, \pm\frac{2}{3}\}$. Простые вычисления показывают, что $g(\frac{1}{3}) = -\frac{10}{9} \neq 0$ и $g(-\frac{1}{3}) = -\frac{10}{3} \neq 0$, но $g(\frac{2}{3}) = 0$. Мы видим, что число $\frac{2}{3}$ является корнем многочлена $g(x)$. В силу следствия из теоремы Безу $g(x)$ делится на $x - \frac{2}{3}$. Найдем частное $h(x)$ от деления $g(x)$ на $x - \frac{2}{3}$ с помощью схемы Горнера. Соответствующая таблица имеет вид

	3	−2	3	−2
$\frac{2}{3}$	3	0	3	0

.

Итак, $h(x) = 3x^2 + 3$. Все не найденные ранее корни многочлена $g(x)$ являются корнями многочлена $h(x)$. Но последний многочлен не имеет действительных (в частности, рациональных) корней. Следовательно, многочлен $f(x)$ имеет только два рациональных корня: 3 и $\frac{2}{3}$.

Ответ. 3, $\frac{2}{3}$.

Последним (но весьма мощным) средством сокращения перебора при поиске рациональных корней многочлена с целыми коэффициентами является предложение 11.3. Приведем пример использования этого утверждения.

Задача III.12. Найти все рациональные корни многочлена $f(x) = x^5 - 2x^4 - 3x^3 - 2x^2 + 2x + 12$.

Решение. Пусть $\frac{p}{q}$ — корень многочлена $f(x)$. В силу следствия 11.2 можно считать, что $q = 1$, а $p \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. Чтобы сократить этот список, учтем, что, согласно предложению 11.3 при $k = 1$, $(p-1) \mid f(1)$. Поскольку $f(1) = 8$, получаем, что $p - 1 \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$ и потому $p \in \{2, 0, 3, -1, 5, -3, 9, -7\}$. С учетом сказанного выше это означает, что $p \in \{-1, 2, 3, -3\}$. Используя предложение 11.3 при $k = -1$, получаем, что $(p+1) \mid f(-1)$. Поскольку $f(-1) = 8$, это означает, что $p + 1 \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$ и потому $p \in \{0, -2, 1, -3, 3, -5, 7, -9\}$. Учитывая сказанное ранее, получаем, что $p \in \{3, -3\}$. Наконец, из предложения 11.3 при $k = 2$ вытекает, что $(p-2) \mid f(2)$. Поскольку $f(2) = -16$ делится на $3 - 2 = 1$, но не делится на $-3 - 2 = -5$, остается только один претендент на роль рационального корня многочлена $f(x)$ — число 3. Поскольку

$$f(3) = 243 - 162 - 81 - 18 + 6 + 12 = 0,$$

это число является корнем многочлена $f(x)$.

Ответ. 3.

Глава IV

Разложение многочленов на неприводимые множители

В арифметике немаловажную роль играет то обстоятельство, что произвольное натуральное число, отличное от 1, можно *разложить на простые множители*, т. е. представить, причем единственным образом, в виде произведения простых чисел. Связанные с этим вопросы и рассматриваются в данной главе — сначала для многочленов над произвольным полем, а затем для многочленов над полями $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$. В последнем параграфе главы ее результаты применяются для изучения рациональных дробей.

§ 12. Неприводимые множители многочленов над произвольным полем

Многочлен f над областью целостности R называется *неприводимым* над R, если $\deg f > 0$ и f нельзя представить в виде про-

изведения двух многочленов из $R[x]$, степень каждого из которых меньше степени f. Как мы увидим ниже, неприводимые многочлены как раз и являются аналогом простых чисел.

В дальнейшем мы многократно будем использовать следующее утверждение, не всегда упоминая его в явном виде.

Лемма 12.1. *Если многочлен, неприводимый над полем F, разложим в произведение двух многочленов, то один из этих многочленов принадлежит F.*

Доказательство. Пусть $f \in F[x]$ и $f = gh$. Ясно, что $\deg g, \deg h \leqslant \deg f$. Случай, когда $\deg g, \deg h < \deg f$, невозможен, поскольку f неприводим. Следовательно, степень одного из многочленов g и h равна степени f. Поскольку $\deg f = \deg g + \deg h$, степень другого из них равна 0. Но многочлен, степень которого равна 0, принадлежит F. □

Следующее свойство неприводимых многочленов является аналогом хорошо известного свойства простых чисел.

Предложение 12.2. *Если f — многочлен, неприводимый над полем F, и f делит произведение некоторых многочленов g и h над F, то f делит один из этих двух многочленов.*

Доказательство. Обозначим через d наибольший общий делитель многочленов f и g. Тогда $f = dq$ для некоторого многочлена q. В силу леммы 12.1 один из многочленов d и q принадлежит F. Если $d \in F$, то d ассоциирован с 1. Следовательно, 1 является наибольшим общим делителем g и f, т. е. эти два многочлена взаимно просты. По условию $f \mid gh$. В силу п. 2) предложения 5.5 $f \mid h$. Предположим теперь, что $q \in F$. Ясно, что $q \neq o$ (иначе $f = dq = o$) и потому $d = q^{-1}f$. Из определения многочлена d вытекает, что $g = ds$ для некоторого многочлена s. Следовательно, $g = q^{-1}sf$ и потому $f \mid g$. □

Следующее утверждение немедленно вытекает из следствия из теоремы Безу.

Замечание 12.3. *Если f — многочлен над полем F, $\deg f > 1$ и f имеет по крайней мере один корень в поле F, то f приводим над F.* □

Посмотрим, что можно сказать о неприводимых многочленах малых степеней. Многочлены степени 1 называются *линейными*. Следующее замечание очевидно.

Замечание 12.4. *Произвольный линейный многочлен над любым полем F неприводим над F.* □

Предложение 12.5. *Многочлен f степени 2 или 3 над произвольным полем F неприводим над F тогда и только тогда, когда он не имеет корней в F.*

Доказательство. Необходимость немедленно вытекает из замечания 12.3.

Достаточность. Предположим, что $2 \leqslant \deg f \leqslant 3$ и f приводим над F. Тогда $f = gh$ для некоторых многочленов g и h таких, что $\deg g, \deg h < \deg f$. Если степень одного из многочленов g и h равна 0, то степень другого из них равна степени f. Следовательно, $\deg g, \deg h > 0$. Если $\deg g, \deg h > 1$, то $\deg f = \deg g + \deg h \geqslant 4$. Таким образом, хотя бы один из многочленов g и h линеен. Без ограничения общности можно считать, что $\deg g = 1$ и $\ell c(g) = 1$ (если $\ell c(g) = \alpha \neq 1$, мы можем заменить g на $\frac{1}{\alpha} \cdot g$, а h на αh). Иными словами, $g = x - a$ для некоторого $a \in F$. Но тогда $f = (x - a)h$ и a является корнем многочлена f, лежащим в F. □

Следующий пример показывает, что аналог этого предложения для многочленов степени > 3 места не имеет.

Пример 12.6 (пример приводимого многочлена, не имеющего корней)**.** Многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим над полем $\mathbb{R}$, но не имеет действительных корней.

Перейдем к утверждению, упоминавшемуся в начале данной главы.

Теорема 12.7. *Всякий ненулевой многочлен f над полем F представим в виде*

$$f = \alpha g_1 g_2 \cdots g_n, \tag{12.1}$$

где $\alpha \in F$, а $g_1, g_2, \ldots, g_n$ — неприводимые над F унитарные многочлены. Это представление единственно с точностью до порядка следования сомножителей в правой части равенства.

Доказательство. Существование. Пусть $f \in F[x]$ и $f \neq o$. Докажем, что f представим в виде (12.1). Если $\deg f = 0$, то f имеет вид (12.1), где $\alpha = f$, а $n = 0$. Будем далее считать, что $\deg f > 0$. Если f неприводим над F, то он также представим в виде (12.1), где на этот раз $\alpha = \ell c(f)$, $n = 1$ и $g_1 = \alpha^{-1} f$. Пусть, наконец, f приводим, т. е. $f = gh$, где $\deg g, \deg h < \deg f$. В частности, $\deg f = \deg g + \deg h$. Если степень одного из многочленов g и h равна 0, то степень другого из этих многочленов равна $\deg f$ вопреки сказанному выше. Следовательно, $\deg g, \deg h > 0$. Мы доказали, что если многочлен f приводим, то его можно разложить в произведение многочленов g и h, таких, что $0 < \deg g, \deg h < \deg f$.

Если какой-то из многочленов g и h приводим, представим его в виде произведения многочленов, степени которых > 0 и меньше степени этого многочлена. Будем продолжать этот процесс до тех пор, пока среди получаемых многочленов будут встречаться приводимые. Поскольку на каждом шаге степени новых многочленов уменьшаются, через конечное число шагов этот процесс оборвется и мы представим многочлен f как произведение неприводимых многочленов $h_1, h_2, \ldots, h_n$. Для всякого $i = 1, 2, \ldots, n$ положим $\ell c(h_i) = \alpha_i$ и $g_i = \alpha_i^{-1} h_i$. Пусть $\alpha = \alpha_1 \alpha_2 \cdots \alpha_n$. Тогда выполнено равенство (12.1), причем $g_1, g_2, \ldots, g_n$ — неприводимые над F унитарные многочлены.

Единственность. Пусть $f = \alpha g_1 \cdots g_n = \beta h_1 \cdots h_m$, где $\alpha, \beta \in F$, а $g_1, \ldots, g_n, h_1, \ldots, h_m$ — неприводимые над F унитарные многочлены. Ясно, что, с одной стороны, $\ell c(f) = \ell c(\alpha g_1 \cdots g_n) = \alpha$, а с другой — $\ell c(f) = \ell c(\beta h_1 \cdots h_m) = \beta$. Следовательно, $\alpha = \beta$ и потому $\alpha g_1 \cdots g_n = \alpha h_1 \cdots h_m$. Разделив обе части последнего равенства на α, получим равенство $g_1 \cdots g_n = h_1 \cdots h_m$. Тогда $g_1 \mid (h_1 \cdots h_m)$. В силу предложения 12.2 $g_1 \mid h_i$ для некоторого $1 \leqslant i \leqslant m$. Не ограничивая общности, можно считать, что $i = 1$ (в противном случае можно переставить сомножители в произведении $h_1 \cdots h_m$). Итак, $h_1 = w g_1$ для некоторого многочлена w. Поскольку многочлен g_1 неприводим, $\deg g_1 > 0$, и потому $g_1 \notin F$. Из леммы 12.1 вытекает, что $w \in F$. Поскольку $\ell c(h_1) = w \cdot \ell c(g_1) = w \cdot 1 = w$, получаем, что $w = 1$ и потому $h_1 = g_1$. Без ограничения общности будем считать, что $n \leqslant m$. Если $n = m = 1$, то все доказано. Если $n = 1$, а $m > 1$, то $\deg h_1 \cdots h_m > \deg h_1 = \deg g_1$ вопреки равенству $g_1 =$

$= h_1 \cdots h_m$. Следовательно, $n > 1$. Тогда $g_1 g_2 \cdots g_n = g_1 h_2 \cdots h_m$, откуда $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Если $g_2 \cdots g_n - h_2 \cdots h_m \neq o$, то $\deg\bigl(g_1(g_2 \cdots g_n - h_2 \cdots h_m)\bigr) \geqslant \deg g_1 > 0$ вопреки равенству $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Следовательно, $g_2 \cdots g_n = h_2 \cdots h_m$.

Рассуждая так же, как в предыдущем абзаце, получаем, что $g_2 = h_2$. Если $m = n = 2$, то все доказано. Если $n = 2$, а $m > 2$, то $\deg h_2 \cdots h_m > \deg h_2 = \deg g_2$ вопреки равенству $g_2 = h_2 \cdots h_m$. Следовательно, $n > 2$. Тогда $g_2 g_3 \cdots g_n = g_2 h_3 \cdots h_m$, откуда $g_2(g_3 \cdots g_n - h_3 \cdots h_m) = o$. Как и в предыдущем абзаце, отсюда выводится, что $g_3 \cdots g_n = h_3 \cdots h_m$. Продолжая этот процесс, мы в конце концов получим, что $g_i = h_i$ для всех $i = 1, 2, \ldots, n$. Если $n = m$, то все доказано. Если же $n < m$, то $g_1 \cdots g_n = g_1 \cdots g_n h_{n+1} \cdots h_m$. Но это равенство противоречит тому, что $\deg(g_1 \cdots g_n h_{n+1} \cdots h_m) > \deg(g_1 \cdots g_n)$. □

Пусть f — многочлен над полем F. Многочлены g_1, g_2, …, g_n из равенства (12.1) не обязаны быть попарно различными. Ясно, что это равенство можно переписать в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}, \tag{12.2}$$

где $\alpha \in F$, $p_1, p_2, \ldots, p_m$ — попарно различные неприводимые над полем F унитарные многочлены, а $k_1, k_2, \ldots, k_m \in \mathbb{N}$. Равенство (12.2) называется *разложением многочлена f на неприводимые множители*, а многочлены $p_1, p_2, \ldots, p_m$ называются *неприводимыми множителями* многочлена f. Число k_i называется *кратностью* неприводимого множителя p_i. Неприводимый множитель p_i называется *кратным*, если $k_i > 1$, и *простым*, если $k_i = 1$. Чтобы упростить рассуждения, нам будет иногда удобно рассматривать неприводимый многочлен, не являющийся неприводимым множителем многочлена f, как неприводимый множитель f *кратности* 0.

Разложение многочленов на неприводимые множители можно использовать для нахождения наибольшего общего делителя двух многочленов. В самом деле, предположим, что $f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ и $g = \beta q_1^{\ell_1} q_2^{\ell_2} \cdots q_m^{\ell_m}$ — разложения многочленов f и g на неприводимые множители. Если f и g не имеют общих неприводимых множителей, т. е. $\{p_1, p_2, \ldots, p_n\} \cap \{q_1, q_2, \ldots, q_m\} = \varnothing$, то многочлены f и g взаимно просты. В противном случае можно без ограничения общности считать, что $p_1 = q_1$, $p_2 = q_2$, …, $p_r = q_r$ для

некоторого $1 \leqslant r \leqslant \min\{n, m\}$, причем r — максимальное число с таким свойством. Ясно, что в этом случае наибольшим общим делителем многочленов f и g является многочлен $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, где $a_i = \min\{k_i, \ell_i\}$ для всякого $i = 1, 2, \ldots, r$. Недостатком изложенного способа нахождения наибольшего общего делителя является то обстоятельство, что он не позволяет найти линейную форму наибольшего общего делителя.

§ 13. Отделение кратных множителей

Задача разложения произвольного многочлена f на неприводимые множители в общем случае очень сложна. Опишем один из способов упростить ее решение. Пусть (12.2) — разложение многочлена f на неприводимые множители и $k = \max\{k_1, k_2, \ldots, k_m\}$. Для всякого $i = 1, 2, \ldots, k$ обозначим через $d_i(f)$ произведение всех неприводимых множителей кратности i многочлена f (если f не имеет неприводимых множителей кратности i, полагаем $d_i(f) = 1$). Если $k > 1$ (т. е. если многочлен f имеет по крайней мере один кратный множитель), то степени многочленов $d_1(f), d_2(f), \ldots, d_k(f)$ меньше, чем степень f, и потому разложить их на неприводимые множители проще, чем f. Если это сделать, то разложение f на неприводимые множители находится очень просто, поскольку, очевидно,

$$f = \alpha d_1(f) d_2^2(f) \cdots d_k^k(f), \tag{13.1}$$

где $\alpha = \ell c(f)$. Возникает вопрос: как вычислить многочлены $d_1(f)$, $d_2(f)$, $\ldots$, $d_k(f)$, не разлагая f на неприводимые множители? Чтобы ответить на него, нам понадобится информация о неприводимых множителях многочлена и его производной.

Как мы уже отмечали (см. замечание 12.4), линейный многочлен над любым полем неприводим. Используя введенные выше термины, лемму 10.3 можно переформулировать так: если f — многочлен над полем $\mathbb{R}$, то его линейный неприводимый множитель кратности k является неприводимым множителем кратности $k - 1$ многочлена f'. Как мы увидим ниже, существуют нелинейные многочлены,

неприводимые над полем $\mathbb{R}$ (см. предложение 14.2). Но оказывается, что аналог сформулированного только что факта справедлив для всякого неприводимого множителя многочлена над произвольным полем характеристики 0 (в частности, над полем $\mathbb{R}$).

Чтобы доказать это, нам понадобятся некоторые новые понятия и результаты. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ — многочлен над кольцом R. Если $n > 0$, то *производной* многочлена $f(x)$ называется многочлен $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$, обозначаемый через $f'(x)$. Если же $n = 0$ или $f = o$, то, по определению, $f'(x) = o$. Если $R = \mathbb{R}$, то введенное только что понятие производной многочлена совпадает с понятием производной многочлена как функции от одной переменной, известным из математического анализа.

Следующий пример показывает, что степень производной многочлена степени n может отличаться от $n - 1$.

Пример 13.1 (пример многочлена, степень которого намного больше степени его производной)**.** Рассмотрим многочлен $f(x) = x^p$ над полем $\mathbb{Z}_p$, где p — произвольное простое число. Тогда $f'(x) = px^{p-1} = o$, поскольку для произвольного $x \in \mathbb{Z}_p$ выполнено равенство $px = 0$. Таким образом, $\deg f(x) = p$, но $\deg f'(x) = -\infty$.

Напомним, что поле $\mathbb{Z}_p$ имеет характеристику p. Следующее утверждение показывает, что над полем характеристики 0 аналога примера 13.1 не существует.

Замечание 13.2. *Если f — многочлен над полем F характеристики 0, а $\deg f > 0$, то $\deg f' = \deg f - 1$.*

Доказательство. Пусть $\ell m(f) = a_n x^n$. В частности, $a_n \neq 0$ и $\deg f = n$. По условию $n > 0$. Коэффициент при x^{n-1} в многочлене f' равен na_n. Если $na_n = 0$, то в силу замечания 1.3 $nx = 0$ для всякого $x \in F$. Но это невозможно, так как $\operatorname{char} F = 0$. Следовательно, $na_n \neq 0$ и потому $\deg f' = n - 1 = \deg f - 1$. □

Укажем некоторые свойства производной многочлена. Для многочленов над полем $\mathbb{R}$ они известны из курса математического анализа, но для многочленов над произвольным кольцом их надо доказывать.

Лемма 13.3. *Если $f(x)$ и $g(x)$ — многочлены над кольцом R, $t \in R$, а m — натуральное число такое, что $m > 1$, то:*

1) $(tf)' = tf'$;

2) $(f+g)' = f' + g'$;

3) $(fg)' = f'g + fg'$;

4) $(f^m)' = mf^{m-1}f'$.

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ и $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.

1) Имеем

$$\begin{aligned}(tf)' &= (ta_n x^n + ta_{n-1}x^{n-1} + \cdots + ta_1 x + ta_0)' = \\ &= nta_n x^{n-1} + (n-1)ta_{n-1}x^{n-2} + \cdots + ta_1 = \\ &= t(na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1) = tf'.\end{aligned}$$

2) Для определенности будем считать, что $n \geqslant m$. Если $n > m$, то будем записывать $g(x)$ в виде $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$, где $b_{m+1} = \cdots = b_n = 0$. Тогда

$$\begin{aligned}(f+g)' &= \big((a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + \\ &\quad + (a_0 + b_0)\big)' = \\ &= n(a_n + b_n)x^{n-1} + (n-1)(a_{n-1} + b_{n-1})x^{n-2} + \cdots + \\ &\quad + (a_1 + b_1) = \\ &= (na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1) + \\ &\quad + (nb_n x^{n-1} + (n-1)b_{n-1}x^{n-2} + \cdots + b_1) = f' + g'.\end{aligned}$$

3) Предположим сначала, что $f(x) = x^n$, а $g(x) = x^m$. Тогда

$$\begin{aligned}(fg)' &= (x^{n+m})' = (n+m)x^{n+m-1} = nx^{n+m-1} + mx^{n+m-1} = \\ &= nx^{n-1} \cdot x^m + x^n \cdot mx^{m-1} = f'g + fg'.\end{aligned}$$

Если же $f(x)$ и $g(x)$ — произвольные многочлены, то свойство 3) вытекает из доказанного только что равенства и доказанных выше свойств 1) и 2).

4) Докажем это свойство индукцией по m.

База индукции. Пусть $m = 2$. Используя свойство 3), имеем $(f^2)' = (f \cdot f)' = f'f + ff' = 2ff'$.

Шаг индукции. Пусть теперь $m > 2$. Используя предположение индукции и свойство 3), имеем

$$\begin{aligned}(f^m)' &= (f^{m-1} \cdot f)' = (f^{m-1})'f + f^{m-1}f' = \\ &= (m-1)f^{m-2}f'f + f^{m-1}f' = \\ &= (m-1)f^{m-1}f' + f^{m-1}f' = mf^{m-1}f'.\end{aligned}$$

Это завершает доказательство. □

Далее мы используем эти свойства производной без явных ссылок на лемму 13.3.

Лемма 13.4. *Если p — многочлен, неприводимый над полем F характеристики 0, то многочлены p и p' взаимно просты.*

Доказательство. Из неприводимости многочлена p вытекает, что $\deg p > 0$. Поскольку $\operatorname{char} F = 0$, из замечания 13.2 вытекает, что $\deg p' = \deg p - 1 \geqslant 0$. В частности, $p' \neq o$. Обозначим через d наибольший общий делитель многочленов p и p'. Тогда $p = dq$ для некоторого многочлена q. Если $\deg q = 0$, то $\deg p = \deg d \leqslant \deg p' = \deg p - 1$ (неравенство $\deg d \leqslant \deg p'$ вытекает из того, что $d \mid p'$). Полученное противоречие показывает, что $\deg q \neq 0$ и потому $q \notin F$. В силу леммы 12.1 $d \in F$. В частности, d ассоциирован с 1 и потому многочлены p и p' взаимно просты. □

Следующее утверждение является упомянутым выше обобщением леммы 10.3 на произвольные неприводимые множители многочлена над всяким полем характеристики 0. Доказательства этих двух утверждений во многом аналогичны, но есть и некоторые отличия. В дальнейшем мы будем иногда использовать символ $\nmid$, который означает «не делит».

Предложение 13.5. *Пусть f — многочлен степени > 0 над полем F характеристики 0, а p — неприводимый множитель многочлена f кратности k. Если $k = 1$, то p не делит f'. Если $k > 1$, то p является неприводимым множителем многочлена f' кратности $k - 1$.*

Доказательство. Обозначим через g произведение старшего коэффициента многочлена f и всех неприводимых множителей этого многочлена, отличных от p. Тогда $f = p^k g$ и многочлены p и g взаимно просты. В силу леммы 13.4 многочлены p и p' также взаимно просты. Из п. 3) предложения 5.5 вытекает теперь, что и многочлены p и $p'g$ взаимно просты. В частности, $p \nmid p'g$.

Если $k = 1$, то $f = pg$ и потому $f' = (pg)' = p'g + pg'$. Если бы p делил f', то p делил бы и $p'g = f' - pg'$. Следовательно, если $k = 1$, то $p \nmid f'$.

Пусть теперь $k > 1$. Тогда

$$f' = (p^k g)' = (p^k)'g + p^k g' = kp^{k-1}p'g + p^k g' = p^{k-1}(kp'g + pg').$$

Осталось проверить, что $p \nmid (kp'g + pg')$. Предположим, напротив, что $p \mid (kp'g + pg')$. Тогда, очевидно, $p \mid (kp'g)$, т. е. $kp'g = ph$ для некоторого многочлена h. Будем обозначать единицу поля F через e, чтобы отличать ее от числа 1. Положим $a = ke$. Если $a = 0$, то в силу замечания 1.3 $kx = 0$ для всякого $x \in F$, что невозможно, поскольку $\operatorname{char} F = 0$. Следовательно, $a \neq 0$ и потому существует элемент a^{-1}. Используя (1.1), получаем, что $kp'g = k(ep'g) = (ke)p'g = ap'g$. Следовательно, $ap'g = kp'g = ph$. Умножая обе части равенства $ap'g = ph$ слева на a^{-1}, получаем, что $p'g = a^{-1}(ph) = (a^{-1}h)p$. Это означает, что $p \mid p'g$. Но выше было показано, что это не так. □

Следующее утверждение обобщает следствие 10.4.

Следствие 13.6. *Пусть f — многочлен степени > 0 над полем F характеристики 0, а d — наибольший общий делитель многочленов f и f'. Многочлены f и $g = \frac{f}{d}$ имеют одни и те же неприводимые множители, причем второй из них не имеет кратных неприводимых множителей.*

Доказательство. Ясно, что все неприводимые множители многочлена g являются неприводимыми множителями многочлена f. А в силу предложения 13.5 все неприводимые множители многочлена f являются неприводимыми множителями кратности 1 многочлена g. □

Это следствие (при $F = \mathbb{R}$) используется в математическом анализе при интегрировании дробно-рациональных функций (определение последних дано в начале § 16).

Приведем теперь алгоритм нахождения многочленов вида $d_i(f)$. Процесс вычисления этих многочленов называется *отделением кратных множителей*.

Алгоритм 13.7 (алгоритм отделения кратных множителей)**.** Дан многочлен f степени > 0 над полем характеристики 0. Пусть $k = \max\{i \mid d_i(f) \neq 1\}$. Требуется найти многочлены $d_j(f)$ для всех $j = 1, 2, \ldots, k$. Полагаем $f_0 = \frac{f}{\ell c(f)}$ и $i = 1$. Обозначаем через f_i наибольший общий делитель многочленов f_{i-1} и f'_{i-1}. Если $\deg f_i > 0$, увеличиваем значение i на единицу и повторяем вычисление многочлена f_i. Продолжаем этот процесс до тех пор, пока не окажется, что $\deg f_i = 0$. В тот момент, когда это равенство оказывается выполненным, полагаем $k = i$, $d_j(f) = \frac{f_{j-1} f_{j+1}}{f_j^2}$ для всех $j = 1, 2, \ldots, k-1$ и $d_k(f) = f_{k-1}$. На этом работа алгоритма завершается.

Обоснование алгоритма 13.7. Работа алгоритма завершится через конечное число шагов, поскольку $\deg f_0 > \deg f_1 > \deg f_2 > \cdots$. Напомним, что выполнено равенство (13.1), где $\alpha = \ell c(f)$. Следовательно, $f_0 = d_1(f) d_2^2(f) d_3^3(f) \cdots d_k^k(f)$, а из предложения 13.5 вытекает, что $f_1 = d_2(f) d_3^2(f) \cdots d_k^{k-1}(f)$, $f_2 = d_3(f) \cdots d_k^{k-2}(f)$, $\ldots$, $f_{k-1} = d_k(f)$ и $f_k = 1$. Мы доказали, что $d_k(f) = f_{k-1}$. Кроме того, для всякого $m = 0, 1, \ldots, k-1$ выполнено равенство $\frac{f_m}{f_{m+1}} = d_{m+1}(f) d_{m+2}(f) \cdots d_k(f)$, и потому

$$d_j(f) = \frac{d_j(f) d_{j+1}(f) \cdots d_k(f)}{d_{j+1}(f) d_{j+2}(f) \cdots d_k(f)} = \frac{f_{j-1}}{f_j} : \frac{f_j}{f_{j+1}} = \frac{f_{j-1} f_{j+1}}{f_j^2}$$

для всякого $j = 1, 2, \ldots, k-1$. □

§ 14. Многочлены, неприводимые над полями $\mathbb{C}$ и $\mathbb{R}$

Из следствия 9.2 и замечания 12.4 вытекает следующее утверждение.

Предложение 14.1. *Многочленами, неприводимыми над полем* $\mathbb{C}$*, являются линейные многочлены и только они.* □

Предложение 14.2. *Многочленами, неприводимыми над полем* $\mathbb{R}$*, являются линейные многочлены, многочлены степени* 2 *с отрицательными дискриминантами и только они.*

Доказательство. Линейные многочлены над любым полем неприводимы (см. замечание 12.4). Как хорошо известно, квадратные трехчлены с отрицательным дискриминантом действительных корней не имеют. Поэтому их неприводимость над полем $\mathbb{R}$ вытекает из предложения 12.5. Осталось доказать, что других неприводимых над $\mathbb{R}$ многочленов не существует, т. е. что любой многочлен степени > 0 над полем $\mathbb{R}$ разлагается на множители с действительными коэффициентами, каждый из которых либо линеен, либо является многочленом степени 2 с отрицательным дискриминантом.

Пусть $f(x) \in \mathbb{R}[x]$ и $\deg f > 0$. В силу следствия 9.2 $f = \alpha(x - \gamma_1)\cdots(x - \gamma_n)$, где $\alpha, \gamma_1, \ldots, \gamma_n \in \mathbb{C}$. При этом $\alpha \in \mathbb{R}$, поскольку $f \in \mathbb{R}[x]$. Если $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$, то все доказано. Поэтому без ограничения общности можно считать, что $\gamma_1, \ldots, \gamma_m \in \mathbb{R}$ и $\gamma_{m+1}, \ldots, \gamma_n \notin \mathbb{R}$ для некоторого $m < n$. Для всякого $k = m+1, \ldots, n$ положим $\gamma_k = \alpha_k + \beta_k i$. Ясно, что $\beta_k \neq 0$. По лемме 9.6 число $\overline{\gamma_k} = \alpha_k - \beta_k i$ также является корнем многочлена f, причем кратности корней γ_k и $\overline{\gamma_k}$ совпадают. Это означает, что набор чисел $\gamma_{m+1}, \ldots, \gamma_n$ можно переписать в виде γ_{m+1}, $\overline{\gamma_{m+1}}$, γ_{m+2}, $\overline{\gamma_{m+2}}$, $\ldots$, $\gamma_{m+\ell}$, $\overline{\gamma_{m+\ell}}$ для некоторого ℓ. Следовательно, для всякого $k = m+1, m+2, \ldots, m+\ell$, многочлен f делится на

$$\begin{aligned}(x - \gamma_k)(x - \overline{\gamma_k}) &= (x - \alpha_k - \beta_k i)(x - \alpha_k + \beta_k i) = \\ &= (x - \alpha_k)^2 - (\beta_k i)^2 = \\ &= x^2 - 2\alpha_k x + \alpha_k^2 + \beta_k^2.\end{aligned}$$

Осталось заметить, что полученный квадратный трехчлен имеет отрицательный дискриминант. В самом деле, $4\alpha_k^2 - 4(\alpha_k^2 + \beta_k^2) = -4\beta_k^2 < 0$, поскольку $\beta_k \neq 0$. □

§ 15. Многочлены, неприводимые над полем $\mathbb{Q}$

Простого и удобного для применения критерия неприводимости многочленов над полем $\mathbb{Q}$ не существует. Есть только весьма сильное достаточное условие. Чтобы доказать его, нам понадобятся некоторые вспомогательные понятия и результаты.

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$ — многочлен над кольцом $\mathbb{Z}$. Обозначим через $d(f)$ наибольший общий делитель чисел $\alpha_n, \alpha_{n-1}, \ldots, \alpha_0$. Если $d(f) = 1$, то многочлен f называется *примитивным*. Если в многочлене $f \in \mathbb{Z}[x]$ вынести за скобки наибольший общий делитель всех его коэффициентов, то в скобках будет стоять примитивный многочлен над $\mathbb{Z}$. Таким образом, *произвольный многочлен* $f \in \mathbb{Z}[x]$ *представим в виде* $f = d(f) \cdot f_0$, *где* f_0 — *примитивный многочлен над* $\mathbb{Z}$.

Лемма 15.1 (лемма Гаусса). *Произведение двух примитивных многочленов над кольцом* $\mathbb{Z}$ *примитивно.*

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ и $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ — многочлены над кольцом $\mathbb{Z}$. Предположим, что многочлены f и g примитивны, а их произведение не примитивно. Следовательно, существует простое число p, делящее $d(fg)$. В силу примитивности многочленов f и g существуют индексы s и t такие, что p не делит a_s и b_t. Пусть s и t — минимальные индексы с таким свойством. Коэффициент при x^{s+t} в многочлене fg будет равен

$$\begin{aligned} c_{s+t} = a_s b_t \;&+\; a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots + \\ &+\; a_{s-1}b_{t+1} + a_{s-2}b_{t+2} + \cdots . \end{aligned} \tag{15.1}$$

В силу выбора индексов s и t коэффициенты a_{s-i} и b_{t-i} при $i > 0$ делятся на p, а из того, что $p \mid d(fg)$, вытекает, что $p \mid c_{s+t}$. Отсюда и из равенства (15.1) вытекает, что $p \mid a_s b_t$. Но тогда, будучи простым, число p делит либо a_s, либо b_t, что противоречит выбору числа p и индексов s и t. □

Предложение 15.2. *Многочлен* $f \in \mathbb{Z}[x]$ *неприводим над* $\mathbb{Z}$ *тогда и только тогда, когда он неприводим над* $\mathbb{Q}$.

Доказательство. Достаточность очевидна.

Необходимость. Предположим, что f неприводим над $\mathbb{Z}$, но приводим над $\mathbb{Q}$. Пусть $f = gh$, где $g, h \in \mathbb{Q}[x]$ и $\deg g, \deg h < \deg f$. Тогда $\deg g, \deg h > 0$. Обозначим через a наименьшее общее кратное знаменателей всех коэффициентов многочлена g, а через b — наименьшее общее кратное знаменателей всех коэффициентов многочлена h. Тогда $gh = \frac{1}{ab} \cdot g_1 h_1$, где g_1 и h_1 — многочлены над $\mathbb{Z}$. Теперь положим $c = d(g_1)$ и $d = d(h_1)$. Тогда $g_1 = cg_2$ и $h_1 = dh_2$, где g_2 и h_2 — примитивные многочлены над $\mathbb{Z}$. Объединяя сказанное, имеем $f = gh = \frac{1}{ab} \cdot g_1 h_1 = \frac{cd}{ab} \cdot g_2 h_2$. Поскольку все коэффициенты многочлена f являются целыми числами, ab делит все коэффициенты многочлена cdg_2h_2, т. е. $ab \mid cd \cdot d(g_2h_2)$. В силу леммы Гаусса многочлен g_2h_2 примитивен. Это означает, что $d(g_2h_2) = 1$ и потому $ab \mid cd$. Положим $\frac{cd}{ab} = k$. В силу сказанного выше k — целое число и $f = (kg_2)h_2$. Это означает, что многочлен f приводим над $\mathbb{Z}$ вопреки его выбору. □

Если $f \in \mathbb{Q}[x]$, то, умножив многочлен f на наименьшее общее кратное знаменателей всех его коэффициентов, мы получим многочлен g с целыми коэффициентами. Ясно, что многочлен g неприводим над $\mathbb{Q}$ тогда и только тогда, когда f неприводим над $\mathbb{Q}$. Таким образом, *при изучении многочленов, неприводимых над $\mathbb{Q}$, можно ограничиться рассмотрением многочленов над $\mathbb{Q}$ с целыми коэффициентами.*

Следующее утверждение дает упомянутое выше достаточное условие неприводимости многочлена над полем $\mathbb{Q}$, которое по традиции называется *критерием Эйзенштейна.* Ниже в данном параграфе будет приведен пример, показывающий, что критерий Эйзенштейна не является необходимым условием неприводимости многочлена над $\mathbb{Q}$. Таким образом, название этого утверждения противоречит общепринятому в математике пониманию слова «критерий» как «необходимое и достаточное условие», и его следовало бы называть не критерием, а признаком Эйзенштейна или даже скорее признаком Шёнемана, поскольку оно было впервые доказано Шёнеманом в 1846 г. и переоткрыто Эйзенштейном спустя четыре года. Несмотря на все это, название «критерий Эйзенштейна» общепринято и потому мы будем им пользоваться.

Теорема 15.3 (критерий Эйзенштейна). *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *— многочлен с целыми коэффициентами над полем* $\mathbb{Q}$ *такой, что* $\deg f > 0$*, и существует простое число* p *такое, что* a_n *не делится на* p*,* $a_{n-1}, \ldots, a_0$ *делятся на* p *и* a_0 *не делится на* p^2*. Тогда* f *неприводим над* $\mathbb{Q}$*.*

Доказательство. Предположим, что f приводим над $\mathbb{Q}$. Тогда в силу предложения 15.2 f приводим над $\mathbb{Z}$. Следовательно, f представим в виде $f = gh$, где $g(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0$ и $h(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0$ — многочлены степени > 0 над $\mathbb{Z}$. Ясно, что $a_0 = b_0 c_0$. Поскольку a_0 делится на p, но не делится на p^2, из простоты числа p вытекает, что p делит одно из чисел b_0 и c_0, но не оба этих числа одновременно. Предположим для определенности, что p делит b_0, но не делит c_0. Если p делит все коэффициенты многочлена g, то оно делит и все коэффициенты многочлена f, включая a_n. Следовательно, существует индекс i такой, что $p \nmid b_i$. Пусть i — минимальный индекс с таким свойством. Ясно, что $\deg g < \deg f$ и потому $i \leqslant k < n$. В частности, $p \mid a_i$. По определению произведения многочленов имеем $a_i = b_i c_0 + b_{i-1}c_1 + b_{i-2}c_2 + \cdots$. Поскольку p делит a_i и b_j для всех $j < i$, из этого равенства вытекает, что $p \mid b_i c_0$. Но это невозможно, так как p не делит ни b_i, ни c_0. □

Всякий неприводимый многочлен над полем $\mathbb{C}$ имеет степень 1 (см. предложение 14.1), а всякий неприводимый многочлен над полем $\mathbb{R}$ — степень $\leqslant 2$ (см. предложение 14.2). С этими двумя фактами резко контрастирует следующее утверждение.

Следствие 15.4. *Для любого натурального числа* n *существует неприводимый над полем* $\mathbb{Q}$ *многочлен степени* n*.*

Доказательство. Достаточно учесть, что при любом n многочлен $x^n + 2$ удовлетворяет посылке критерия Эйзенштейна при $p = 2$. □

В качестве любопытного «побочного» следствия из критерия Эйзенштейна отметим следующий факт, обычно доказываемый средствами элементарной математики.

Следствие 15.5. *Для всякого натурального числа* $n > 1$ *и всякого простого числа* p *число* $\sqrt[n]{p}$ *иррационально.*

Доказательство. Если число $\sqrt[n]{p}$ рационально, то оно является рациональным корнем многочлена $x^n - p$. В силу замечания 12.3 отсюда вытекает, что многочлен $x^n - p$ приводим над полем $\mathbb{Q}$. Но из критерия Эйзенштейна вытекает, что это не так. □

В частности, из следствия 15.5 вытекает иррациональность числа $\sqrt{2}$.

Приведем теперь обещанный выше пример, показывающий, что критерий Эйзенштейна не является необходимым условием неприводимости многочлена над полем $\mathbb{Q}$.

Пример 15.6 (пример неприводимого над полем $\mathbb{Q}$ многочлена, не удовлетворяющего посылке критерия Эйзенштейна)**.** Рассмотрим многочлен $f(x) = x^3 + 4$. Пользуясь следствием 11.2, легко проверить, что этот многочлен не имеет рациональных корней. Из предложения 12.5 вытекает теперь, что он неприводим над $\mathbb{Q}$. В то же время $f(x)$ не удовлетворяет посылке критерия Эйзенштейна, поскольку единственное простое число, которое делит свободный член многочлена $f(x)$, это число 2, и свободный член $f(x)$ делится на квадрат этого числа.

Отсутствие критерия приводимости многочлена над полем $\mathbb{Q}$ частично компенсируется существованием алгоритмов, позволяющих по произвольному многочлену над $\mathbb{Q}$ установить, приводим он над $\mathbb{Q}$ или нет. Приведем один из таких алгоритмов, называемый *алгоритмом Кронекера.* Отметим, что этот алгоритм впервые был опубликован Шубертом в 1793 г. и переоткрыт Кронекером почти 100 лет спустя — в 1882 г.

Алгоритм 15.7 (алгоритм Кронекера)**.** Дан многочлен f степени > 0 над полем $\mathbb{Q}$. Требуется установить, является ли он приводимым над $\mathbb{Q}$. Если $\deg f = 1$, то алгоритм устанавливает, что f неприводим над $\mathbb{Q}$, и завершает работу. Далее считаем, что $\deg f > 1$. Если не все коэффициенты многочлена f являются целыми числами, умножим f на наименьшее общее кратное знаменателей всех его коэффициентов. Ясно, что на приводимость или неприводимость f это не влияет. Все коэффициенты полученного многочлена являются целыми числами. Поэтому можно считать, что f — многочлен с целыми коэффициентами. Положим

$m = \left[\frac{\deg f}{2}\right]$ (через $[x]$ обозначается целая часть действительного числа x). Пусть $x_0, x_1, \ldots, x_m$ — произвольные попарно различные целые числа. Вычисляем последовательно числа $f(x_0)$, $f(x_1)$, $\ldots$, $f(x_m)$. Ясно, что все эти числа — целые. Если оказывается, что $f(x_j) = 0$ для некоторого $j \in \{1, 2, \ldots, m\}$, то алгоритм делает вывод, что многочлен f приводим над $\mathbb{Q}$, и завершает работу. Далее считаем, что $f(x_j) \neq 0$ для всех $j = 0, 1, \ldots, m$. Для всякого набора чисел $(n_0, n_1, \ldots, n_m)$ такого, что $n_j \mid f(x_j)$ для всех $j = 0, 1, \ldots, m$, обозначим через $g_{(n_0,n_1,\ldots,n_m)}$ интерполяционный многочлен Лагранжа, соответствующий набору пар (x_0, n_0), (x_1, n_1), $\ldots$, (x_m, n_m). Число многочленов вида $g_{(n_0,n_1,\ldots,n_m)}$ конечно, поскольку существует лишь конечное число наборов чисел $(n_0, n_1, \ldots, n_m)$ таких, что $n_j \mid f(x_j)$ для всех $j = 0, 1, \ldots, m$. Обозначим эти многочлены через $g_1, g_2, \ldots, g_k$. Перебираем последовательно многочлены $g_1, g_2, \ldots, g_k$. Если найдется $i \in \{1, 2, \ldots, k\}$ такое, что $\deg g_i > 0$ и $g_i \mid f$, то алгоритм устанавливает, что многочлен f приводим над $\mathbb{Q}$, и завершает работу. Если же для всякого $i = 1, 2, \ldots, k$ либо $\deg g_i = 0$, либо $g_i \nmid f$, то алгоритм делает вывод, что многочлен f неприводим над $\mathbb{Q}$, и завершает работу.

Обоснование алгоритма Кронекера. В силу замечаний 12.3 и 12.4 можно считать, что $\deg f > 1$ и $f(x_j) \neq 0$ для всех $j = 0, 1, \ldots, m$. Все коэффициенты многочлена f можно считать целыми числами. Предположим, что f приводим над $\mathbb{Q}$. В силу предложения 15.2 f приводим и над $\mathbb{Z}$. Следовательно, существуют многочлены $g, h \in \mathbb{Z}[x]$ такие, что $f = gh$ и $0 < \deg g, \deg h < \deg f$. Положим $m = \left[\frac{\deg f}{2}\right]$. Если $\deg g, \deg h > m$, то $\deg f = \deg g + \deg h > \deg f$. Поэтому без ограничения общности можно считать, что $\deg g \leqslant m$. Пусть $\xi \in \mathbb{Z}$. Тогда $f(\xi) = g(\xi) \cdot h(\xi)$. Следовательно, если $g(\xi) = 0$, то и $f(\xi) = 0$, а если $g(\xi) \neq 0$, то $g(\xi) \mid f(\xi)$. Следовательно, $g(x_j) \neq 0$ и $g(x_j) \mid f(x_j)$ для всех $j = 0, 1, \ldots, m$. Для всякого $j = 0, 1, \ldots, m$ положим $n_j = g(x_j)$. Тогда $n_j \mid f(x_j)$ и $g(x_j) = g_{(n_0,n_1,\ldots,n_m)}(x_j)$ для всех $j = 0, 1, \ldots, m$. Из теоремы 6.1 вытекает, что $g = g_{(n_0,n_1,\ldots,n_m)}$. Итак, если f приводим над $\mathbb{Q}$, то один из многочленов вида $g_{(n_0,n_1,\ldots,n_m)}$ делит f и имеет степень > 0. Следовательно, если все многочлены такого вида либо не делят f, либо имеют степень 0, то f неприводим над $\mathbb{Q}$.

Обратно, предположим, что g — многочлен вида $g_{(n_0,n_1,\ldots,n_m)}$, $g \mid f$ и $\deg g > 0$. Ясно, что $\deg g \leqslant m < \deg f$. Из формул (6.3) и (6.4) вытекает, что $g \in \mathbb{Q}[x]$. Но тогда и $h = \frac{f}{g} \in \mathbb{Q}[x]$. Ясно, что $\deg h = \deg f - \deg g < \deg f$. Следовательно, многочлен $f = gh$ приводим над $\mathbb{Q}$. □

Если многочлен f приводим над полем $\mathbb{Q}$, то алгоритм Кронекера находит многочлен g над $\mathbb{Q}$ такой, что $g \mid f$ и $0 < \deg g < \deg f$. Разделив f на g, мы найдем многочлен h над $\mathbb{Q}$ такой, что $f = gh$ и $0 < \deg g, \deg h < \deg f$. Если какой-то из многочленов g и h приводим над $\mathbb{Q}$, то, установив этот факт, мы представим этот многочлен в виде произведения многочленов над $\mathbb{Q}$ меньшей степени. Продолжая этот процесс, мы в конце концов получим разложение f на неприводимые множители над полем $\mathbb{Q}$.

§ 16. Рациональные дроби

В этом параграфе мы применяем результат о разложимости произвольного многочлена в произведение неприводимых множителей для изучения некоторого обобщения понятия многочлена. *Рациональной дробью* или *дробно-рациональной функцией* над полем F называется функция вида $\frac{f}{g}$, где $f, g \in F[x]$ и $g \neq o$. Очевидно, что произвольный многочлен f является рациональной дробью вида $\frac{f}{1}$. Рациональная дробь $\frac{f}{g}$ называется *правильной*, если $\deg f < \deg g$. Рациональная дробь $\frac{f}{g}$ называется *простейшей*, если существуют многочлен p, неприводимый над полем F, и натуральное число n такие, что $g = p^n$ и $\deg f < \deg p$. Очевидно, что всякая простейшая дробь является правильной.

Замечание 16.1. *Любая рациональная дробь над произвольным полем может быть представлена, причем единственным образом, в виде суммы многочлена и правильной рациональной дроби.*

Доказательство. Пусть $\frac{f}{g}$ — рациональная дробь. Разделим f на g с остатком: $f = qg + r$ для некоторых многочленов q и r, причем $\deg r < \deg g$. Тогда $\frac{f}{g} = \frac{qg+r}{g} = q + \frac{r}{g}$, причем дробь $\frac{r}{g}$ является правильной. Представление дроби $\frac{f}{g}$ в виде суммы многочлена q и

правильной дроби $\frac{r}{g}$ единственно ввиду единственности частного q и остатка r (см. теорему 4.1). □

Основным результатом параграфа является следующее утверждение, которое играет важную роль в курсе математического анализа при вычислении интегралов от дробно-рациональных функций.

Теорема 16.2. *Любая правильная рациональная дробь над произвольным полем может быть представлена, причем единственным образом, в виде суммы простейших дробей.*

Доказательство. Существование. Пусть $\frac{f}{g}$ — правильная рациональная дробь. Без ограничения общности можно считать, что $\ell c(g) = 1$ (в противном случае можно разделить каждый из многочленов f и g на $\ell c(g)$). Пусть $g = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ — разложение многочлена g на неприводимые множители. Доказательство того, что дробь $\frac{f}{g}$ может быть представлена в виде суммы простейших дробей, разобьем на два шага. На первом шаге мы докажем, что дробь $\frac{f}{g}$ может быть представлена как сумма правильных рациональных дробей, у каждой из которых знаменатель есть степень неприводимого многочлена. На втором шаге будет доказано, что правильную рациональную дробь, у которой знаменатель есть степень неприводимого многочлена, можно представить как сумму простейших дробей.

Шаг 1. Докажем индукцией по n, что

$$\frac{f}{g} = \frac{f_1}{p_1^{k_1}} + \frac{f_2}{p_2^{k_2}} + \cdots + \frac{f_n}{p_n^{k_n}} \tag{16.1}$$

для некоторых многочленов $f_1, f_2, \ldots, f_n$ таких, что $\deg f_i < \deg p_i^{k_i}$ для всех $i = 1, 2, \ldots, n$.

База индукции очевидна: если $n = 1$, то равенство (16.1) выполнено при $f_1 = f$.

Шаг индукции. Пусть $n > 1$. Положим $g_1 = p_1^{k_1}$ и $g_2 = p_2^{k_2} \cdots p_n^{k_n}$. Многочлены g_1 и g_2 взаимно просты. В силу следствия 5.4 существуют многочлены u и v такие, что $ug_1 + vg_2 = 1$. Следовательно,

$f = fug_1 + fvg_2$. Разделим fu на g_2 с остатком: $fu = qg_2 + r$, где $\deg r < \deg g_2$. Имеем:

$$f = fug_1 + fvg_2 = (qg_2 + r)g_1 + fvg_2 = rg_1 + (qg_1 + fv)g_2.$$

Положим $f_1 = qg_1 + fv$. Тогда $f = rg_1 + f_1g_2$, откуда

$$\frac{f}{g} = \frac{f_1g_2 + rg_1}{g_1g_2} = \frac{f_1}{g_1} + \frac{r}{g_2}.$$

Напомним, что $g_2 = p_2^{k_2} \cdots p_n^{k_n}$ и $\deg r < \deg g_2$. Это позволяет применить к дроби $\frac{r}{g_2}$ предположение индукции и заключить, что

$$\frac{r}{g_2} = \frac{f_2}{p_2^{k_2}} + \cdots + \frac{f_n}{p_n^{k_n}}$$

для некоторых многочленов $f_2, \ldots, f_n$ таких, что $\deg f_i < \deg p_i^{k_i}$ для всех $i = 2, \ldots, n$. Для того чтобы завершить шаг 1, осталось проверить, что $\deg f_1 < \deg g_1$. Очевидно, что это равносильно неравенству $\deg f_1 + \deg g_2 < \deg g_1 + \deg g_2$, которое мы и докажем. Учитывая, что $f - rg_1 = f_1g_2$, имеем:

$$\deg f_1 + \deg g_2 = \deg(f_1g_2) = \deg(f - rg_1) \leqslant \max\bigl\{\deg f, \deg(rg_1)\bigr\}.$$

Поскольку $\deg f < \deg g = \deg(g_1g_2) = \deg g_1 + \deg g_2$ и $\deg(rg_1) = \deg r + \deg g_1 < \deg g_2 + \deg g_1$, получаем, что

$$\deg f_1 + \deg g_2 \leqslant \max\bigl\{\deg f, \deg(rg_1)\bigr\} < \deg g_1 + \deg g_2.$$

Шаг 2. Осталось доказать, что каждое из слагаемых, стоящих в правой части равенства (16.1), представимо в виде суммы простейших дробей. Иными словами, требуется доказать, что в таком виде представима всякая рациональная дробь вида $\frac{h}{w^k}$, где w — неприводимый многочлен и $\deg h < \deg w^k$. Проведем доказательство индукцией по k.

База индукции очевидна: если $k = 1$, то $\deg h < \deg w$ и дробь $\frac{h}{w^k} = \frac{h}{w}$ является простейшей.

Шаг индукции. Пусть теперь $k > 1$. Разделим h на w с остатком: $h = qw + r$, где $\deg r < \deg w$. Тогда

$$\frac{h}{w^k} = \frac{qw + r}{w^k} = \frac{q}{w^{k-1}} + \frac{r}{w^k}.$$

Дробь $\frac{r}{w^k}$ является простейшей, поскольку $\deg r < \deg w$. Осталось доказать, что дробь $\frac{q}{w^{k-1}}$ представима в виде суммы простейших дробей. По предположению индукции для этого достаточно убедиться в том, что эта дробь является правильной. В самом деле, поскольку $\deg r < \deg w \leqslant \deg qw$, из равенства $h = qw + r$ вытекает, что $\deg h = \deg qw$. Следовательно, $\deg qw = \deg h < \deg w^k$. Иными словами, $\deg q + \deg w < k \deg w$, откуда $\deg q < (k-1)\deg w = \deg w^{k-1}$. Мы доказали, что дробь $\frac{q}{w^{k-1}}$ является правильной.

Единственность. Предположим, что дробь $\frac{f}{g}$ двумя разными способами представлена в виде суммы простейших дробей:

$$\frac{f}{g} = \frac{a_1}{p_1^{k_1}} + \cdots + \frac{a_m}{p_m^{k_m}} \quad \text{и} \quad \frac{f}{g} = \frac{b_1}{q_1^{\ell_1}} + \cdots + \frac{b_n}{q_n^{\ell_n}}$$

(имеется в виду, что в правых частях каждого из этих равенств все знаменатели попарно различны, но некоторые из многочленов $p_1, \ldots, p_m$, равно как и некоторые из многочленов $q_1, \ldots, q_n$, могут совпадать). Тогда

$$\frac{a_1}{p_1^{k_1}} + \cdots + \frac{a_m}{p_m^{k_m}} = \frac{b_1}{q_1^{\ell_1}} + \cdots + \frac{b_n}{q_n^{\ell_n}}. \tag{16.2}$$

Разумеется, все слагаемые в обеих частях этого равенства можно считать ненулевыми. Если левая и правая части равенства (16.2) содержат одно и то же слагаемое, вычеркнем его из обеих частей равенства. Проделаем это для всех пар одинаковых слагаемых. Если после этого получится равенство $0 = 0$, значит, исходно мы имели два совпадающих разложения дроби $\frac{f}{g}$ в сумму простейших дробей. В этом случае доказательство завершено.

Предположим, что в результате описанного выше процесса в равенстве (16.2) будут вычеркнуты не все слагаемые. Перенеся все оставшиеся в правой части равенства слагаемые в левую часть с обратным знаком и изменив обозначения, мы получим равенство вида

$$\frac{s_1}{t_1} + \cdots + \frac{s_r}{t_r} = 0. \tag{16.3}$$

Все слагаемые в левой части этого равенства являются простейшими дробями. В частности, $t_1 = p^k$ для некоторого неприводимого

многочлена p и некоторого числа k. Если $r = 1$, то единственное слагаемое в левой части равенства (16.3), совпадающее, с точностью до знака, с одним из слагаемых равенства (16.2), равно нулю. Но это противоречит нашей договоренности о том, что все слагаемые в обеих частях равенства (16.2) являются ненулевыми. Следовательно, $r > 1$.

Поменяв при необходимости слагаемые в левой части равенства (16.3) местами, можно добиться того, чтобы каждый из многочленов $t_2, t_3, \ldots, t_r$ имел либо вид p^m, где $m < k$, либо вид q^ℓ, где q — неприводимый многочлен, отличный от p. Обозначим через Q общий знаменатель всех дробей, стоящих в левой части равенства (16.3), у которых знаменатель имеет второй из указанных только что видов. Из п. 3) предложения 5.5 вытекает, что многочлены p и Q взаимно просты. Умножим обе части равенства (16.3) на $p^{k-1}Q$. Получим равенство вида $\frac{s_1 Q}{p} + R = 0$, где R — некоторый многочлен. Следовательно, $s_1 Q = -pR$. Таким образом, $p \mid s_1 Q$. Поскольку p взаимно прост с Q, из п. 2) предложения 5.5 вытекает, что $p \mid s_1$. Но это невозможно, так как дробь $\frac{s_1}{p^k}$ является простейшей и потому $\deg s_1 < \deg p$. □

Решение типовых задач

Основными типами задач по теме данной главы являются следующие:

1) задачи об отделении кратных множителей;
2) задачи о разложении многочлена на неприводимые множители над одним из полей $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$;
3) задачи о приводимости или неприводимости данного многочлена над полем $\mathbb{Q}$;
4) задачи о представлении правильной рациональной дроби в виде суммы простейших дробей над одним из полей $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$.

Решим задачу первого типа.

Задача IV.1. Отделить кратные множители многочлена $f(x) = x^6 + x^4 - x^2 - 1$ и разложить его на неприводимые множители над полем $\mathbb{R}$.

Решение. Мы используем ниже обозначения, введенные при изложении алгоритма отделения кратных множителей. Строим последовательность многочленов $f_0, f_1, \ldots, f_k$. Имеем $f_0 = f = x^6 + x^4 - x^2 - 1$ и $f_0' = 6x^5 + 4x^3 - 2x$. С помощью алгоритма Евклида вычислим наибольший общий делитель многочленов f_0 и f_0'. Делим f_0 на f_0'. Получаем $f_0 = q_1 f_0' + r_1$, где $q_1 = \frac{1}{6}x$ и $r_1 = \frac{1}{3}x^4 - \frac{2}{3}x^2 - 1$. Поскольку $r_1 \neq o$, делим f_0' на r_1. Получаем $f_0' = q_2 r_1 + r_2$, где $q_2 = 18x$ и $r_2 = 16x^3 + 16x$. Поскольку $r_2 \neq o$, делим r_1 на r_2. Получаем $r_1 = q_3 r_2 + r_3$, где $q_3 = \frac{1}{48}x$ и $r_2 = -x^2 - 1$. Поскольку $r_3 \neq o$, делим r_2 на r_3. Получаем $r_2 = q_4 r_4$, где $q_4 = -16x$. Поскольку остаток при последнем делении равен o, работа алгоритма Евклида завершена.

Многочлен f_1 ассоциирован с последним ненулевым остатком, т. е. с многочленом $-x^2 - 1$. Мы можем считать, что $f_1 = x^2 + 1$. Следовательно, $f_1' = 2x$. С помощью алгоритма Евклида вычислим наибольший общий делитель многочленов f_1 и f_1'. Делим f_1 на f_1'. Получаем $f_1 = q_1 f_1' + r_1$, где $q_1 = \frac{1}{2}x$ и $r_1 = 1$. Ясно, что остаток от деления f_1' на r_1 равен o. Следовательно, работа алгоритма Евклида завершена. Мы получили, что $f_2 = 1$. Следовательно, $k = 2$,

$$d_1(f) = \frac{f_0 f_2}{f_1^2} = \frac{x^6 + x^4 - x^2 - 1}{x^4 + 2x^2 + 1} = x^2 - 1$$

и $d_2(f) = f_1 = x^2 + 1$.

Осталось разложить многочлен f на неприводимые множители над полем $\mathbb{R}$. В силу (13.1) выполнено равенство $f = d_1(f) d_2^2(f)$. Разложение многочлена $d_1(f)$ на неприводимые множители над $\mathbb{R}$ имеет вид $d_1(f) = (x-1)(x+1)$, а многочлен $d_2(f)$ неприводим над $\mathbb{R}$. Следовательно, разложение f на неприводимые множители над полем $\mathbb{R}$ имеет вид $f = (x-1)(x+1)(x^2+1)^2$.

Ответ. $d_1(f) = x^2 - 1$, $d_2(f) = x^2 + 1$, $f = (x-1)(x+1)(x^2+1)^2$.

Рассмотрим теперь задачу второго типа.

Задача IV.2. Разложить многочлен $f(x) = x^4 - x^2 - 2$ на неприводимые множители:

а) над полем $\mathbb{C}$;

б) над полем $\mathbb{R}$;

в) над полем $\mathbb{Q}$.

Решение. а) Найдем все комплексные корни многочлена $f(x)$. Для этого надо решить уравнение $x^4 - x^2 - 2 = 0$. Это биквадратное уравнение. Сделав замену $t = x^2$, получим квадратное уравнение $t^2 - t - 2 = 0$, имеющее два корня: 2 и -1. В первом случае получаем уравнение $x^2 = 2$, имеющее два действительных (а значит, и комплексных) корня: $x_1 = \sqrt{2}$ и $x_2 = -\sqrt{2}$. Во втором случае имеем уравнение $x^2 = -1$, имеющее два комплексных корня: $x_3 = i$ и $x_4 = -i$. Следовательно, разложение многочлена $f(x)$ на неприводимые множители над полем $\mathbb{C}$ имеет вид $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$.

б) Перемножив две последние скобки из правой части полученного только что равенства, получаем разложение $f(x)$ на неприводимые множители над полем $\mathbb{R}$: $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$.

в) Поскольку числа $\sqrt{2}$ и $-\sqrt{2}$ иррациональны, полученное только что равенство не является разложением $f(x)$ на множители над полем $\mathbb{Q}$. Чтобы получить последнее, перемножим первые две скобки из правой части этого равенства. Получим $f(x) = (x^2-2)(x^2+1)$. Многочлен x^2-2 неприводим над полем $\mathbb{Q}$, поскольку он удовлетворяет посылке критерия Эйзенштейна при $p = 2$. А многочлен x^2+1 неприводим над $\mathbb{Q}$ потому, что он неприводим уже над $\mathbb{R}$. Таким образом, равенство $f(x) = (x^2 - 2)(x^2 + 1)$ является разложением $f(x)$ на неприводимые множители над полем $\mathbb{Q}$.

Ответ. а) $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$; б) $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$; в) $f(x) = (x^2 - 2)(x^2 + 1)$.

Продемонстрируем, как с помощью разложения многочленов на неприводимые множители можно найти наибольший общий делитель многочленов.

Задача IV.3. Найти наибольший общий делитель многочленов $f(x) = x^4 - x^3 - x + 1$ и $g(x) = x^4 + x^3 - x - 1$.

Решение. Разложим многочлен $f(x)$ на неприводимые множители над полем $\mathbb{R}$. Заметим, что $f(1) = 1 - 1 - 1 + 1 = 0$. Следовательно, $f(x)$ делится на $x - 1$. Разделим $f(x)$ на $x - 1$ по схеме Горнера. Соответствующая таблица имеет вид

	1	−1	0	−1	1
1	1	0	0	−1	0

.

Следовательно, $f(x) = (x-1)(x^3-1)$. Воспользовавшись формулой разности кубов, получаем, что $x^3 - 1 = (x-1)(x^2+x+1)$ и потому $f(x) = (x-1)^2(x^2+x+1)$. Поскольку квадратный трехчлен x^2+x+1 имеет отрицательный дискриминант, он неприводим над полем $\mathbb{R}$ и потому равенство $f(x) = (x-1)^2(x^2+x+1)$ является разложением многочлена $f(x)$ на неприводимые множители над полем $\mathbb{R}$.

Теперь разложим на неприводимые множители над полем $\mathbb{R}$ многочлен $g(x)$. Заметим, что $g(1) = 1 + 1 - 1 - 1 = 0$. Следовательно, $g(x)$ делится на $x - 1$. Разделим $g(x)$ на $x - 1$ по схеме Горнера. На этот раз таблица имеет вид

	1	1	0	−1	−1
1	1	2	2	1	0

.

Следовательно, $g(x) = (x-1)g_1(x)$, где $g_1(x) = x^3 + 2x^2 + 2x + 1$. Теперь заметим, что $g_1(-1) = -1 + 2 - 2 + 1 = 0$. Следовательно, $g_1(x)$ делится на $x + 1$. Разделим $g_1(x)$ на $x + 1$ по схеме Горнера. Соответствующая таблица имеет вид

	1	2	2	1
−1	1	1	1	0

.

Таким образом, $g_1(x) = (x+1)(x^2+x+1)$ и потому $g(x) = (x-1)(x+1)(x^2+x+1)$. Ясно, что это равенство является разложением многочлена $g(x)$ на неприводимые множители над полем $\mathbb{R}$.

Сравнивая найденные разложения многочленов $f(x)$ и $g(x)$ на неприводимые множители, получаем, что наибольшим общим делителем многочленов f и g является многочлен $(x-1)(x^2+x+1) = x^3 - 1$.

Ответ. $x^3 - 1$.

Перейдем к задачам третьего типа. Выяснить, является ли данный многочлен приводимым или неприводимым над полем $\mathbb{Q}$, можно несколькими способами. Простейшим из них (но далеко не всегда применимым) является использование критерия Эйзенштейна. Приведем соответствующий пример.

Задача IV.4. Доказать, что многочлен $f(x) = 5x^5 - 6x^4 + 12x^2 - 21$ неприводим над полем $\mathbb{Q}$.

Решение. Заметим, что старший коэффициент многочлена $f(x)$ не делится на 3, все остальные его коэффициенты делятся на 3, а его свободный член не делится на 9. В силу критерия Эйзенштейна многочлен $f(x) = 5x^5 - 6x^4 + 12x^2 - 21$ неприводим над полем $\mathbb{Q}$.

Неприводимость над полем $\mathbb{Q}$ многочленов степени 2 или 3 можно установить с помощью предложения 12.5. Приведем соответствующий пример.

Задача IV.5. Выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x) = x^3 - x^2 + x - 4$.

Решение. Вычислим значения многочлена $f(x)$ от всех делителей его свободного члена:

$$\begin{aligned} f(1) &= 1 - 1 + 1 - 4 = -3 \neq 0; \\ f(-1) &= -1 - 1 - 1 - 4 = -7 \neq 0; \\ f(2) &= 8 - 4 + 2 - 4 = 2 \neq 0; \\ f(-2) &= -2 - 4 - 2 - 4 = -12 \neq 0; \\ f(4) &= 64 - 16 + 4 - 4 = 48 \neq 0; \\ f(-4) &= -64 - 16 - 4 - 4 = -88 \neq 0. \end{aligned}$$

Мы видим, что ни один из делителей свободного члена многочлена $f(x)$ не является его корнем. В силу следствия 11.2 этот многочлен не имеет рациональных корней. Из предложения 12.5 теперь вытекает, что $f(x)$ неприводим над полем $\mathbb{Q}$.

Ответ. Неприводим.

Отметим, что критерий Эйзенштейна к многочлену из задачи IV.5 неприменим, поскольку простого числа, на которое делились бы все коэффициенты этого многочлена, кроме старшего, не существует.

Наконец, наиболее трудоемкий, но зато универсальный способ выяснения того, приводим ли данный многочлен над полем $\mathbb{Q}$, дает алгоритм Кронекера. Приведем три примера применения этого алгоритма. Во всех этих задачах мы без специальных оговорок используем обозначения, введенные при изложении алгоритма Кронекера.

Задача IV.6. Выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x) = x^5 - 3x^3 - x - 6$.

Решение. Ясно, что $m = \left[\frac{\deg f(x)}{2}\right] = 2$. Положим $x_0 = 1$, $x_1 = 2$ и $x_2 = 3$. Тогда $f(x_0) = f(1) = -9$ и $f(x_1) = f(2) = 0$. В соответствии с алгоритмом Кронекера последнее равенство означает, что многочлен $f(x)$ приводим.

Ответ. Приводим.

В этом примере нам повезло: мы случайно выбрали в качестве одного из значений переменной корень многочлена $f(x)$. В результате работа алгоритма Кронекера, если так можно выразиться, закончилась, не успев начаться. Фактически она свелась к ссылке на замечание 12.3. В следующих двух задачах применить алгоритм Кронекера таким образом невозможно, поскольку возникающие в них многочлены не имеют целых корней (в этом легко убедиться с помощью следствия 11.2). Отметим, что решить эти задачи, не используя алгоритм Кронекера, также нельзя, поскольку критерий Эйзенштейна в них не применим, а упомянутые многочлены имеют степень > 3.

Задача IV.7. Выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x) = x^4 - 3x^3 + 2x^2 + 1$.

Решение. Как и в предыдущей задаче, $m = \left[\frac{\deg f(x)}{2}\right] = 2$. Положим $x_0 = 0$, $x_1 = 1$ и $x_2 = 2$. Найдем значения многочлена $f(x)$ в этих трех точках: $f(x_0) = f(0) = 1$, $f(x_1) = f(1) = 1$ и $f(x_2) = f(2) = 1$. Поскольку все найденные значения многочлена $f(x)$ не равны 0, нам надо найти интерполяционные многочлены Лагранжа, значения которых в точках x_0, x_1 и x_2 делят соответственно числа $f(x_0)$, $f(x_1)$ и $f(x_2)$. В соответствии с формулой (6.4) всякий такой многочлен имеет вид $y_0p_0(x) + y_1p_1(x) + y_2p_2(x)$ для некоторых чисел y_0, y_1 и y_2 и некоторых многочленов $p_0(x)$, $p_1(x)$ и $p_2(x)$, которые, как показывает формула (6.3), зависят только от чисел x_0, x_1 и x_2. Найдем эти многочлены:

$$p_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 1}{-1} \cdot \frac{x - 2}{-2} = \frac{x^2}{2} - \frac{3x}{2} + 1;$$

$$p_1(x) = \frac{x-x_0}{x_1-x_0}\cdot\frac{x-x_2}{x_1-x_2} = \frac{x}{1}\cdot\frac{x-2}{-1} = -x^2+2x;$$
$$p_2(x) = \frac{x-x_0}{x_2-x_0}\cdot\frac{x-x_1}{x_2-x_1} = \frac{x}{2}\cdot\frac{x-1}{1} = \frac{x^2}{2}-\frac{x}{2}.$$

Каждое из чисел $f(x_0)$, $f(x_1)$ и $f(x_2)$ имеет ровно два делителя: 1 и -1. Следовательно, существует восемь наборов чисел вида (n_0,n_1,n_2), где $n_j \mid f(x_j)$ при $j=0,1,2$. В силу (6.4)

$$\begin{aligned} g_{(-n_0,-n_1,-n_2)} &= -n_0p_0(x) - n_1p_1(x) - n_2p_2(x) = \\ &= -(n_0p_0(x) + n_1p_1(x) + n_2p_2(x)) = -g_{(n_0,n_1,n_2)}. \end{aligned}$$

Поскольку умножение многочлена на -1 не меняет его степень и не влияет на то, делится ли многочлен $f(x)$ на данный многочлен, достаточно рассмотреть только те наборы чисел вида (n_0,n_1,n_2), в которых $n_0>0$, а именно наборы $(1,1,1)$, $(1,1,-1)$, $(1,-1,1)$ и $(1,-1,-1)$. Выясним, есть ли среди многочленов вида $g_{(n_0,n_1,n_2)}$, соответствующих этим наборам, многочлен со следующими двумя свойствами: $\deg g_{(n_0,n_1,n_2)}>0$ и $g_{(n_0,n_1,n_2)} \mid f$. Имеем:

$$\begin{aligned} g_{(1,1,1)}(x) &= p_0(x)+p_1(x)+p_2(x) = \\ &= \frac{x^2}{2}-\frac{3x}{2}+1-x^2+2x+\frac{x^2}{2}-\frac{x}{2} = \\ &= 1 \text{ — многочлен степени } 0; \\ g_{(1,1,-1)}(x) &= p_0(x)+p_1(x)-p_2(x) = \\ &= \frac{x^2}{2}-\frac{3x}{2}+1-x^2+2x-\frac{x^2}{2}+\frac{x}{2} = \\ &= -x^2+x+1 \text{ не делит } f(x), \text{ поскольку} \\ &\quad f(x) = (-x^2+2x-1)(-x^2+x+1)-x+2; \\ g_{(1,-1,1)}(x) &= p_0(x)-p_1(x)+p_2(x) = \\ &= \frac{x^2}{2}-\frac{3x}{2}+1+x^2-2x+\frac{x^2}{2}-\frac{x}{2} = \\ &= 2x^2-4x+1 \text{ не делит } f(x), \text{ поскольку} \\ &\quad f(x) = \Big(\frac{x^2}{2}-\frac{x}{2}-\frac{1}{4}\Big)(2x^2-4x+1)-\frac{x}{2}+\frac{5}{4}; \\ g_{(1,-1,-1)}(x) &= p_0(x)-p_1(x)-p_2(x) = \end{aligned}$$

$$= \frac{x^2}{2} - \frac{3x}{2} + 1 + x^2 - 2x - \frac{x^2}{2} + \frac{x}{2} =$$
$$= x^2 - 3x + 1 \text{ не делит } f(x), \text{ поскольку}$$
$$f(x) = (x^2+1)(x^2-3x+1) + 3x.$$

Итак, среди многочленов вида $g_{(n_0,n_1,n_2)}$ нет многочленов степени > 0, делящих $f(x)$. В соответствии с алгоритмом Кронекера это означает, что многочлен $f(x)$ неприводим над полем $\mathbb{Q}$.

Ответ. Неприводим.

В задаче IV.7 многочлены вида $g_{(n_0,n_1,\ldots,n_m)}$ искались с помощью формул (6.3) и (6.4). Их можно искать и по-другому, решая системы линейных уравнений вида (6.2). Приведем соответствующий пример. Этот пример также показывает, как с помощью алгоритма Кронекера можно найти разложение многочлена на неприводимые множители над полем $\mathbb{Q}$.

Задача IV.8. Выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x) = x^4 - x^2 - 2x - 1$; если да, разложить его на неприводимые множители над полем $\mathbb{Q}$.

Решение. Как и в двух предыдущих задачах, $m = \left[\frac{\deg f(x)}{2}\right] = 2$. Положим $x_0 = -1$, $x_1 = 0$ и $x_2 = 1$. Найдем значения многочлена $f(x)$ в этих трех точках: $f(x_0) = f(-1) = 1$, $f(x_1) = f(0) = -1$ и $f(x_2) = f(1) = -3$. Поскольку все найденные значения многочлена $f(x)$ не равны 0, нам надо найти интерполяционные многочлены Лагранжа, значения которых в точках x_0, x_1 и x_2 делят соответственно числа $f(x_0)$, $f(x_1)$ и $f(x_2)$. Числа $f(x_0)$ и $f(x_1)$ имеют ровно два делителя: 1 и -1, а число $f(x_2)$ — четыре делителя: 1, -1, 3 и -3. Следовательно, существуют 16 наборов чисел вида (n_0, n_1, n_2), где $n_j \mid f(x_j)$ при $j = 0, 1, 2$. Как и в предыдущей задаче, мы можем рассматривать только те наборы, в которых $n_0 > 0$. Таким образом, достаточно рассмотреть 8 наборов чисел: $(1,1,1)$, $(1,1,-1)$, $(1,1,3)$, $(1,1,-3)$, $(1,-1,1)$, $(1,-1,-1)$, $(1,-1,3)$ и $(1,-1,-3)$. Будем искать многочлены Лагранжа, соответствующие этим наборам, решая системы линейных уравнений вида (6.2), и для тех из найденных многочленов, степень которых > 0, выяснять, делят ли они $f(x)$. Поскольку $g_{(n_0,n_1,n_2)} \leqslant 2$ для любой тройки чисел (n_0, n_1, n_2),

можно считать, что $g_{(n_0,n_1,n_2)} = ax^2 + bx + c$ для некоторых чисел a, b, c.

а) $n_0 = n_1 = n_2 = 1$. Подставляя в многочлен $g_{(1,1,1)}(x) = ax^2 + bx + c$ вместо x сначала -1, потом 0 и потом 1, получаем систему линейных уравнений

$$\begin{cases} a - b + c = 1, \\ c = 1, \\ a + b + c = 1. \end{cases}$$

Итак, $c = 1$. Подставив 1 вместо c в первое и третье уравнения системы, получаем, что $a - b = 0$ и $a + b = 0$. Складывая эти уравнения, имеем $2a = 0$, т. е. $a = 0$. Отсюда и из первого уравнения получаем, что $b = 0$. Следовательно, $g_{(1,1,1)}(x) = 1$ — многочлен степени 0.

б) $n_0 = n_1 = 1$, а $n_2 = -1$. На этот раз требуется решить систему

$$\begin{cases} a - b + c = 1, \\ c = 1, \\ a + b + c = -1. \end{cases}$$

Как и ранее, $c = 1$. Следовательно, $a - b = 0$ и $a + b = -2$. Складывая эти уравнения, имеем $2a = -2$, т. е. $a = -1$. Отсюда и из первого уравнения получаем, что $b = -1$. Следовательно, $g_{(1,1,-1)}(x) = -x^2 - x + 1$. Этот многочлен не делит $f(x)$, поскольку $f(x) = (x^2 + x - 1)(-x^2 - x + 1) - 4x$.

в) $n_0 = n_1 = 1$, а $n_2 = 3$. На этот раз требуется решить систему

$$\begin{cases} a - b + c = 1, \\ c = 1, \\ a + b + c = 3. \end{cases}$$

Вновь $c = 1$. Следовательно, $a - b = 0$ и $a + b = 2$. Складывая эти уравнения, имеем $2a = 2$, т. е. $a = 1$. Отсюда и из первого уравнения получаем, что $b = 1$. Следовательно, $g_{(1,1,3)}(x) = x^2 + x + 1$. Этот многочлен делит $f(x)$, поскольку $f(x) = (x^2 - x - 1)(x^2 + x + 1)$.

Итак, среди многочленов вида $g_{(n_0,n_1,n_2)}$ нашелся многочлен степени > 0, делящий $f(x)$. Это означает, что многочлен $f(x)$ приводим над полем $\mathbb{Q}$. Работа алгоритма Кронекера завершена. Одновременно мы нашли разложение многочлена $f(x)$ в произведение

многочленов меньшей степени над полем $\mathbb{Q}$: $f(x) = (x^2-x-1)(x^2+x+1)$. Из следствия 11.2 и предложения 12.5 легко вытекает, что многочлены x^2+x+1 и x^2-x-1 неприводимы над полем $\mathbb{Q}$. Следовательно, разложение многочлена $f(x)$ на неприводимые множители над полем $\mathbb{Q}$ имеет вид $f(x) = (x^2+x+1)(x^2-x-1)$.

Ответ. Приводим; $f(x) = (x^2+x+1)(x^2-x-1)$.

Перейдем, наконец, к задачам четвертого типа.

Задача IV.9. Представить рациональную дробь

$$\frac{4x^3-2x^2+4x+4}{x^4-x^2-2}$$

в виде суммы простейших дробей:

а) над полем $\mathbb{C}$;

б) над полем $\mathbb{R}$;

в) над полем $\mathbb{Q}$.

Решение. а) При решении задачи IV.2а) показано, что разложение многочлена x^4-4x^2-2 на неприводимые множители над полем $\mathbb{C}$ имеет вид $x^4-4x^2-2 = \big(x-\sqrt{2}\,\big)\big(x+\sqrt{2}\,\big)(x-i)(x+i)$. Следовательно, представление данной в условии рациональной дроби в виде суммы простейших дробей над полем $\mathbb{C}$ имеет вид

$$\frac{4x^3-2x^2+4x+4}{x^4-x^2-2} = \frac{A}{x-\sqrt{2}} + \frac{B}{x+\sqrt{2}} + \frac{C}{x-i} + \frac{D}{x+i}$$

для некоторых $A, B, C, D \in \mathbb{C}$. Приведем правую часть этого равенства к общему знаменателю и умножим обе части полученного равенства на этот знаменатель. Получим

$$\begin{aligned} 4x^3-2x^2+4x+4 &= A(x+\sqrt{2}\,)(x^2+1) + B(x-\sqrt{2}\,)(x^2+1) + \\ &\quad + C(x^2-2)(x+i) + D(x^2-2)(x-i) = \\ &= (A+B+C+D)x^3 + \\ &\quad + (\sqrt{2}A - \sqrt{2}B + iC - iD)x^2 + \\ &\quad + (A+B-2C-2D)x + \\ &\quad + (\sqrt{2}A - \sqrt{2}B - 2iC + 2iD). \end{aligned}$$

Приравняв коэффициенты при одинаковых степенях переменной x, получим систему линейных уравнений

$$\begin{cases} A + B + C + D = 4, \\ \sqrt{2}A - \sqrt{2}B + iC - iD = -2, \\ A + B - 2C - 2D = 4, \\ \sqrt{2}A - \sqrt{2}B - 2iC + 2iD = 4. \end{cases}$$

Вычтя из первого уравнения третье, получаем $3C + 3D = 0$, откуда $D = -C$. А умножив первое уравнение на 2 и прибавив к нему третье, получаем $3A + 3B = 12$, откуда $B = 4 - A$. Подставив полученные выражения для B и D во второе уравнение, имеем $\sqrt{2}A - \sqrt{2}(4 - A) + 2iC = -2$, откуда $2\sqrt{2}A + 2iC = -2 + 4\sqrt{2}$, т. е.

$$\sqrt{2}A + iC = -1 + 2\sqrt{2}. \qquad (\star)$$

Аналогичным образом, подставив выражения для B и D в четвертое уравнение системы, получаем, что $\sqrt{2}A - \sqrt{2}(4 - A) - 4iC = 4$, откуда $2\sqrt{2}A - 4iC = 4 + 4\sqrt{2}$, т. е. $\sqrt{2}A - 2iC = 2 + 2\sqrt{2}$. Вычтя это равенство из $(\star)$, имеем $3iC = -3$. Умножив последнее равенство на $-\frac{i}{3}$, получаем, что $C = i$, и потому $D = -C = -i$. Отсюда и из $(\star)$ вытекает, что $\sqrt{2}A - 1 = -1 + 2\sqrt{2}$, откуда $A = 2$, и потому $B = 4 - A = 2$. Следовательно,

$$\frac{4x^3 - 2x^2 + 4x + 4}{x^4 - x^2 - 2} = \frac{2}{x - \sqrt{2}} + \frac{2}{x + \sqrt{2}} + \frac{i}{x - i} + \frac{-i}{x + i}.$$

б) Решение задачи IV.2б) показывает, что разложение многочлена $x^4 - 4x^2 - 2$ на неприводимые множители над полем $\mathbb{R}$ имеет вид $x^4 - 4x^2 - 2 = \big(x - \sqrt{2}\big)\big(x + \sqrt{2}\big)(x^2 + 1)$. Следовательно, представление нашей дроби в виде суммы простейших дробей над полем $\mathbb{R}$ имеет вид

$$\frac{4x^3 - 2x^2 + 4x + 4}{x^4 - x^2 - 2} = \frac{A}{x - \sqrt{2}} + \frac{B}{x + \sqrt{2}} + \frac{Cx + D}{x^2 + 1}$$

для некоторых $A, B, C, D \in \mathbb{R}$. На этот раз, приведя правую часть равенства к общему знаменателю и умножив обе части полученного равенства на этот знаменатель, мы получим

$$4x^3 - 2x^2 + 4x + 4 = A(x + \sqrt{2})(x^2 + 1) + B(x - \sqrt{2})(x^2 + 1) + \\ + (Cx + D)(x^2 - 2) =$$

$$= (A+B+C)x^3 + (\sqrt{2}A - \sqrt{2}B + D)x^2 + \\ + (A+B-2C)x + (\sqrt{2}A - \sqrt{2}B - 2D).$$

Приравняв коэффициенты при одинаковых степенях переменной x, получим систему линейных уравнений

$$\begin{cases} A + B + C = 4, \\ \sqrt{2}A - \sqrt{2}B + D = -2, \\ A + B - 2C = 4, \\ \sqrt{2}A - \sqrt{2}B - 2D = 4. \end{cases}$$

Вычтя из первого уравнения третье, получаем, что $3C = 0$, т. е. $C = 0$. А вычтя из второго уравнения четвертое, находим, что $3D = -6$, т. е. $D = -2$. Из первого уравнения теперь вытекает, что $A + B = 4$, а из второго — что $\sqrt{2}A - \sqrt{2}B = 0$, т. е. $A - B = 0$. Складывая два полученных равенства, имеем $2A = 4$, т. е. $A = 2$. Учитывая еще раз, что $A - B = 0$, получаем, что $B = 2$. Следовательно,

$$\frac{4x^3 - 2x^2 + 4x + 4}{x^4 - x^2 - 2} = \frac{2}{x - \sqrt{2}} + \frac{2}{x + \sqrt{2}} + \frac{-2}{x^2 + 1}.$$

в) Как показано при решении задачи IV.2в), разложение многочлена $x^4 - 4x^2 - 2$ на неприводимые множители над полем $\mathbb{Q}$ имеет вид $x^4 - 4x^2 - 2 = (x^2 - 2)(x^2 + 1)$. Следовательно, представление нашей дроби в виде суммы простейших дробей над полем $\mathbb{Q}$ имеет вид

$$\frac{4x^3 - 2x^2 + 4x + 4}{x^4 - x^2 - 2} = \frac{Ax + B}{x^2 - 2} + \frac{Cx + D}{x^2 + 1}$$

для некоторых $A, B, C, D \in \mathbb{Q}$. Отсюда

$$4x^3 - 2x^2 + 4x + 4 = (Ax + B)(x^2 + 1) + (Cx + D)(x^2 - 2) = \\ = (A + C)x^3 + (B + D)x^2 + (A - 2C)x + \\ + (B - 2D).$$

Приравнивая коэффициенты при одинаковых степенях перемен-

ной x, получаем систему линейных уравнений

$$\begin{cases} A & + & C & & = & 4, \\ & B & & + & D & = -2, \\ A & - & 2C & & = & 4, \\ & B & & - & 2D & = & 4. \end{cases}$$

Вычтя из первого уравнения третье, имеем $3C = 0$, т. е. $C = 0$. Отсюда и из первого уравнения вытекает, что $A = 4$. Далее, вычтя из второго уравнения четвертое, находим, что $3D = -6$, т. е. $D = -2$. А отсюда и из второго уравнения получаем, что $B = 0$. Следовательно,

$$\frac{4x^3 - 2x^2 + 4x + 4}{x^4 - x^2 - 2} = \frac{4x}{x^2 - 2} + \frac{-2}{x^2 + 1}.$$

Ответ. а) $\frac{2}{x-\sqrt{2}} + \frac{2}{x+\sqrt{2}} + \frac{i}{x-i} + \frac{-i}{x+i}$; б) $\frac{2}{x-\sqrt{2}} + \frac{2}{x+\sqrt{2}} + \frac{-2}{x^2+1}$; в) $\frac{4x}{x^2-2} + \frac{-2}{x^2+1}$.

В задаче IV.9 знаменатель рациональной дроби раскладывается на неприводимые множители кратности 1 (над каждым из трех рассмотренных полей). Рассмотрим случай, когда это не так.

Задача IV.10. Представить рациональную дробь

$$\frac{x^4 + 1}{x^5 + 2x^3 + x}$$

в виде суммы простейших дробей над полем $\mathbb{R}$.

Решение. Разложение знаменателя дроби на неприводимые множители в данном случае находится очень легко:

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

Поэтому представление данной дроби в виде суммы простейших дробей имеет вид

$$\frac{x^4 + 1}{x^5 + 2x^3 + x} = \frac{A}{x} + \frac{Bx + C}{x^2 + 1} + \frac{Dx + E}{(x^2 + 1)^2}$$

для некоторых $A, B, C, D, E \in \mathbb{R}$. Приведем правую часть равенства к общему знаменателю и приравняем числители полученных дробей. Получим

$$\begin{aligned} x^4 + 1 &= A(x^2+1)^2 + (Bx+C)x(x^2+1) + (Dx+E)x = \\ &= Ax^4 + 2Ax^2 + A + Bx^4 + Bx^2 + Cx^3 + Cx + Dx^2 + Ex = \\ &= (A+B)x^4 + Cx^3 + (2A+B+D)x^2 + (C+E)x + A. \end{aligned}$$

Приравнивая коэффициенты при одинаковых степенях переменной x, получаем систему линейных уравнений

$$\begin{cases} A + B = 1, \\ C = 0, \\ 2A + B + D = 0, \\ C + E = 0, \\ A = 1. \end{cases}$$

В частности, $A = 1$ и $C = 0$. Из первого уравнения теперь вытекает, что $B = 0$, а из четвертого — что $E = 0$. Наконец, подставив найденные значения A и B в третье уравнение, получаем, что $D = -2$. Следовательно,

$$\frac{x^4+1}{x^5+2x^3+x} = \frac{1}{x} + \frac{-2x}{(x^2+1)^2}.$$

Ответ. $\frac{1}{x} + \frac{-2x}{(x^2+1)^2}$.

В задачах IV.9 и IV.10 неприводимые множители знаменателей рациональных дробей имели степень $\leqslant 2$. Для рациональных дробей над полем $\mathbb{Q}$ это может не выполняться (см. следствие 15.4). Рассмотрим соответствующий пример.

Задача IV.11. Представить рациональную дробь

$$\frac{2x^2+3x}{x^6+x^4+2x^3+2x^2+2x+2}$$

в виде суммы простейших дробей над полем $\mathbb{Q}$.

Решение. Заметим, что

$$\begin{aligned} &x^6 + x^4 + 2x^3 + 2x^2 + 2x + 2 = \\ &= x^4(x^2+1) + 2x(x^2+1) + 2(x^2+1) = \\ &= (x^2+1)(x^4+2x+2). \end{aligned}$$

Многочлен x^2+1 неприводим над $\mathbb{R}$, а значит и над $\mathbb{Q}$, а многочлен x^4+2x+2 удовлетворяет посылке критерия Эйзенштейна при $p=2$ и потому также неприводим над $\mathbb{Q}$. Следовательно, равенство

$$x^6 + x^4 + 2x^3 + 2x^2 + 2x + 2 = (x^2+1)(x^4+2x+2)$$

является разложением знаменателя данной в условии дроби на неприводимые множители над полем $\mathbb{Q}$. Поэтому представление данной дроби в виде суммы простейших дробей над $\mathbb{Q}$ имеет вид

$$\frac{2x^2+3x}{x^6+x^4+2x^3+2x^2+2x+2} = \frac{Ax+B}{x^2+1} + \frac{Cx^3+Dx^2+Ex+F}{x^4+2x+2}$$

для некоторых $A, B, C, D, E, F \in \mathbb{Q}$. Приведем правую часть равенства к общему знаменателю и приравняем числители полученных дробей. Получим

$$\begin{aligned} 2x^2+3x &= (Ax+B)(x^4+2x+2) + \\ &\quad + (Cx^3+Dx^2+Ex+F)(x^2+1) = \\ &= (A+C)x^5 + (B+D)x^4 + (C+E)x^3 + \\ &\quad + (2A+D+F)x^2 + (2A+2B+E)x + (2B+F). \end{aligned}$$

Приравнивая коэффициенты при одинаковых степенях переменной x, получаем систему линейных уравнений

$$\begin{cases} A \phantom{{}+2B} + C \phantom{{}+D} \phantom{{}+E} \phantom{{}+F} = 0, \\ B \phantom{{}+2B} + D \phantom{{}+E} \phantom{{}+F} = 0, \\   C \phantom{{}+2B} + E \phantom{{}+F} = 0, \\ 2A \phantom{{}+2B} + D \phantom{{}+E} + F = 2, \\ 2A + 2B \phantom{{}+D} + E \phantom{{}+F} = 3, \\ 2B \phantom{{}+D} \phantom{{}+E} + F = 0. \end{cases}$$

Решим ее методом Гаусса. Запишем расширенную матрицу системы и приведем ее к ступенчатому виду:

$$\left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 2&0&0&1&0&1&2\\ 2&2&0&0&1&0&3\\ 0&2&0&0&0&1&0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&-2&1&0&1&2\\ 0&2&-2&0&1&0&3\\ 0&2&0&0&0&1&0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&-2&1&0&1&2\\ 0&0&-2&-2&1&0&3\\ 0&0&0&-2&0&1&0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&0&1&2&1&2\\ 0&0&0&-2&3&0&3\\ 0&0&0&-2&0&1&0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&0&1&2&1&2\\ 0&0&0&0&7&2&7\\ 0&0&0&0&4&3&4 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1&0&1&0&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&0&1&2&1&2\\ 0&0&0&0&7&2&7\\ 0&0&0&0&0&13&0 \end{array}\right).$$

Из полученной матрицы последовательно находим, что $F = 0$, $E = 1$, $D = 0$, $C = -1$, $B = 0$, $A = 1$. Следовательно,

$$\frac{2x^2+3x}{x^6+x^4+2x^3+2x^2+2x+2} = \frac{x}{x^2+1} + \frac{-x^3+x}{x^4+2x+2}.$$

Ответ. $\frac{x}{x^2+1} + \frac{-x^3+x}{x^4+2x+2}$.

Задачи для самостоятельного решения

Во всех задачах, в которых явно не оговорено противное, речь идет о многочленах над полем $\mathbb{R}$.

1. Найти частное $q(x)$ и остаток $r(x)$ от деления многочлена $f(x)$ на многочлен $g(x)$:

а) $f(x) = x^4 - x^3 - 3x^2 + 3x - 2$, $g(x) = x - 2$;

б) $f(x) = x^4 - x^3 - 3x^2 + 3x - 8$, $g(x) = x + 2$;

в) $f(x) = x^4 + x^3 + 3x^2 - x - 2$, $g(x) = x^3 + 2x - 3$;

г) $f(x) = x^3 + x - 1$, $g(x) = x^2 + x + 1$;

д) $f(x) = x^4 + x^3 + 2x^2 + 3x$, $g(x) = x^2 + 1$;

е) $f(x) = x^5 + x^4 + 2x^3 - 2x^2 + 3x$, $g(x) = x^3 + x^2 + x - 3$;

ж) $f(x) = x^6 + 3x^5 - 2x^4 - 7x^3 - 2x + 3$, $g(x) = x^4 + 2x^3 + x - 1$.

2. Найти частное $q(x)$ и остаток $r(x)$ от деления многочлена $f(x) = x^5 + x^3 + 1$ на многочлен $g(x) = x^2 + x + 1$:

а) над полем $\mathbb{R}$;

б) над полем $\mathbb{Z}_2$;

в) над полем $\mathbb{Z}_3$.

3. Доказать, что многочлен над произвольным полем F делится на свою производную тогда и только тогда, когда он ассоциирован с многочленом $(x-\alpha)^n$ для некоторого $\alpha \in F$ и некоторого натурального n.

4. Для многочленов $f(x)$ и $g(x)$ найти их наибольший общий делитель $d(x)$ и многочлены $u(x)$ и $v(x)$ такие, что $d = uf + vg$:

а) $f(x) = x^5 - 3x^4 - 2x^3 + 3x^2 + 7x + 6$, $g(x) = x^4 - x^3 - x^2 - x - 2$;

б) $f(x) = x^5 - 4x^4 + 2x^3 - 8x^2 - 3x + 12$, $g(x) = x^4 + x^3 - x - 1$;

в) $f(x) = x^5 - 2x^4 + x^3 - 9x^2 - 6x - 9$, $g(x) = x^7 - x^6 - x^5 - 7x^4 - 17x^3 - 15x^2 - 15x - 9$;

г) $f(x) = x^7 + 2x^6 - 2x^5 - 3x^4 + 2x^3 - 2x^2 - 4x$, $g(x) = x^6 + 2x^5 - 5x^4 - 6x^3 + 8x^2 + 4x - 4$.

5. Доказать, что многочлены $f(x)$ и $g(x)$ взаимно просты и найти многочлены $u(x)$ и $v(x)$ такие, что $uf + vg = 1$:

а) $f(x) = x^4 + x^3 + 3x^2 - x - 2$, $g(x) = x^3 + 2x - 3$;

б) $f(x) = x^3 + x - 1$, $g(x) = x^2 + x + 1$;

в) $f(x) = x^4 + x^3 + 2x^2 + 3x$, $g(x) = x^2 + 1$;

г) $f(x) = x^3 + x^2 + x - 3$, $g(x) = x^5 + x^4 + 2x^3 - 2x^2 + 3x$;

д) $f(x) = x^4 + 2x^3 + x - 1$, $g(x) = x^6 + 3x^5 - 2x^4 - 7x^3 - 2x + 4$.

6. Для многочленов $f(x)$ и $g(x)$ над полем $\mathbb{Z}_2$ найти их наибольший общий делитель $d(x)$ и многочлены $u(x)$ и $v(x)$ такие, что $d = uf + vg$:

а) $f(x) = x^5 + x^4 + 1$, $g(x) = x^4 + x^2 + 1$;

б) $f(x) = x^5 + x^3 + x + 1$, $g(x) = x^4 + 1$;

в) $f(x) = x^5 + x + 1$, $g(x) = x^4 + x^3 + 1$;

г) $f(x) = x^5 + x^3 + x$, $g(x) = x^4 + x + 1$.

7. Пусть f и g — многочлены над произвольным полем, d — их наибольший общий делитель, а многочлены u и v таковы, что $d = uf + vg$. Доказать, что многочлены u и v взаимно просты.

8. Найти многочлен наименьшей степени $p(x)$, принимающий в указанных ниже точках следующие значения:

а)

x	-1	0	1	2
$p(x)$	3	7	9	-3

б)
x	-1	0	1	2
$p(x)$	2	-4	-8	2

;

в)
x	-2	-1	0	1
$p(x)$	-3	1	1	3

;

г)
x	-2	-1	0	1
$p(x)$	-14	-3	0	1

.

9. Построить интерполяционный многочлен Лагранжа $p(x)$ для функции $f(x)$, принимающей следующие значения:

а)
x	-1	0	1	2
$f(x)$	-10	-4	-2	2

;

б)
x	-1	0	1	2
$f(x)$	-9	-3	-3	-3

;

в)
x	-2	-1	0	1
$f(x)$	-10	4	6	4

;

г)
x	-2	-1	0	1
$f(x)$	0	-4	-8	-6

.

10. Выяснить, при каких значениях параметра λ среди корней многочлена $x^3 - 7x + \lambda$ есть два, один из которых в два раза больше другого.

11. Выяснить, при каких значениях параметра λ среди корней многочлена $2x^3 - x^2 - 7x + \lambda$ есть два, сумма которых равна 1.

12. Выяснить, корнем какой кратности многочлена $f(x)$ является число a:

а) $f(x) = x^5 - 5x^3 - 9x^2 - 8x - 3$, $a = -1$;

б) $f(x) = x^5 - 15x^4 + 74x^3 - 110x^2 - 75x + 125$, $a = 5$;

в) $f(x) = x^4 - 4x^3 + 3x^2 + 4x - 4$, $a = 2$;

г) $f(x) = x^5 + x^4 + x^3 - x^2 - x - 1$, $a = 1$;

д) $f(x) = x^5 - 5x^4 + 2x^3 + 14x^2 - 3x - 9$, $a = 3$.

13. Пусть $f(x)$ — произвольный многочлен. Выяснить, корнем какой кратности многочлена

$$g(x) = \frac{x-a}{2} \cdot \big(f'(x) + f'(a)\big) - f(x) + f(a)$$

является число a.

14. Выяснить, при каких значениях параметров a и b число 1 является корнем кратности 2 многочлена $ax^{n+1} + bx^n + 1$.

15. Доказать, что при любом натуральном $n > 4$ число 1 является корнем кратности 3 многочлена $x^{2n} - nx^{n+1} + nx^{n-1} - 1$.

16. Доказать, что при любом натуральном n многочлен

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + \frac{x^2}{2!} + x + 1$$

не имеет кратных корней.

17. Решить уравнения в поле $\mathbb{R}$ и в поле $\mathbb{C}$:

а) $x^4 - 3x^3 + x^2 + 4 = 0$;

б) $x^4 - 2x^3 + 3x^2 - 4x + 2 = 0$;

в) $x^5 + 3x^4 + 2x^3 + 6x^2 + x + 3 = 0$;

г) $x^6 - 2x^5 + 2x^4 - 10x^3 - 11x^2 - 8x - 12 = 0$.

18. Найти число действительных корней многочлена $f(x) = x^3 + 3x^2 - 6x - 9$

а) на всей числовой прямой;

б) на отрезке $[0, 2]$.

19. Найти число действительных корней многочлена $f(x) = 2x^3 + 3x^2 + 3x + 6$

а) на всей числовой прямой;

б) на отрезке $[-2, 1]$.

20. Найти число действительных корней многочлена $f(x) = x^3 + x + 1$

а) на всей числовой прямой;

б) на отрезке $[-1, 0]$.

21. Найти число действительных корней многочлена $f(x) = 4x^4 + x^2 - 3x + 1$

а) на всей числовой прямой;
б) на отрезке $[0, 3]$.

22. Найти рациональные корни многочлена $f(x)$:
а) $f(x) = x^3 - x^2 - 7x + 3$;
б) $f(x) = x^4 + 5x^3 + 5x^2 - 5x - 6$;
в) $f(x) = x^5 + 2x^4 + 3x^3 + 3x^2 + 2x + 1$;
г) $f(x) = 12x^3 - 28x^2 + 13x + 3$;
д) $f(x) = 5x^4 - 4x^3 - 16x^2 + 12x + 3$;
е) $f(x) = 2x^5 + x^4 - 9x^3 + 10x - 4$;
ж) $f(x) = x^4 - \frac{4}{3}x^3 + \frac{10}{3}x^2 - 4x + 1$.

23. Пусть $f(x)$ — многочлен над полем $\mathbb{R}$ с целыми коэффициентами. Доказать, что если существует целое число m такое, что числа $f(m)$ и $f(m+1)$ нечетны, то многочлен $f(x)$ не имеет целых корней.
24. Пусть $f(x)$ — многочлен над полем $\mathbb{R}$ с целыми коэффициентами. Доказать, что если существуют целые числа k и m такие, что $|k - m| > 2$ и каждое из чисел $f(k)$ и $f(m)$ равно либо 1, либо -1, то многочлен $f(x)$ не имеет рациональных корней.
25. Отделить кратные множители многочлена f и разложить его на неприводимые множители над полем $\mathbb{R}$:
а) $f(x) = x^4 + 3x^3 + 4x^2 + 3x + 1$;
б) $f(x) = x^4 + 2x^3 - 2x - 1$;
в) $f(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$;
г) $f(x) = x^5 - 3x^4 + 4x^3 - 4x^2 + 3x - 1$;
д) $f(x) = x^5 - x^4 + 4x^3 - 4x^2 + 4x - 4$;
е) $f(x) = x^6 - 4x^5 + 6x^4 - 8x^3 + 9x^2 - 4x + 4$.

26. Разложить многочлен $f(x)$ на неприводимые множители над полем $\mathbb{C}$ и над полем $\mathbb{R}$:
а) $f(x) = x^4 - x^3 - x^2 - x - 2$;
б) $f(x) = x^4 + 4x^3 + 4x^2 - 4x - 5$;
в) $f(x) = x^4 + 5x^3 + 10x^2 + 9x + 3$;
г) $f(x) = x^5 + x^4 + 2x^3 - 6x^2 - 3x + 5$;
д) $f(x) = x^4 + 4$;
е) $f(x) = 2x^3 - 3x^2 + 1$.

27. Разложить многочлен $f(x)$ на неприводимые множители над полем $\mathbb{Q}$:

а) $f(x) = x^4 - 5x^2 + 6$;

б) $f(x) = x^5 - 3x^3 - 5x^2 + 15$;

в) $f(x) = x^3 + 2x^2 - 2x - 1$;

г) $f(x) = x^5 + x^4 + 2x^2 + 8x + 6$.

28. Доказать неприводимость над полем $\mathbb{Q}$ следующих многочленов:

а) $x^4 + 2x^3 - 6x^2 + 4x - 2$;

б) $2x^4 + 6x^3 - 9x^2 + 12x - 12$;

в) $x^2 + 2x - 4$;

г) $x^3 + 2x^2 + 3x + 4$.

29. Используя алгоритм Кронекера, выяснить, приводим ли над полем $\mathbb{Q}$ многочлен $f(x)$; если да, разложить его на неприводимые множители над полем $\mathbb{Q}$:

а) $f(x) = x^4 + x^3 - 2x^2 - 2x + 1$;

б) $f(x) = x^4 - x^3 - 3x^2 + 2x + 2$;

в) $f(x) = x^4 + 2x^3 - x^2 - 2x + 1$.

30. Представить правильные рациональные дроби в виде суммы простейших дробей над полем $\mathbb{C}$:

а) $\frac{3x^2-4x-4}{x^3-x^2+4x-4}$;

б) $\frac{x^3+4x^2-2x+9}{x^4+x^3+x^2+3x-6}$;

в) $\frac{x^2+2x-1}{x^3+x^2+x+1}$;

г) $\frac{3x^2+6x-5}{x^4+4x^3+5x^2+4x+4}$.

31. Представить правильные рациональные дроби в виде суммы простейших дробей над полем $\mathbb{R}$:

а) $\frac{2x^3-2x^2-6x-4}{x^4-4x^3+3x^2-4x+12}$;

б) $\frac{4x^2-12x-10}{x^3-2x^2-5x+6}$;

в) $\frac{x^2-3x-7}{x^4+4x^3+5x^2+8x+6}$;

г) $\frac{2x+6}{x^3+x^2-3x-3}$;

д) $\frac{x^2-5x+5}{x^3-5x^2+8x-4}$.

32. Представить правильные рациональные дроби в виде суммы простейших дробей над полем $\mathbb{Q}$:

а) $\frac{2x^3-2x^2+2x+10}{x^4-4x^2-5}$;

б) $\frac{4x^3+2x}{x^4+x^2-12}$;

в) $\frac{-3}{x^4-x^3+2x-2}$.

33. Представить рациональную дробь в виде суммы многочлена и простейших дробей над полем $\mathbb{R}$:

а) $\frac{2x^4+x^3+4x^2-3}{x^3+x^2+x+1}$;

б) $\frac{x^5-4x^4+10x^2+14x-12}{x^4-5x^3+4x^2+3x+9}$.

Ответы и указания

1. а) $q(x) = x^3 + x^2 - x + 1$, $r(x) = 0$; б) $q(x) = x^3 - 3x^2 + 3x - 3$, $r(x) = -2$; в) $q(x) = x + 1$, $r(x) = x^2 + 1$; г) $q(x) = x - 1$, $r(x) = x$; д) $q(x) = x^2 + x + 1$, $r(x) = 2x - 1$; е) $q(x) = x^2 + 1$, $r(x) = 2x + 3$; ж) $q(x) = x^2 + x - 4$, $r(x) = 3x - 1$.
2. а) $q(x) = x^3 - x^2 + x$, $r(x) = -x + 1$; б) $q(x) = x^3 + x^2 + x$, $r(x) = x + 1$; в) $q(x) = x^3 + 2x^2 + x$, $r(x) = 2x + 1$.
4. а) $d(x) = 10x^2 - 10x - 20$, $u(x) = 3x - 1$, $v(x) = -3x^2 + 7x + 7$; б) $d(x) = 21x^2 - 21$, $u(x) = -x - 2$, $v(x) = x^2 - 3x - 3$; в) $d(x) = x^3 - 3x^2 + 3x - 9$, $u(x) = x^3 + x^2 + 1$, $v(x) = -x$; г) $d(x) = 6x^3 + 6x^2 - 12x - 12$, $u(x) = -2x^2 - 3x + 7$, $v(x) = 2x^3 + 3x^2 - x + 3$.
5. а) $u(x) = \frac{1}{10}(x^2 + 3x + 1)$, $v(x) = -\frac{1}{10}(x^3 + 4x^2 + 5x + 4)$; б) $u(x) = -x - 1$, $v(x) = x^2$; в) $u(x) = -\frac{2}{5}x - \frac{1}{5}$, $v(x) = \frac{2}{5}x^3 + \frac{3}{5}x^2 + \frac{3}{5}x + 1$; г) $u(x) = -\frac{4}{45}x^4 + \frac{2}{45}x^3 - \frac{11}{45}x^2 + \frac{2}{45}x - \frac{1}{3}$, $v(x) = \frac{4}{45}x^2 - \frac{2}{45}x + \frac{7}{45}$; д) $u(x) = -\frac{1}{3}x^5 - x^4 + \frac{2}{3}x^3 + \frac{7}{3}x^2 - \frac{1}{3}x + \frac{1}{3}$, $v(x) = \frac{1}{3}x^3 + \frac{2}{3}x^2 + \frac{1}{3}$.
6. а) $d(x) = x^2 + x + 1$, $u(x) = x + 1$, $v(x) = x^2$; б) $d(x) = x + 1$, $u(x) = x$, $v(x) = x^2 + 1$; в) $d(x) = 1$, $u(x) = x + 1$, $v(x) = x^2$; г) $d(x) = 1$, $u(x) = x^3 + x$, $v(x) = x^4 + x + 1$.
7. *Указание:* использовать следствие 5.4.
8. а) $p(x) = -2x^3 - x^2 + 5x + 7$; б) $p(x) = 2x^3 + x^2 - 7x - 4$; в) $p(x) = x^3 + x^2 + 1$; г) $p(x) = x^3 - x^2 + x$.
9. а) $p(x) = x^3 - 2x^2 + 3x - 4$; б) $p(x) = x^3 - 3x^2 + 2x - 3$; в) $p(x) = x^3 - 3x^2 - 2x + 6$; г) $p(x) = x^3 + 3x^2 - 2x - 8$.

10. $\lambda = \pm 6$. **11.** $\lambda = -3$. **12.** а) 2; б) 3; в) 2; г) 1; д) 2.
13. $k+3$, где k — кратность a как корня многочлена $f(x)$.
14. $a = n$, $b = -n-1$. **15**, **16.** *Указание:* использовать лемму 10.3.
17. а) в $\mathbb{R}$: $x_1 = 2$, в $\mathbb{C}$: $x_1 = 2$, $x_{2,3} = \frac{-1\pm\sqrt{3}i}{2}$; б) в $\mathbb{R}$: $x_1 = 1$, в $\mathbb{C}$: $x_1 = 1$, $x_{2,3} = \pm\sqrt{2}i$; в) в $\mathbb{R}$: $x_1 = -3$, в $\mathbb{C}$: $x_1 = -3$, $x_{2,3} = \pm i$; г) в $\mathbb{R}$: $x_1 = -1$, $x_2 = 3$, в $\mathbb{C}$: $x_1 = -1$, $x_2 = 3$, $x_{3,4} = \pm i$, $x_{5,6} = \pm 2i$.
18. а) 3; б) 0. **19**. а) 1; б) 1. **20**. а) 1; б) 1. **21**. а) 1; б) 1.
22. а) 3; б) 1, -1, -2, -3; в) -1; г) 1, $\frac{3}{2}$, $-\frac{1}{6}$; д) 1, $-\frac{1}{5}$; е) 1, -2, $\frac{1}{2}$; ж) 1, $\frac{1}{3}$.
23, **24.** *Указание:* использовать предложение 11.3.
25. а) $d_1(f) = x^2+x+1$, $d_2(f) = x+1$, $f = (x^2+x+1)(x+1)^2$; б) $d_1(f) = x-1$, $d_2(f) = 1$, $d_3(f) = x+1$, $f = (x-1)(x+1)^3$; в) $d_1(f) = 1$, $d_2(f) = x+1$, $d_3(f) = x-1$, $f = (x+1)^2(x-1)^3$; г) $d_1(f) = x^2+1$, $d_2(f) = 1$, $d_3(f) = x+1$; $f = (x^2+1)(x+1)^3$; д) $d_1(f) = x-1$, $d_2(f) = x^2+2$, $f = (x-1)(x^2+2)^2$; е) $d_1(f) = 1$, $d_2(f) = x^3-2x^2+x-2$, $f = (x-2)^2(x^2+1)^2$.
26. а) над $\mathbb{C}$: $f(x) = (x-i)(x+i)(x-2)(x+1)$, над $\mathbb{R}$: $(x^2+1)(x-2)(x+1)$; б) над $\mathbb{C}$: $f(x) = (x+2+i)(x+2-i)(x-1)(x+1)$, над $\mathbb{R}$: $f(x) = (x^2+4x+5)(x-1)(x+1)$; в) над $\mathbb{C}$: $f(x) = \big(x+\frac{3}{2} - \frac{\sqrt{3}}{2}i\big)\big(x+\frac{3}{2}+\frac{\sqrt{3}}{2}i\big)(x+1)^2$, над $\mathbb{R}$: $f(x) = (x^2+3x+3)(x+1)^2$; г) над $\mathbb{C}$: $f(x) = (x+1-2i)(x+1+2i)(x-1)^2(x+1)$, над $\mathbb{R}$: $f(x) = (x^2+2x+5)(x-1)^2(x+1)$; д) над $\mathbb{C}$: $f(x) = (x-1-i)(x-1+i)(x+1+i)(x+1-i)$, над $\mathbb{R}$: $f(x) = (x^2-2x+2)(x^2+2x+2)$; е) над $\mathbb{C}$ и над $\mathbb{R}$: $f(x) = (x-1)^2(2x+1)$.
27. а) $(x^2-3)(x^2-2)$; б) $(x^3-5)(x^2-3)$; в) $(x^2+3x+1)(x-1)$; г) $(x+1)(x^4+2x+6)$.
28. *Указания:* а), б) использовать критерий Эйзенштейна; в), г) использовать предложения 11.1 и 12.5.
29. а) неприводим; б) приводим, $f(x) = (x^2-x-1)(x^2-2)$; в) приводим, $f(x) = (x^2+x-1)^2$.
30. а) $\frac{2}{x-2i}+\frac{2}{x+2i}+\frac{-1}{x-1}$; б) $\frac{1}{2(x+\sqrt{3}i)}+\frac{1}{2(x-\sqrt{3}i)}+\frac{-1}{x+2}+\frac{1}{x-1}$; в) $\frac{1}{x+i}+\frac{1}{x-i}+\frac{-1}{x+1}$; г) $\frac{1}{x+i}+\frac{1}{x-i}+\frac{-2}{x+2}+\frac{-1}{(x+2)^2}$.
31. а) $\frac{1}{x-2}+\frac{1}{x-3}+\frac{1}{x^2+x+2}$; б) $\frac{3}{x-1}+\frac{2}{x+2}+\frac{-1}{x-3}$; в) $\frac{-1}{2(x+1)}+\frac{-1}{2(x+3)}+\frac{x-1}{x^2+2}$; г) $\frac{1}{x-\sqrt{3}}+\frac{1}{x+\sqrt{3}}+\frac{-2}{x+1}$; д) $\frac{1}{x-1}+\frac{-1}{(x-2)^2}$.
32. а) $\frac{-2}{x^2+1}+\frac{2x}{x^2-5}$; б) $\frac{2x}{x^2+4}+\frac{2x}{x^2-3}$; в) $\frac{-1}{x-1}+\frac{x^2+x+1}{x^3+2}$.
33. а) $2x-1+\frac{1}{x+1}+\frac{2x-3}{x^2+1}$; б) $x+1+\frac{2}{x-3}+\frac{3}{(x-3)^2}+\frac{-x-2}{x^2+x+1}$.

Список литературы

1. *Винберг Э. Б.* Алгебра многочленов: учеб. пособие / Э. Б. Винберг. — Москва : Просвещение, 1980. — 176 с.

2. *Кострикин А. И.* Введение в алгебру. Ч. 1 : Основы алгебры / А. И. Кострикин. — Москва : МЦНМО, 2020. — 272 с. — ISBN 978-5-4439-4117-2.

3. *Курош А. Г.* Курс высшей алгебры / А. Г. Курош. — Санкт-Петербург [и др.] : Лань, 2021. — 432 с. — ISBN 978-5-8114-6851-5.

4. *Прасолов В. В.* Многочлены / В. В. Прасолов. — Москва : МЦНМО, 2014. — 335 с. — ISBN 978-5-4439-0233-3.

5. *Фаддеев Д. К.* Лекции по алгебре / Д. К. Фаддеев. — Санкт-Петербург [и др.] : Лань, 2020. — 416 с. — ISBN 978-5-8114-4867-8.

6. *Фаддеев Д. К.* Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. — Санкт-Петербург [и др.] : Лань, 2008. — 287 с. — ISBN 978-5-8114-0427-8.

Список обозначений

$\mathbb{N}$ — множество всех натуральных чисел.

$\mathbb{Z}$ — множество всех целых чисел.

$\mathbb{Q}$ — множество всех рациональных чисел.

$\mathbb{R}$ — множество всех действительных чисел.

$\mathbb{C}$ — множество всех комплексных чисел.

$\mathbb{Z}_n$ — кольцо вычетов по модулю n.

$\operatorname{char} F$ — характеристика поля F.

i — мнимая единица.

$\overline{z}$ — комплексное число, комплексно сопряженное к числу z.

$|z|$ — модуль комплексного числа z.

$R[x]$ — множество всех многочленов над кольцом R.

$\deg f$ — степень многочлена f.

$\ell m(f)$ — старший член многочлена f.

$\ell c(f)$ — старший коэффициент многочлена f.

$g \mid f$ — многочлен или целое число g делит соответственно многочлен или целое число f.

$g \nmid f$ — многочлен или целое число g не делит соответственно многочлен или целое число f.

R_f — константа, вычисляемая для многочлена $f(x) = a_n x^n + + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ над полем $\mathbb{C}$ следующим образом:

$$R_f = \frac{\max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}}{|a_n|} + 1.$$

$W_f(\xi)$ — число перемен знаков в упорядоченной последовательности чисел, полученной после вычеркивания нулей из последовательности $f_0(\xi)$, $f_1(\xi)$, …, $f_m(\xi)$, где $f_0(x)$, $f_1(x)$, …, $f_m(x)$ — по-

следовательность многочленов Штурма для многочлена $f(x)$ над полем $\mathbb{R}$, а $\xi \in \mathbb{R}$.

$d_i(f)$, где $i \in \mathbb{N}$, — произведение всех неприводимых множителей кратности i многочлена f, если они существуют, и 1 в противном случае.

$d(f)$ — наибольший общий делитель всех коэффициентов многочлена f над кольцом $\mathbb{Z}$.

Предметный указатель