



Министерство
просвещения РСФСР

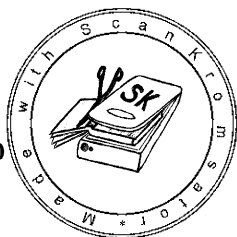
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ЗАОЧНЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Э. Б. ВИНБЕРГ

АЛГЕБРА МНОГОЧЛЕНОВ

Учебное пособие
для студентов-заочников III—IV курсов
физико-математических факультетов
педагогических институтов

МОСКВА «ПРОСВЕЩЕНИЕ» 1980



*Рекомендовано
к печати Главным управлением
высших и средних педагогических учебных заведений
Министерства просвещения РСФСР*

Р е ц е н з е н т ы:

доктор физико-математических наук *М. М. Глухов*,
доктор физико-математических наук *К. А. Родосский*,
кандидат физико-математических наук *Г. В. Дорофеев*.

Редактор МГЗПИ *О. А. Павлович*

В 60602 — 192
103(03)—80 заказное 4309020400

© Московский государственный заочный педагогический институт (МГЗПИ), 1980 г.



ПРЕДИСЛОВИЕ

Настоящая книга представляет собой учебное пособие для студентов-заочников педагогических институтов. Она написана в соответствии с действующей программой и посвящена алгебре многочленов, которая составляет последнюю (четвертую) часть курса «Алгебра и теория чисел». Предполагаются известными основные понятия теории колец и теория делимости в евклидовых кольцах. По этим вопросам мы отсылаем читателя к книге «Алгебра и теория чисел», ч. III, авторов Н. А. Казачека, Г. Н. Перлатова, Н. Я. Виленкина, А. И. Бородина (М., Просвещение, 1974).

Почти все разделы алгебры многочленов так или иначе связаны с решением алгебраических уравнений и систем уравнений. Этот материал особенно близок школьному курсу математики. Поэтому в настоящем пособии проблеме решения уравнений уделяется довольно много внимания, несмотря на то что в современной алгебре многочленов она занимает скромное место.

В § 2 гл. III наряду со способом исключения неизвестного из системы двух алгебраических уравнений с двумя неизвестными при помощи результата излагается способ решения системы алгебраических уравнений, основанный на «элементарных преобразованиях». Это соответствует духу всего курса, в котором, например, решение систем линейных уравнений проводится сначала при помощи элементарных преобразований и лишь затем излагается метод определителей, имеющий большее значение для теории, чем для решения конкретных систем уравнений.

В § 1 и 4 гл. IV рассказывается о геометрическом изображении и тригонометрической форме комплексных чисел, а также о решении в радикалах уравнений третьей и четвертой степени. Этот материал по программе относится к первой части курса, но не вошел в соответствующее пособие, так как логически более тесно связан с алгеброй многочленов.

В связи с тем что данное пособие рассчитано на студентов-заочников, доказательства теорем проводятся подробно, теоретический материал иллюстрирован большим количеством примеров, в конце каждого из параграфов приводятся вопросы для самопроверки и упражнения. Благодаря этому книга может служить в какой-то степени и задачником. Многие упражнения взяты из «Сборника задач по высшей алгебре» Д. К. Фаддеева и И. С. Соминского (М., Наука, 1977), где можно при желании найти и другие задачи по большинству разделов курса.

Нумерация теорем, лемм и формул производится в пределах каждого параграфа, нумерация параграфов — в пределах каждой главы. При ссылке на теорему или формулу в пределах того же параграфа номер параграфа не указывается.

Во всей книге используются следующие обозначения, ставшие в последнее время общепринятыми:

$\mathbf{Z}$ — кольцо целых чисел,
 $\mathbf{Q}$ — поле рациональных чисел,
 $\mathbf{R}$ — поле действительных чисел,
 $\mathbf{C}$ — поле комплексных чисел.

Автор выражает благодарность профессору А. С. Солодовникову и профессору Н. Я. Виленкину, которые своими предложениями в значительной степени способствовали улучшению рукописи.

Просим читателей присылать свои критические замечания и пожелания по адресу: Москва 109004, Верхняя Радищевская ул., д. 18. Редакционно-издательский отдел МГЗПИ.

Глава I

МНОГОЧЛЕНЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

§ 1. ПОНЯТИЕ МНОГОЧЛЕНА

1. Многочлены как функции действительной переменной. Понятие многочлена (или целой рациональной функции) знакомо читателю из курса математического анализа, в котором функция $f(x)$ действительной переменной x называется *многочленом*, если она может быть представлена в виде

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad (1)$$

где $a_0, a_1, a_2, \dots, a_n$ — какие-то действительные числа (некоторые из них или даже все могут равняться нулю). Например, функция

$$f(x) = 1 - x^2 + 2x^4 = 1 + 0x + (-1)x^2 + 0x^3 + 2x^4$$

является многочленом. Функция $f(x) = ((x-1)^2 + x)(x+1) - x^2$ также является многочленом, так как после раскрытия скобок она представляется в виде $f(x) = 1 - x^2 + x^3$. Частным случаем многочлена является постоянная функция $f(x) = a$, принимающая одно и то же значение a при всех значениях x .

Выражение

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0x^{n+1} + \dots + 0x^m$$

определяет ту же функцию (многочлен), что и выражение (1), поскольку при любом значении x имеет место равенство

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0x^{n+1} + \dots + 0x^m.$$

Обратно, можно доказать, что если при всех значениях x выполняется равенство

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n = b_0 + b_1x + b_2x^2 + \dots + b_mx^m,$$

где $m \geq n$, то $b_k = a_k$ при $k = 0, 1, 2, \dots, n$ и $b_k = 0$ при $k = n+1, \dots, m$. Одно из доказательств этого утверждения будет дано в п. 6. Отсюда следует, что с точностью до приписывания или отбрасывания членов с нулевыми коэффициентами представление многочлена $f(x)$ в виде выражения (1) единственно.

Число a_k в выражении (1) называется *коэффициентом* многочлена $f(x)$ при x^k .

Поскольку, не меняя многочлена $f(x)$, к его выражению (1) можно приписать любое количество членов с нулевыми коэффициентами, то говорят также о коэффициентах многочлена $f(x)$ при x^k ,

где $k > n$, считая их равными нулю. Многочлен, все коэффициенты которого равны нулю, называется *нулевым многочленом*.

Если многочлен (1) не является нулевым, то наибольшее из таких чисел k , что $a_k \neq 0$, называется его *степенью*. Например, $f(x) = 1 - x^2 + 2x^4$ — многочлен четвертой степени. Постоянные функции, отличные от нуля, — это многочлены нулевой степени.

Сумма, разность и произведение двух многочленов также являются многочленами. В самом деле, пусть

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad (2)$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m. \quad (3)$$

Тогда

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_p + b_p)x^p, \quad (4)$$

$$f(x) - g(x) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \dots + (a_p - b_p)x^p, \quad (5)$$

где $p = \max\{n, m\}$ (наибольшее из чисел n, m), причем считается, что $a_k = 0$ при $k > n$ и $b_k = 0$ при $k > m$. Например,

$$\begin{aligned} & (2 - 3x + x^3 + 2x^4) + (-1 + 3x + 2x^2 + x^3) = \\ & = (2 - 1) + (-3 + 3)x + (0 + 2)x^2 + (1 + 1)x^3 + (2 + 0)x^4 = \\ & = 1 + 2x^2 + 2x^3 + 2x^4. \end{aligned}$$

Произведение многочленов $f(x)$ и $g(x)$ равно сумме всевозможных произведений uv , где u — любой член многочлена $f(x)$, а v — любой член многочлена $g(x)$. После приведения подобных членов получается многочлен

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n+m}x^{n+m}, \quad (6)$$

где

$$\begin{aligned} c_k x^k &= a_0 \cdot b_k x^k + a_1 x \cdot b_{k-1} x^{k-1} + a_2 x^2 \cdot b_{k-2} x^{k-2} + \\ &+ \dots + a_k x^k \cdot b_0 = (a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0) x^k, \end{aligned}$$

так что

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0. \quad (7)$$

(Здесь, как и выше, считается, что $a_l = 0$ при $l > n$ и $b_l = 0$ при $l > m$.) Например,

$$\begin{aligned} & (2 - 3x + x^3 + 2x^4)(-1 + 3x + 2x^2) = \\ & = -2 + 9x - 5x^2 - 7x^3 + x^4 + 8x^5 + 4x^6; \end{aligned}$$

в частности, коэффициент при x^4 может быть получен по формуле (7) в результате следующих вычислений:

$$2 \cdot 0 + (-3) \cdot 0 + 0 \cdot 2 + 1 \cdot 3 + 2 \cdot (-1) = 1.$$

Итак, сумма, разность и произведение многочленов также являются многочленами. Это означает, что многочлены образуют подкольцо в кольце всех функций действительной переменной. Кольцо многочленов от действительной переменной x обозначается через $R[x]$. Символ R является обозначением поля действительных чисел. Поскольку кольцо всех функций коммутативно и ассоциативно, кольцо $R[x]$ также обладает этими свойствами. В нем есть единственный элемент — постоянная функция $f(x) = 1$.

2. Алгебраическое определение кольца многочленов. В математике приходится рассматривать не только многочлены с действительными коэффициентами, но и многочлены с коэффициентами из других полей или колец. При этом точка зрения на многочлен как на функцию, изложенная в п. 1, не всегда оказывается пригодной. Например, если рассматривать с этой точки зрения многочлены с коэффициентами из кольца Z_2 вычетов по модулю 2 (состоящего из двух элементов: $\bar{0}$ и $\bar{1}$; см. АТЧ III, § 2, гл. III *), то многочлены $f_1(x) = \bar{1}x$ и $f_2(x) = \bar{1}x^2$ пришлось бы считать равными, так как $f_1(x) = f_2(x)$ при всех значениях x , а именно:

$$f_1(\bar{0}) = f_2(\bar{0}) = \bar{0}, \quad f_1(\bar{1}) = f_2(\bar{1}) = \bar{1}.$$

Изложим алгебраический подход к понятию многочлена. При этом мы будем рассматривать многочлены с коэффициентами из любого кольца. Представление о многочлене как о функции должно быть временно забыто. Мы вернемся к нему на более высоком уровне в п. 4.

Пусть K — произвольное кольцо. *Многочленом от x с коэффициентами из K* назовем формальное выражение вида

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad (8)$$

где n — любое неотрицательное целое число и $a_0, a_1, a_2, \dots, a_n$ — элементы кольца K . Подчеркнем, что выражение (8) должно рассматриваться как единый символ; никаких операций сложения или умножения над отдельными его частями не подразумевается. Элемент a_k ($k = 0, 1, 2, \dots, n$) кольца K будем называть *коэффициентом* многочлена (8) *при x^k* ; для $k > n$ условимся считать, что коэффициент при x^k равен нулю. Для обозначения многочленов будем пользоваться символами $f(x), g(x)$ и т. п.

Многочлены $f_1(x)$ и $f_2(x)$ будем считать *равными*, если для любого k коэффициент многочлена $f_1(x)$ при x^k равен коэффициенту многочлена $f_2(x)$ при x^k . Равенство будем записывать обычным образом:

$$f_1(x) = f_2(x).$$

Для многочленов $f(x)$ и $g(x)$, заданных формулами (2) и (3) (где $a_0, a_1, a_2, \dots, a_n, b_0, b_1, b_2, \dots, b_m$ — элементы кольца K), о п р е -

* Здесь и далее АТЧ III означает ссылку на книгу авторов Н. А. Казачека, Г. Н. Перлатова, Н. Я. Виленкина, А. И. Бородина «Алгебра и теория чисел», ч. III.

делим их сумму $f(x) + g(x)$ по формуле (4) и произведение $f(x)g(x)$ по формулам (6) и (7). Легко видеть, что эти определения согласуются с данным выше определением равенства многочленов, т. е. если

$$f_1(x) = f_2(x) \text{ и } g_1(x) = g_2(x),$$

то

$$f_1(x) + g_1(x) = f_2(x) + g_2(x) \text{ и } f_1(x)g_1(x) = f_2(x)g_2(x).$$

З а м е ч а н и я. 1) Роль буквы x в записи многочленов может играть любая буква. Если из контекста ясно, какая буква исполняет эту роль, обозначения многочленов $f(x)$, $g(x)$, ... могут сокращаться до f , g , ...

2) Так как для задания многочлена (8) существенны лишь коэффициенты $a_0, a_1, a_2, \dots, a_n$, то можно было бы назвать многочленом просто последовательность $(a_0, a_1, a_2, \dots, a_n)$ элементов кольца K , определив соответствующим образом операции сложения и умножения таких последовательностей. Однако в конечном счете запись многочлена в виде выражения (8) оказывается более удобной.

Установим теперь некоторые свойства операций сложения и умножения многочленов.

1°. Коммутативность сложения. Пусть многочлены $f(x)$ и $g(x)$ заданы формулами (2) и (3). Тогда, согласно определению,

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_p + b_p)x^p, \\ g(x) + f(x) &= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + \dots + (b_p + a_p)x^p, \end{aligned}$$

где $p = \max\{n, m\}$. Так как в кольце K сложение коммутативно, то $a_k + b_k = b_k + a_k$ ($k = 0, 1, 2, \dots, p$) и, значит,

$$f(x) + g(x) = g(x) + f(x).$$

2°. Ассоциативность сложения можно доказать аналогично, исходя из ассоциативности сложения в кольце K .

3°. Существование нуля. Назовем *нулевым многочленом* и обозначим символом 0 многочлен, все коэффициенты которого равны нулю. Этот многочлен играет роль нулевого (нейтрального по отношению к сложению) элемента. В самом деле, из определения сложения многочленов ясно, что $f(x) + 0 = f(x)$ для любого многочлена $f(x)$.

4°. Существование противоположного элемента. Обозначим через $-f(x)$ многочлен, все коэффициенты которого противоположны соответствующим коэффициентам многочлена $f(x)$. Ясно, что $f(x) + (-f(x)) = 0$, т. е. $-f(x)$ — это многочлен, противоположный многочлену $f(x)$.

5°. Дистрибутивность умножения относительно сложения. Пусть даны три многочлена:

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots + b_mx^m, \\ h(x) &= c_0 + c_1x + c_2x^2 + \dots + c_lx^l. \end{aligned}$$

Докажем, что

$$(f(x) + g(x))h(x) = f(x)h(x) + g(x)h(x). \quad (9)$$

Многочлен $f(x) + g(x)$ задается формулой (4). Согласно определению умножения многочленов,

$$(f(x) + g(x))h(x) = d_0 + d_1x + d_2x^2 + \dots + d_{p+l}x^{p+l},$$

где

$$d_k = (a_0 + b_0)c_k + (a_1 + b_1)c_{k-1} + (a_2 + b_2)c_{k-2} + \dots + (a_k + b_k)c_0.$$

Воспользовавшись дистрибутивностью в кольце K , мы можем представить d_k в виде суммы $d'_k + d''_k$,

где

$$d'_k = a_0c_k + a_1c_{k-1} + a_2c_{k-2} + \dots + a_kc_0,$$

$$d''_k = b_0c_k + b_1c_{k-1} + b_2c_{k-2} + \dots + b_kc_0.$$

Ясно, что d'_k есть коэффициент при x^k многочлена $f(x)h(x)$, а d''_k — коэффициент при x^k многочлена $g(x)h(x)$. Отсюда и следует равенство (9). Аналогично доказывается другое соотношение дистрибутивности:

$$h(x)(f(x) + g(x)) = h(x)f(x) + h(x)g(x).$$

Свойства 1^0 — 5^0 означают, что *многочлены с коэффициентами из кольца K сами образуют кольцо относительно определенных нами операций сложения и умножения*. Это кольцо называется *кольцом многочленов (от x) над K* и обозначается через $K[x]$. В п. 4 мы покажем, что в случае $K = \mathbf{R}$ имеется естественный изоморфизм между этим кольцом и тем, которое было обозначено через $\mathbf{R}[x]$ в п. 1.

Как и во всяком кольце, в кольце многочленов определена операция *вычитания*, обратная операции сложения. Мы будем предполагать известными простейшие свойства этой операции, вытекающие из аксиом кольца (см. АТЧ III, п. 4 § 1 гл. II). Разность многочленов $f(x)$ и $g(x)$, задаваемых формулами (2) и (3), находится по формуле (5). Это утверждение легко доказать, представив разность в виде

$$f(x) - g(x) = f(x) + (-g(x)).$$

Многочлены, не содержащие x , т. е. выражения (8), в которых $n = 0$, — это элементы кольца K . Их сложение и умножение, как видно из определений, производится так же, как в кольце K . Иными словами, *кольцо K является подкольцом кольца $K[x]$* .

Формальные слагаемые $a_0, a_1x, a_2x^2, \dots, a_nx^n$ называются *членами* многочлена (8); в частности, a_0 называется *свободным членом*. Обычно в записи многочлена опускают члены, коэффициенты которых равны нулю. Например, многочлен $6 + 0x + 2x^2 + 3x^3 + 0x^4$ записывают как $6 + 2x^2 + 3x^3$.

Многочлен вида ax^k называется *одночленом*. Из определения сложения многочленов следует, что многочлен (8) равен сумме одночленов $a_0, a_1x, a_2x^2, \dots, a_nx^n$. Таким образом, рассматривая каждый член многочлена как одночлен, можно истолковывать символ «+» в записи многочлена как знак сложения. При таком толковании записи многочлена его члены можно располагать в произвольном порядке, например «по убывающим степеням x », т. е. в виде

$$c_0x^n + c_1x^{n-1} + \dots + c_{n-1}x + c_n.$$

Одночлен $(-a)x^k$ противоположен одночлену ax^k . Поэтому прибавление к какому-либо многочлену одночлена $(-a)x^k$ равносильно вычитанию одночлена ax^k . Это позволяет в записи многочлена вместо $+(-a)x^k$ писать $-ax^k$, рассматривая «—» как знак вычитания. Например, многочлен $1 + (-2)x + 3x^2$ можно записать как $1 - 2x + 3x^2$.

Предположим теперь, что в кольце K имеется единица. Рассмотрим многочлен $p(x) = 1x$. По формуле для произведения многочленов находим, что $p(x)^2 = p(x) \cdot p(x) = 1x^2$, $p(x)^3 = p(x)^2 \cdot p(x) = 1x^3$ и т. д.

Вообще

$$p(x)^k = p(x)^{k-1} \cdot p(x) = 1x^k.$$

Умножая в кольце $K[x]$ многочлен $1x^k$ на элемент a кольца K , находим:

$$a \cdot p(x)^k = ax^k.$$

Наконец, путем сложения нескольких таких равенств получаем, что

$$\begin{aligned} a_0 + a_1 \cdot p(x) + a_2 \cdot p(x)^2 + \dots + a_n \cdot p(x)^n &= \\ = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \end{aligned}$$

для любых $a_0, a_1, a_2, \dots, a_n \in K \subset K[x]$.

В чем смысл этого равенства? Его правая часть есть, согласно нашему определению многочлена, просто формальное выражение, в то время как левая часть получена из элементов $a_0, a_1, a_2, \dots, a_n$ и $p(x)$ кольца $K[x]$ путем фактического выполнения операций сложения и умножения в этом кольце. Поэтому (если в кольце K есть единица) можно отождествить букву x с многочленом, который мы обозначили через $p(x)$, и придать тем самым записи многочлена неформальный смысл. В дальнейшем мы всегда будем иметь это в виду.

В заключение введем понятие степени многочлена и другие связанные с ним понятия. *Степенью* ненулевого многочлена $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ называется наибольшее из таких чисел k , что $a_k \neq 0$; степень нулевого многочлена считается равной $-\infty$. (В дальнейшем читатель убедится в целесообразности такого определения степени нулевого многочлена.) Степень многочлена $f(x)$ обозначается ст. $f(x)$.

Отметим, что многочлены нулевой степени — это элементы кольца K , отличные от нуля. Всякий многочлен степени $n \geq 0$ может быть записан в виде

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n,$$

где $a_n \neq 0$. При этом a_nx^n называется его *старшим членом*, а a_n — *старшим коэффициентом*. Многочлен, старший коэффициент которого равен единице (если в кольце K есть единица), называется *нормированным**.

Рассматривая формулы (4) и (6), по которым определялись сумма и произведение многочленов, мы видим, что формула для суммы не содержит членов, степень которых выше, чем $\max\{n, m\}$, а формула для произведения — членов, степень которых выше, чем $n + m$. Отсюда следует, что

$$\text{ст.}(f(x) + g(x)) \leq \max\{\text{ст.}f(x), \text{ст.}g(x)\}, \quad (10)$$

$$\text{ст.}f(x)g(x) \leq \text{ст.}f(x) + \text{ст.}g(x). \quad (11)$$

Для того чтобы эти неравенства были справедливы и тогда, когда среди многочленов $f(x)$, $g(x)$, $f(x) + g(x)$, $f(x)g(x)$ имеются нулевые (степени которых, согласно определению, равны $-\infty$), нужно считать, что $-\infty \leq n$ и $-\infty + n = -\infty$ для любого n .

3. Кольцо многочленов над областью целостности. В п. 2 мы не налагали никаких ограничений на кольцо K (скажем, не требовали коммутативности или ассоциативности умножения). Чтобы умножение в кольце $K[x]$ обладало теми или иными «хорошими» свойствами, надо требовать выполнения соответствующих свойств в кольце K . Чаще всего приходится иметь дело со случаем, когда K — область целостности, т. е. коммутативное ассоциативное кольцо с единицей и без делителей нуля (см. АТЧ III, п. 9 § 1 гл. II).

Начиная с этого момента на протяжении всей книги мы будем рассматривать только многочлены с коэффициентами из области целостности. Это всегда будет подразумеваться, даже если не будет оговорено специально.

Установим некоторые дополнительные свойства умножения многочленов, которые выполняются при условии, что K — область целостности. (Мы продолжим нумерацию свойств, начатую в п. 2.)

6°. Коммутативность умножения легко вытекает непосредственно из его определения (см. формулы (6) и (7)). Однако мы приведем здесь другое, более поучительное рассуждение. Докажем сначала коммутативность умножения одночленов. Для одночленов ax^n и bx^m имеем:

$$ax^n \cdot bx^m = abx^{n+m}, \quad bx^m \cdot ax^n = bax^{n+m}.$$

Так как в кольце K умножение коммутативно, то $ab = ba$ и, значит,

$$ax^n \cdot bx^m = bx^m \cdot ax^n.$$

* В школе такие многочлены называются *приведенными*.

Пусть теперь $f(x)$ и $g(x)$ — произвольные многочлены. Многочлен $f(x)g(x)$ равен сумме всевозможных произведений вида uv , где u — член многочлена $f(x)$, а v — член многочлена $g(x)$ (например, $(2 - 3x + x^2)(3 + 5x) = 2 \cdot 3 + 2 \cdot 5x + (-3x) \cdot 3 + (-3x) \times \times 5x + x^2 \cdot 3 + x^2 \cdot 5x$).

Аналогично многочлен $g(x)f(x)$ равен сумме всевозможных произведений вида vu , где u и v имеют тот же смысл, что и выше (например, $(3 + 5x)(2 - 3x + x^2) = 3 \cdot 2 + 5x \cdot 2 + 3 \cdot (-3x) + + 5x \cdot (-3x) + 3 \cdot x^2 + 5x \cdot x^2$).

Так как умножение одночленов по доказанному коммутативно, то $uv = vu$ для любого члена u многочлена $f(x)$ и любого члена v многочлена $g(x)$. Следовательно,

$$f(x)g(x) = g(x)f(x).$$

7°. Ассоциативность умножения. Многочлен $(f(x)g(x))h(x)$ равен сумме всевозможных произведений вида $(uv)w$, где u — член многочлена $f(x)$, v — член многочлена $g(x)$, w — член многочлена $h(x)$. Аналогично многочлен $f(x)(g(x)h(x))$ равен сумме всевозможных произведений вида $u(vw)$, где u , v и w имеют тот же смысл. Поэтому достаточно проверить, что $(uv)w = = u(vw)$ для любых одночленов u , v , w , т. е. доказать ассоциативность умножения одночленов. Для одночленов ax^n , bx^m , cx^p имеем:

$$(ax^n \cdot bx^m) \cdot cx^p = abx^{n+m} \cdot cx^p = (ab)cx^{n+m+p},$$

$$ax^n \cdot (bx^m \cdot cx^p) = ax^n \cdot bcx^{m+p} = a(bc)x^{n+m+p}.$$

Так как $(ab)c = a(bc)$, то

$$(ax^n \cdot bx^m) \cdot cx^p = ax^n \cdot (bx^m \cdot cx^p),$$

что и требовалось доказать.

8°. Существование единицы. Единицей (нейтральным элементом по отношению к умножению) в кольце $K[x]$ является единица кольца K . В самом деле, из определения умножения многочленов ясно, что $1 \cdot f(x) = f(x)$ для любого многочлена $f(x)$. В частности, $1 \cdot x^k = x^k$. Поэтому в записи многочлена обычно опускают коэффициенты, равные единице.

9°. Отсутствие делителей нуля. Пусть даны два ненулевых многочлена:

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n,$$

$$g(x) = b_0 + b_1x + \dots + b_{m-1}x^{m-1} + b_mx^m.$$

Докажем, что их произведение также не равно нулю.

Поскольку

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} + a_nb_mx^{n+m},$$

то коэффициент многочлена $f(x)g(x)$ при x^{n+m} равен a_nb_m . Так как в кольце K нет делителей нуля, то $a_nb_m \neq 0$ и, значит, $f(x)g(x) \neq 0$.

Из нашего рассуждения следует также, что

$$\text{ст. } f(x)g(x) = \text{ст. } f(x) + \text{ст. } g(x). \quad (12)$$

Эта формула является уточнением неравенства (11) для случая, когда в кольце K нет делителей нуля. (Формула (12) справедлива и тогда, когда один из многочленов $f(x)$, $g(x)$ или они оба равны нулю, если считать, как было условлено выше, что $-\infty + n = -\infty$ для любого n .)

Свойства 6^0-9^0 означают, что кольцо $K[x]$ является областью целостности. Таким образом, доказана следующая теорема:

Теорема 1. *Кольцо многочленов над областью целостности само является областью целостности.*

4. Функция, определяемая многочленом. В п. 1 было дано определение многочлена от действительной переменной как функции специального вида. Данное в п. 2 алгебраическое определение многочлена не содержит никакого упоминания о функциях. Тем не менее с каждым многочленом над областью целостности K можно естественным образом связать функцию, которая определена на K и принимает значения в K .

Пусть $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ — многочлен с коэффициентами из K . Для любого $x_0 \in K$ положим

$$f(x_0) = a_0 + a_1x_0 + a_2x_0^2 + \dots + a_nx_0^n, \quad (13)$$

где выражение в правой части понимается как результат операций в кольце K . Получаемый при этом элемент $f(x_0) \in K$ называется *значением многочлена $f(x)$ в точке x_0* . (Слово «точка» употребляется по аналогии со случаем $K = \mathbf{R}$, когда x_0 можно представлять как точку действительной оси.) Таким образом, каждому элементу x_0 кольца K сопоставляется элемент $f(x_0)$ того же кольца и тем самым определяется функция на K со значениями в K .

Покажем, что сложение и умножение многочленов согласуются с обычными операциями, производимыми над функциями, когда складываются или, соответственно, перемножаются значения функций в каждой точке.

Рассмотрим два многочлена:

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots + b_mx^m. \end{aligned}$$

Пусть $h(x) = f(x) + g(x)$ — их сумма. Докажем, что $h(x_0) = f(x_0) + g(x_0)$ для любого $x_0 \in K$. В соответствии с формулой (4)

$$\begin{aligned} h(x_0) &= (a_0 + b_0) + (a_1 + b_1)x_0 + (a_2 + b_2)x_0^2 + \dots + (a_p + b_p)x_0^p = \\ &= (a_0 + a_1x_0 + a_2x_0^2 + \dots + a_px_0^p) + (b_0 + b_1x_0 + b_2x_0^2 + \\ &\quad + \dots + b_px_0^p) = f(x_0) + g(x_0), \end{aligned}$$

что и требовалось доказать.

Пусть теперь $p(x) = f(x)g(x)$ — произведение многочленов $f(x)$ и $g(x)$. Докажем, что $p(x_0) = f(x_0)g(x_0)$ для любого $x_0 \in K$. Перемножим равенства

$$\begin{aligned} f(x_0) &= a_0 + a_1 x_0 + a_2 x_0^2 + \dots + a_n x_0^n, \\ g(x_0) &= b_0 + b_1 x_0 + b_2 x_0^2 + \dots + b_m x_0^m. \end{aligned}$$

Пользуясь свойствами операций в кольце K (в частности, коммутативностью и ассоциативностью умножения), получим:

$$f(x_0)g(x_0) = c_0 + c_1 x_0 + c_2 x_0^2 + \dots + c_{n+m} x_0^{n+m},$$

где

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0.$$

Сравнение полученного результата с формулами (6) и (7) позволяет сделать вывод, что $f(x_0)g(x_0) = p(x_0)$.

Таким образом, *функция, определяемая суммой (соответственно произведением) двух многочленов, есть сумма (соответственно произведение) функций, определяемых этими многочленами.*

Этот результат означает, что отображение, ставящее в соответствие каждому многочлену с коэффициентами из K определяемую им функцию, есть гомоморфизм кольца $K[x]$ в кольцо функций, определенных на K и принимающих значения в K . Заметим, что при фиксированном x_0 отображение $f(x) \rightarrow f(x_0)$ является гомоморфизмом кольца $K[x]$ в кольцо K .

Вообще говоря, соответствие между многочленами и определяемыми ими функциями не является взаимно однозначным. В начале п. 2 мы приводили пример двух различных многочленов из кольца $\mathbb{Z}_2[x]$, определяющих одну и ту же функцию на $\mathbb{Z}_2$. Этот пример допускает следующее обобщение. Пусть p — любое простое число и $\mathbb{Z}_p$ — кольцо вычетов по модулю p (напомним, что оно является полем и, значит, областью целостности). Тогда малая теорема Ферма (см. АТЧ III, п. 3 § 4 гл. III) показывает, что многочлены x и x^p из кольца $\mathbb{Z}_p[x]$ определяют одну и ту же функцию на $\mathbb{Z}_p$.

Однако если кольцо K бесконечно, то различным многочленам из кольца $K[x]$ всегда соответствуют различные функции. Это важное утверждение будет доказано в п. 6. Его доказательство будет основано на теореме Безу, вывод которой дается в п. 5.

5. Деление с остатком на двучлен $x - x_0$. В кольце многочленов деление в обычном смысле слова, как правило, невозможно. Например, в кольце $\mathbb{R}[x]$ многочлен x^2 нельзя разделить на $x + 1$, т. е. не существует такого многочлена $g(x)$, что $x^2 = g(x)(x + 1)$ (если бы такой многочлен существовал, то при $x = -1$ мы получили бы невозможное равенство $1 = g(-1) \cdot 0$). Однако во многих случаях выполнимо так называемое «деление с остатком». Эта операция будет описана в § 1 гл. II, а здесь мы рассмотрим ее частный случай, когда делитель является двучленом вида $x - x_0$.

Теорема 2. Пусть $f(x)$ — многочлен с коэффициентами из кольца K . Для любого $x_0 \in K$ многочлен $f(x)$ можно единственным образом представить в виде

$$f(x) = g(x)(x - x_0) + c, \quad (14)$$

где $g(x) \in K[x]$, $c \in K$; при этом $c = f(x_0)$.

Доказательство. Если $f(x) = a \in K$, то можно взять $g(x) = 0$, $c = a$, причем легко видеть, что это единственная воз-

возможность. Пусть теперь ст. $f(x) = n > 0$. Расположим многочлен $f(x)$ по убывающим степеням x :

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n.$$

Ясно, что если представление $f(x)$ в виде (14) возможно, то ст. $g(x) = n-1$. Запишем $g(x)$ с неопределенными коэффициентами:

$$g(x) = b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}.$$

Подставляя выражения для $f(x)$ и $g(x)$ в (14), получаем:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n = b_0x^n + (b_1 - x_0b_0)x^{n-1} + \\ + (b_2 - x_0b_1)x^{n-2} + \dots + (b_{n-1} - x_0b_{n-2})x + (c - x_0b_{n-1}),$$

откуда, в силу определения равенства двух многочленов,

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + x_0b_0, \\ b_2 &= a_2 + x_0b_1, \\ &\dots \dots \dots \\ b_{n-1} &= a_{n-1} + x_0b_{n-2}, \\ c &= a_n + x_0b_{n-1}. \end{aligned} \tag{15}$$

Эти формулы позволяют последовательно находить $b_0, b_1, b_2, \dots, b_{n-1}$ и c . Проведенное рассуждение доказывает, что многочлен $g(x)$ и элемент c , удовлетворяющие соотношению (14), существуют и определены однозначно.

Для доказательства того, что $c = f(x_0)$, вычислим, пользуясь равенством (14), значение многочлена $f(x)$ в точке x_0 . Поскольку первое слагаемое в правой части обращается в нуль, то $f(x_0) = c$. Теорема доказана.

Элемент x_0 кольца K называется *корнем* многочлена $f(x) \in K[x]$, если $f(x_0) = 0$. Из теоремы 2 получаем следующее следствие:

С л е д с т в и е (т е о р е м а Б е з у). *Многочлен $f(x)$ делится на $x - x_0$ в кольце $K[x]$ тогда и только тогда, когда x_0 — его корень.*

В самом деле, ясно, что $f(x)$ делится на $x - x_0$ тогда и только тогда, когда в равенстве (14) $c = 0$, но так как $c = f(x_0)$, то условие $c = 0$ равносильно тому, что x_0 — корень многочлена $f(x)$.

Нахождение многочлена $g(x)$ и элемента c , удовлетворяющих соотношению (14), называется *делением с остатком многочлена $f(x)$ на $x - x_0$* . При этом $g(x)$ называется *неполным частным*, а c — *остатком*. Формулы (15) дают практический способ деления с остатком многочлена $f(x)$ на $x - x_0$.

Вычисления удобно располагать по следующей схеме, называемой *схемой Горнера*:

a_0	a_1	a_2	$\dots$	a_{n-1}	a_n
x_0	b_0	b_1	b_2	$\dots$	$b_{n-1} \quad c$

Элементы нижней строки вычисляются последовательно по формулам (15): $b_0 = a_0$, а каждый последующий элемент равен сумме элемента, находящегося над ним, и предыдущего элемента нижней строки, умноженного на x_0 . Так как $c = f(x_0)$, то этой схемой можно пользоваться и для вычисления значения многочлена в точке x_0 .

Пример 1. В кольце $R[x]$ разделим с остатком $x^4 - 3x^2 + x + 5$ на $x - 2$.

В данном случае $x_0 = 2$. Коэффициенты делимого соответственно равны 1, 0, -3, 1, 5. Выполним вычисления по схеме Горнера:

	1	0	-3	1	5
2	1	$2 \cdot 1 + 0 = 2$	$2 \cdot 2 - 3 = 1$	$2 \cdot 1 + 1 = 3$	$2 \cdot 3 + 5 = 11$

Получаем неполное частное $g(x) = x^3 + 2x^2 + x + 3$ и остаток $c = 11$.

Пример 2. Вычислим значение многочлена $f(x) = ix^3 + (1 - 2i)x^2 - 2(1 - i)x + 2$ (с комплексными коэффициентами) в точке $1 + i$.

Решение (промежуточные вычисления опущены):

	i	$1 - 2i$	$-2 + 2i$	2
$1 + i$	i	$-i$	$-1 + i$	0

Таким образом, $f(1 + i) = 0$.

6. Алгебраическое и функциональное равенство многочленов. Теорема Безу, доказанная в предыдущем пункте, позволяет указать верхнюю границу числа корней многочлена. А именно имеет место следующая теорема:

Теорема 3. Число корней ненулевого многочлена не превосходит его степени.

Доказательство. Докажем это утверждение с помощью индукции по степени многочлена. Многочлен нулевой степени вообще не имеет корней, так что для него утверждение теоремы справедливо. Предположим теперь, что утверждение теоремы справедливо для всех многочленов степени $n - 1$, и докажем его для любого многочлена $f(x)$ степени n . Предположим, рассуждая от противного, что $x_1, x_2, \dots, x_m$ — корни многочлена $f(x)$, причем $m > n$. По теореме Безу, $f(x)$ делится на $x - x_1$, т. е. $f(x) = (x - x_1)g(x)$, где $g(x)$ — некоторый многочлен степени $n - 1$. Элементы $x_2, \dots, x_m$ кольца K являются корнями многочлена $g(x)$. В самом деле, при $i = 2, \dots, m$ имеем:

$$f(x_i) = (x_i - x_1)g(x_i) = 0.$$

Так как $x_i - x_1 \neq 0$, а кольцо K не имеет делителей нуля, то $g(x_i) = 0$. Таким образом, многочлен $g(x)$ имеет не менее чем $m - 1$ корней, что противоречит предположению индукции, поскольку ст. $g(x) = n - 1 < m - 1$. Теорема доказана.

С л е д с т в и е. *Многочлен степени не выше n однозначно определяется своими значениями в $n + 1$ точках.*

Иначе говоря, существует не более одного многочлена степени не выше n , принимающего в данных (различных) точках $x_1, x_2, \dots, x_{n+1}$ данные значения $y_1, y_2, \dots, y_{n+1}$.

Д о к а з а т е л ь с т в о. Предположим, что $f(x), g(x)$ — два многочлена степени не выше n , принимающие одинаковые значения в точках $x_1, x_2, \dots, x_{n+1}$. Рассмотрим многочлен $h(x) = f(x) - g(x)$. Степень этого многочлена также не выше, чем n . Так как $f(x_i) = g(x_i)$, то $h(x_i) = 0$ при $i = 1, 2, \dots, n + 1$, т. е. $x_1, x_2, \dots, x_{n+1}$ — корни многочлена $h(x)$. Согласно только что доказанной теореме $h(x) = 0$, т. е. $f(x) = g(x)$.

В пп. 2, 4 были приведены примеры, когда различные многочлены определяют одну и ту же функцию, т. е. принимают одинаковые значения во всех точках. В таких случаях говорят о «функциональном равенстве» многочленов, в отличие от «алгебраического равенства», т. е. обычного равенства многочленов в смысле определения, данного в п. 2. Полученные выше результаты позволяют установить, что в случае бесконечного кольца K (например, в случае $K = \mathbf{R}$) функциональное равенство равносильно алгебраическому.

Т е о р е м а 4. *Если кольцо K бесконечно, то равенство функций, определяемых двумя многочленами из кольца $K[x]$, влечет за собой равенство самих многочленов.*

Д о к а з а т е л ь с т в о. Пусть многочлены $f(x), g(x) \in K[x]$ определяют одинаковые функции. Это означает, что $f(x_0) = g(x_0)$ для любого $x_0 \in K$. Обозначим через n наивысшую из степеней многочленов $f(x), g(x)$. Так как кольцо K бесконечно, то в нем найдутся $n + 1$ различных элементов $x_1, x_2, \dots, x_{n+1}$. Согласно нашему предположению, многочлены $f(x)$ и $g(x)$ принимают одинаковые значения в каждой из точек $x_1, x_2, \dots, x_{n+1}$ (как и вообще в любой точке). Следствие теоремы 3 позволяет сделать отсюда вывод, что $f(x) = g(x)$.

Теорема 4 вместе с доказанным в п. 4 утверждением о согласованности операций, определенных для многочленов и для функций, означает, что если кольцо K бесконечно, то отображение, которое сопоставляет каждому многочлену из $K[x]$ определяемую им функцию, является изоморфизмом кольца $K[x]$ на некоторое кольцо функций, определенных на K и принимающих значения в K .

Теорема 4 оправдывает, в частности, функциональную трактовку понятия многочлена от действительной переменной, принятую в математическом анализе (см. п. 1). Имея в виду эту теорему, мы и в этой книге будем иногда (в тех случаях, когда кольцо K бесконечно) говорить о многочлене как о функции (подразумевая функцию, определяемую этим многочленом).

Для конечного кольца K утверждение теоремы 4 неверно. Однако при некоторых дополнительных предположениях и в этом случае оказывается возможным из равенства функций, определяемых двумя многочленами, сделать вывод о равенстве самих многочленов.

Пусть, например, $K = \mathbf{Z}_p$ — кольцо вычетов по простому модулю p . Два многочлена $f(x), g(x) \in \mathbf{Z}_p[x]$ будем для краткости называть *эквивалентными*, если они определяют одну и ту же функцию на $\mathbf{Z}_p$; в этом случае будем писать $f(x) \sim g(x)$. Так как в кольце $\mathbf{Z}_p$ имеется p элементов, то из следствия теоремы 3 непосредственно вытекает следующее утверждение:

Теорема 5. Если многочлены $f(x), g(x) \in \mathbf{Z}_p[x]$, имеющие степень не выше чем $p - 1$, эквивалентны, то они равны.

Укажем теперь способ, позволяющий для любого многочлена $f(x) \in \mathbf{Z}_p[x]$ построить эквивалентный ему многочлен $f_0(x)$ степени не выше $p - 1$.

Любое натуральное число n можно представить в виде

$$n = q(p - 1) + r,$$

где $1 \leq r \leq p - 1$. (Если n не делится на $p - 1$, то такое представление получается в результате деления с остатком; если $n = t(p - 1)$, то следует взять $q = t - 1, r = p - 1$.) Докажем, что $x^n \sim x^r$. При $x = \bar{0}$ каждый из многочленов x^n и x^r принимает значение 0; при $x = x_0 \neq \bar{0}$ по малой теореме Ферма (АТЧ III, п. 3 § 4 гл. III) имеем $x_0^{p-1} = \bar{1}$ и, следовательно,

$$x_0^n = (x_0^{p-1})^q \cdot x_0^r = x_0^r.$$

Если теперь в произвольном многочлене $f(x) \in \mathbf{Z}_p[x]$ заменить все степени x эквивалентными им степенями с показателями, не превосходящими $p - 1$, то и получится многочлен $f_0(x)$, эквивалентный $f(x)$ и имеющий степень не выше $p - 1$.

Например, многочлен $\bar{1} - x - x^3 + x^4 - x^5 + x^7 \in \mathbf{Z}_3[x]$ эквивалентен многочлену $\bar{1} - x - x + x^2 - x + x = \bar{1} + x + x^2$.

7. Расширение основного кольца. Если кольцо K является подкольцом кольца L или, что то же самое, кольцо L является расширением кольца K , то всякий многочлен с коэффициентами из K можно рассматривать и как многочлен с коэффициентами из L . При этом действия над такими многочленами в кольце $L[x]$ приводят к тем же результатам, что и действия в кольце $K[x]$. Это означает, что кольцо $K[x]$ является подкольцом кольца $L[x]$.

Пользуясь этим обстоятельством, иногда говорят о значении многочлена $f(x) \in K[x]$ в точке $x_0 \in L$. Это следует понимать таким образом, что $f(x)$ рассматривается в данном случае как элемент кольца $L[x]$. В этом смысле говорят также о корнях многочлена $f(x) \in K[x]$, лежащих в кольце L .

Если кольцо K не является полем, то можно взять в качестве L его поле отношений (АТЧ III, п. 5 § 3 гл. II). Таким спо-

сбором можно иногда доказывать какие-либо утверждения о кольце $K[x]$, исходя из аналогичных утверждений о кольцах многочленов над полями. Этот прием будет использован в § 3 гл. II.

Другой частный случай, когда $K = \mathbf{R}$, а $L = \mathbf{C}$, особенно важен для приложений. Исследование поведения многочлена с действительными коэффициентами в комплексной области (в частности, исследование его комплексных корней) часто бывает полезным, даже если нас интересуют в конечном счете только его свойства в действительной области.

Вложение кольца $K[x]$ в кольцо $L[x]$, где L — расширение кольца K , является частным случаем следующей конструкции. Пусть φ — гомоморфизм кольца K в некоторое кольцо L . Тогда каждому многочлену

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in K[x]$$

можно сопоставить многочлен

$$\varphi(a_0) + \varphi(a_1)x + \varphi(a_2)x^2 + \dots + \varphi(a_n)x^n \in L[x].$$

Поскольку операции сложения и умножения в кольце $L[x]$ определяются такими же формулами, как в кольце $K[x]$, построенное отображение кольца $K[x]$ в кольцо $L[x]$ является гомоморфизмом. В частном случае, когда L — расширение кольца K , а φ — отображение, которое каждому элементу кольца K сопоставляет самого себя, но уже как элемент кольца L , этот гомоморфизм кольца $K[x]$ в кольцо $L[x]$ совпадает с вложением, о котором мы говорили выше.

Рассмотрим другой частный случай. Пусть $K = \mathbf{Z}$ (кольцо целых чисел), $L = \mathbf{Z}_p$ (кольцо вычетов по простому модулю p), а гомоморфизм φ определяется по формуле

$$\varphi(a) = \bar{a} \quad (a \in \mathbf{Z}),$$

где $\bar{a}$ обозначает класс вычетов числа a по модулю p . Соответствующий гомоморфизм кольца $\mathbf{Z}[x]$ в кольцо $\mathbf{Z}_p[x]$ называется *редукцией по модулю p* . По определению, он сопоставляет каждому многочлену

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbf{Z}_p[x] \quad (16)$$

многочлен

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \dots + \bar{a}_nx^n \in \mathbf{Z}_p[x]. \quad (17)$$

Редукция по модулю p часто бывает полезна по той причине, что кольцо $\mathbf{Z}_p$ в отличие от кольца $\mathbf{Z}$, является полем.

Вопросы для самопроверки

1. Приведите примеры функций действительной переменной, не являющихся многочленами.
2. Как определяется произведение двух многочленов с коэффициентами из произвольного кольца?
3. Докажите ассоциативность умножения многочленов с коэффициентами из ассоциативного кольца.
4. Что такое разность двух многочленов?
5. Чему равна степень произведения двух многочленов над областью целостности?
6. Какие элементы в кольце многочленов над областью целостности обратимы?

7. В каком случае степень суммы двух многочленов меньше максимальной из их степеней?

8. Как определяется равенство многочленов?

9. Приведите пример ненулевого многочлена над полем из двух элементов, значения которого во всех точках равны нулю.

10. Докажите, что при сложении многочленов складываются и определяемые ими функции.

11. Сколько значений многочлена степени n нужно знать для того, чтобы определить его коэффициенты?

12. Что такое эквивалентные многочлены над полем вычетов по модулю p ?

13. Как построить многочлен степени меньше p , эквивалентный данному многочлену $f(x) \in \mathbf{Z}_p[x]$?

14. Каково необходимое и достаточное условие того, чтобы многочлен $f(x)$ делился на $x - x_0$ в кольце $K[x]$?

15. Для чего служит схема Горнера?

16. Докажите, что если $x_1, x_2, \dots, x_m$ — (различные) корни многочлена $f(x)$, то $f(x)$ делится на $(x - x_1)(x - x_2) \dots (x - x_m)$.

17. Какое максимальное число корней может иметь ненулевой многочлен степени n ?

18. Как определить значение многочлена с коэффициентами из кольца K в точке $x_0 \in L$, где L — расширение кольца K ?

19. Какие трудности встретились бы при развитии функциональной точки зрения на многочлены над неассоциативным или некоммутативным кольцом?

Упражнения

1. Пользуясь схемой Горнера, разделите с остатком многочлен $f(x) \in \mathbf{R}[x]$ на $x - x_0$ и вычислите $f(x_0)$:

а) $f(x) = x^4 - 3x^3 + 6x^2 - 10x + 16, x_0 = 4$;

б) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1, x_0 = -1$.

2. Пользуясь схемой Горнера, найдите значение многочлена $f(x) \in \mathbf{C}[x]$ в точке x_0 :

а) $f(x) = x^4 + 2ix^3 - (1 + i)x^2 - 3x + 7 + i, x_0 = -i$;

б) $f(x) = x^5 + (1 + 2i)x^4 - (1 + 3i)x^2 + 7, x_0 = -2 - i$.

3. Пользуясь схемой Горнера, составьте таблицу всех значений многочлена $f(x) \in \mathbf{Z}_p[x]^*$:

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

б) $f(x) = 3x^5 + x^3 - 2x + 1, p = 7$.

4. В кольце $\mathbf{Z}_7[x]$ найдите многочлен наименьшей степени, эквивалентный многочлену $f(x)^*$:

а) $f(x) = 4x^{21} + x^{18} + 2x^{10} - x^8 + 3x^5 - x - 3$;

б) $f(x) = 2x^{16} + x^{11} + 3x^{10} - x^5 + 2x^4$.

* Для удобства мы обозначаем класс вычетов $\bar{n}$, содержащий целое число n , просто через n .

§ 2. КОРНИ МНОГОЧЛЕНА

Напомним, что элемент x_0 кольца K называется *корнем* многочлена $f(x) \in K[x]$, если $f(x_0) = 0$. Отыскание корней заданного многочлена $f(x)$ или, что то же самое, решение *алгебраического уравнения* $f(x) = 0$ — это задача, которая часто возникает в различных разделах математики и в ее приложениях. (Для приложений наиболее важен, конечно, случай, когда K есть поле действительных или комплексных чисел.) Разработка методов решения алгебраических уравнений стимулировала развитие многих разделов алгебры, в том числе алгебры многочленов и теории групп.

В отличие от § 1, где дается определение и исследуются простейшие свойства кольца многочленов над произвольной областью целостности, в данном параграфе, как и в большинстве других параграфов книги, рассматриваются только многочлены над полем, что обусловлено следующими причинами:

1) случай, когда кольцо коэффициентов является полем, наиболее важен;

2) свойства колец многочленов над полями отличаются наибольшей простотой;

3) поскольку кольцо многочленов над областью целостности K является подкольцом кольца многочленов над ее полем отношений P , многие свойства кольца $K[x]$ могут быть доказаны, исходя из аналогичных свойств кольца $P[x]$. (Последнее соображение хорошо иллюстрируется материалом, изложенным в § 3 гл. II.)

В данном параграфе доказываются некоторые общие теоремы о корнях многочленов над произвольным полем P . В гл. IV и V будут более подробно рассмотрены частные случаи, когда $P = \mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$.

1. Число корней. В п. 6 § 1 было установлено, что *число корней ненулевого многочлена степени n не превосходит n* (теорема 3).

Для любого натурального n можно указать многочлены степени n , имеющие ровно n корней. Например, многочлен $(x - 1)(x - 2) \dots (x - n)$ над полем $\mathbb{R}$ имеет n корней $1, 2, \dots, n$. В то же время существуют многочлены, число корней которых меньше их степени*. Так, многочлен $x^2 + 1 \in \mathbb{R}[x]$, степень которого равна 2, вообще не имеет корней. Естествен поэтому интерес к вопросу о точном числе корней многочлена и, в частности, о существовании хотя бы одного корня. Общего ответа на этот вопрос для многочленов над любыми полями дать нельзя. (Что касается многочленов над полями $\mathbb{C}$ и $\mathbb{R}$, то им будет специально посвящена гл. IV.) Кроме того, как будет показано в следующих пунктах, сама постановка вопроса о числе корней многочлена нуждается в уточнении.

2. Кратные корни. Пусть $f(x)$ — многочлен с коэффициентами из поля P и x_0 — его корень. Согласно теореме Безу (см. п. 5 § 1),

* Здесь имеются в виду корни, лежащие в данном поле P .

многочлен $f(x)$ делится на $x - x_0$. Может случиться, что $f(x)$ делится не только на $x - x_0$, но и на $(x - x_0)^2$ или даже на более высокую степень $x - x_0$. Наибольшее целое число k такое, что $f(x)$ делится на $(x - x_0)^k$, называется *кратностью корня* x_0 многочлена $f(x)$. Иначе говоря, кратность корня x_0 равна k , если $f(x)$ делится на $(x - x_0)^k$, но не делится на $(x - x_0)^{k+1}$. Если $k > 1$, то говорят, что x_0 — *кратный корень*; если $k = 1$, то x_0 называется *простым корнем* многочлена $f(x)$.

Удобно считать, что приведенное выше определение кратности корня применимо и для $k = 0$. В таком случае корень кратности 0 — это элемент поля P , вообще не являющийся корнем многочлена $f(x)$.

Пример 1. Найдем кратность корня $x_0 = 1$ многочлена

$$f(x) = x^5 - 5x^4 - 2x^3 + 26x^2 - 31x + 11 \in \mathbf{R}[x].$$

Делим $f(x)$ последовательно на $x - 1$ до тех пор, пока не получим ненулевой остаток. Деление удобно производить по схеме Горнера (см. п. 5 § 1):

		1	-5	-2	26	-31	11
1		1	-4	-6	20	-11	0
		1	-3	-9	11	0	
		1	-2	-11	0		
		1	-1	-12			

При этом вторая строка, содержащая коэффициенты частного $f_1(x)$ от деления $f(x)$ на $x - 1$, служит одновременно первой строкой схемы Горнера для деления $f_1(x)$ на $x - 1$. Коэффициенты частного $f_2(x)$, получающегося при этом делении, располагаются в третьей строке, которая служит одновременно первой строкой схемы Горнера для деления $f_2(x)$ на $x - 1$ и т. д.

Результаты вычислений показывают, что $f(x)$ делится на $(x - 1)^3$, но не делится на $(x - 1)^4$. Следовательно, кратность корня $x_0 = 1$ многочлена $f(x)$ равна 3.

Пример 2. Найдем кратность корня $x_0 = -1$ многочлена

$$f(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbf{Z}_3[x].$$

Делим последовательно $f(x)$ на $x + 1$:

		$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$
$-\bar{1}$		$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$
		$\bar{1}$	$-\bar{1}$	$-\bar{1}$	$\bar{1}$	$\bar{0}$	
		$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{0}$		
		$\bar{1}$	$\bar{0}$	$\bar{1}$			

Искомая кратность равна 3.

Если известно, что многочлен $f(x)$ делится на $(x - x_0)^k$, т. е. что $f(x) = (x - x_0)^k g(x)$, где $g(x) \in P[x]$, и требуется узнать, делится ли $f(x)$ на $(x - x_0)^{k+1}$, то надо проверить, делится ли $g(x)$ на $x - x_0$. По теореме Безу $g(x)$ не делится на $x - x_0$ тогда и только тогда, когда $g(x_0) \neq 0$. Следовательно, элемент x_0 поля P будет корнем кратности k многочлена $f(x) \in P[x]$ тогда и только тогда, когда $f(x) = (x - x_0)^k g(x)$, где $g(x) \in P[x]$, причем $g(x_0) \neq 0$.

Например, многочлен

$$f(x) = (x - 2)^2 (x^5 - 10x + 1) \in R[x]$$

имеет число 2 корнем кратности 2, поскольку многочлен $x^5 - 10x + 1$ в точке 2 не обращается в 0.

Для многочленов с действительными коэффициентами понятия простого и кратного корня имеют следующий геометрический смысл. Корень x_0 многочлена $f(x) \in R[x]$ является простым, если график многочлена $f(x)$ при $x = x_0$ пересекает ось абсцисс, не касаясь ее (рис. 1). Корень x_0 является кратным, если график многочлена $f(x)$ при $x = x_0$ касается оси абсцисс; при этом кратность определяется порядком касания (рис. 2).

В самом деле, если x_0 — корень кратности k , то

$$f(x) = (x - x_0)^k g(x),$$

где $g(x_0) = c \neq 0$.

В этом случае имеем:

$$\lim_{x \rightarrow x_0} \frac{f(x)}{c(x - x_0)^k} = 1,$$

или, что то же,

$$f(x) = c(x - x_0)^k + o(x - x_0)^k.$$

Последнее равенство показывает, что если $k = 1$, то график многочлена $f(x)$ при $x = x_0$ касается прямой $y = c(x - x_0)$; если же $k > 1$, то он касается оси абсцисс, причем порядок касания равен $k - 1$.

3. Число корней с учетом кратностей. Если дискриминант квадратного трехчлена равен нулю, то при вычислении его корней по известной формуле решения квадратного уравнения получаются два одинаковых числа. В школьной алгебре говорят в

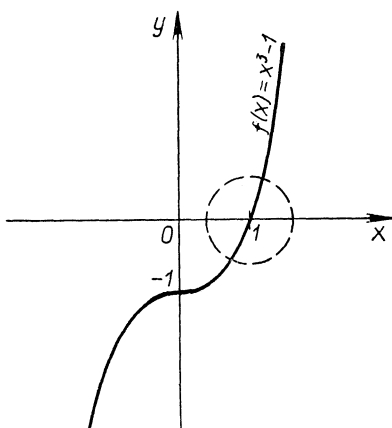


Рис. 1

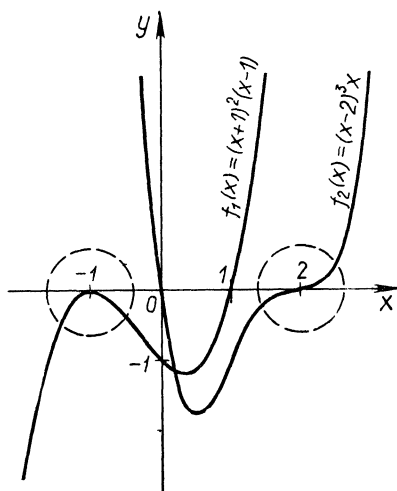


Рис. 2

таких случаях о двух «совпадающих» корнях. Известно, что это бывает тогда и только тогда, когда квадратный трехчлен представляется в виде $c(x - x_0)^2$, т. е. согласно определению, данному в п. 2, имеет двукратный корень. Таким образом, выражение «два совпадающих корня» следует понимать как «один двукратный корень».

Однако вольность речи, которую мы допускаем, говоря о двух или нескольких «совпадающих» корнях, имеет под собой серьезные основания. Подсчитывая число корней многочлена, разумно считать кратный корень столько раз, какова его кратность. В частности, при таком соглашении остается справедливой теорема о том, что число корней многочлена не превосходит его степени. Сформулируем это утверждение более точно.

Т е о р е м а 1. *Сумма кратностей всех корней ненулевого многочлена $f(x)$ не превосходит его степени, причем равенство имеет место тогда и только тогда, когда многочлен $f(x)$ разлагается на линейные множители.*

Заметим, что сумма кратностей всех корней — это и есть число корней, если каждый из них учитывать столько раз, какова его кратность. В дальнейшем мы будем вместо «сумма кратностей всех корней» говорить «число корней с учетом кратностей» или просто «число корней».

Доказательство теоремы 1 будет основано на следующих двух леммах:

Л е м м а 1. *Всякий ненулевой многочлен $f(x) \in P[x]$ может быть представлен в виде*

$$f(x) = (x - x_1)^{k_1} (x - x_2)^{k_2} \dots (x - x_s)^{k_s} g(x), \quad (1)$$

где $x_1, \dots, x_s$ — различные элементы поля P , а $g(x)$ — многочлен, не имеющий корней.

Д о к а з а т е л ь с т в о. Если многочлен $f(x)$ не имеет корней, то доказывать нечего. В противном случае пусть x_1 — какой-либо корень многочлена $f(x)$. Тогда по теореме Безу

$$f(x) = (x - x_1) f_1(x).$$

Если x_2 — корень многочлена $f_1(x)$, то $f_1(x) = (x - x_2) f_2(x)$ и, следовательно,

$$f(x) = (x - x_1)(x - x_2) f(x).$$

Продолжая этот процесс, мы в конце концов представим многочлен $f(x)$ в виде

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_t) g(x),$$

где $g(x)$ — многочлен, не имеющий корней. Собрав одинаковые множители, мы получим представление вида (1).

Л е м м а 2. *Если многочлен $f(x)$ представлен в виде (1), то $x_1, x_2, \dots, x_s$ — это все его корни, причем кратность корня x равна k_i .*

Например, многочлен

$$f(x) = (x+1)^3(x-2)(5x^4+1) \in R[x]$$

имеет трехкратный корень -1 и простой корень 2 .

Д о к а з а т е л ь с т в о. Если $x_0 \neq x_1, x_2, \dots, x_s$, то $f(x_0) = (x_0 - x_1)^{k_1} (x_0 - x_2)^{k_2} \dots (x_0 - x_s)^{k_s} g(x_0) \neq 0$. Следовательно, $f(x)$ не имеет корней, отличных от $x_1, x_2, \dots, x_s$. Далее, поскольку

$$f(x) = (x - x_1)^{k_1} ((x - x_2)^{k_2} \dots (x - x_s)^{k_s} g(x)),$$

причем многочлен $(x - x_2)^{k_2} \dots (x - x_s)^{k_s} g(x)$ не обращается в нуль в точке x_1 , то кратность корня x_1 равна k_1 .

Д о к а з а т е л ь с т в о т е о р е м ы 1. Представим многочлен $f(x)$ в виде (1). Тогда

$$\text{ст. } f(x) = k_1 + k_2 + \dots + k_s + \text{ст. } g(x) \geq k_1 + k_2 + \dots + k_s, \quad (2)$$

а по лемме 2 $k_1 + k_2 + \dots + k_s$ и есть сумма кратностей всех корней многочлена $f(x)$. Тем самым доказано первое утверждение теоремы.

Если в (2) имеет место равенство, то $\text{ст. } g(x) = 0$, т. е. $g(x) = a$ — ненулевой элемент поля P и

$$f(x) = a(x - x_1)^{k_1} (x - x_2)^{k_2} \dots (x - x_s)^{k_s}. \quad (3)$$

«Рассыпав» степени $(x - x_i)^{k_i}$ на отдельные множители вида $x - x_i$, мы получим разложение многочлена $f(x)$ на линейные множители.

Обратно, пусть многочлен $f(x)$ разлагается на линейные множители, т. е.

$$f(x) = a_0(a_1x + b_1)(a_2x + b_2) \dots (a_nx + b_n),$$

где $a_0, a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in P$, причем $a_0, a_1, a_2, \dots, a_n$ отличны от нуля. Вынеся за скобки коэффициенты при x и собрав одинаковые множители, мы получим тогда представления многочлена $f(x)$ в виде (3), например:

$$\begin{aligned} & \frac{3}{2}(2x+1)\left(\frac{1}{3}x-1\right)\left(5x+\frac{5}{2}\right) = \\ & = \left(\frac{3}{2} \cdot 2 \cdot \frac{1}{3} \cdot 5\right)\left(x+\frac{1}{2}\right)(x-3)\left(x+\frac{1}{2}\right) = 5\left(x+\frac{1}{2}\right)^2(x-3). \end{aligned}$$

Из равенства (3) следует, что $\text{ст. } f(x) = k_1 + k_2 + \dots + k_s$, а по лемме 2 $k_1 + k_2 + \dots + k_s$ и есть сумма кратностей всех корней многочлена $f(x)$.

Теорема полностью доказана.

В § 2 гл. IV будет показано, что *всякий многочлен $f(x) \in C[x]$ степени $n \geq 1$ разлагается на линейные множители и, стало быть, имеет n корней*. Если $f(x)$ — многочлен степени $n \geq 1$ с коэффициентами из какого-либо числового поля P (т. е. подполя поля C), то в кольце $P[x]$ он, вообще говоря, не разлагается на линейные множители, но всегда может быть разложен на линейные множители в кольце $C[x]$.

Можно доказать, что для любого поля P и любого многочлена $f(x) \in P[x]$ степени $n \geq 1$ существует такое расширение L поля P , что $f(x)$ разлагается на линейные множители в кольце $L(x)$. Мы не будем доказывать этой теоремы, так как в наиболее важном для нас случае, когда P — числовое поле, в качестве такого расширения L , как мы заметили выше, можно взять поле C .

4. Формулы Виета. Если многочлен $f(x)$ степени n имеет n корней (с учетом кратностей), то его коэффициенты могут быть выражены через корни и старший коэффициент по так называемым формулам Виета.

Пусть

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n,$$

причем $a_0 \neq 0$, и пусть $x_1, x_2, \dots, x_n$ — корни многочлена, каждый из которых повторен столько раз, какова его кратность. Тогда коэффициент a_k ($k = 1, 2, \dots, n$) равен произведению $(-1)^k a_0$ на сумму всевозможных произведений по k элементов из $x_1, x_2, \dots, x_n$, т. е.

$$\begin{aligned} a_1 &= -a_0(x_1 + x_2 + \dots + x_n), \\ a_2 &= a_0(x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n), \\ a_n &= (-1)^n a_0 x_1 x_2 \dots x_n. \end{aligned} \quad (4)$$

(Выражение для a_k содержит C_n^k слагаемых.) Формулы (4) и называются формулами Виета.

Для вывода формул Виета воспользуемся теоремой 1. Согласно этой теореме, многочлен $f(x)$ при сделанных предположениях может быть представлен в виде

$$f(x) = a_0(x - x_1)(x - x_2) \dots (x - x_n). \quad (5)$$

Напомним, что $x_1, x_2, \dots, x_n$ не обязательно различны. Точнее, каждый корень многочлена $f(x)$ встречается в последовательности $x_1, x_2, \dots, x_n$ столько раз, какова его кратность. Столько же раз повторяется и соответствующий линейный множитель в разложении (5).

Выполним умножение в правой части равенства (5), воспользовавшись свойством дистрибутивности. Члены, содержащие x^{n-k} , будут получаться при перемножении первых слагаемых из каких-то $n - k$ скобок и вторых слагаемых из остальных k скобок. Коэффициент каждого такого члена будет равен произведению каких-то k элементов из $x_1, x_2, \dots, x_n$, умноженному на $(-1)^k a_0$. После приведения подобных членов в правой части равенства (5) получится многочлен, коэффициент которого при x^{n-k} равен сумме всевозможных произведений по k элементов из $x_1, x_2, \dots, x_n$, умноженной на $(-1)^k a_0$. Приравняв коэффициенты этого многочлена соответствующим коэффициентам многочлена $f(x)$, получим формулы (4).

Формулы Виета могут быть записаны также в следующем виде:

$$x_1 + x_2 + \dots + x_n = -\frac{a_1}{a_0},$$

$$x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n = \frac{a_2}{a_0}, \quad (6)$$

$$x_1 x_2 \dots x_n = (-1)^n \frac{a_n}{a_0}.$$

В частности, для квадратного трехчлена $f(x) = ax^2 + bx + c$ получаем формулы, известные из школьного курса алгебры:

$$x_1 + x_2 = -\frac{b}{a}, \quad x_1 x_2 = \frac{c}{a}.$$

Для нормированного многочлена $f(x)$ формулы (6) принимают более простой вид:

$$\begin{aligned} x_1 + x_2 + \dots + x_n &= -a_1, \\ x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n &= a_2, \\ &\vdots \\ x_1x_2 \dots x_n &= (-1)^n a_n. \end{aligned} \quad (7)$$

Подчеркнем, что формулы Виета имеют смысл лишь тогда, когда число корней многочлена $f(x)$ равно его степени; например, это имеет место для любых многочленов над полем комплексных чисел.

Пример 3. Запишем формулы Виета для многочлена $f(x) = 4x^3 - x^2 - 2x + 4 \in C[x]$:

$$\begin{aligned}x_1 + x_2 + x_3 &= -\frac{-1}{4} = \frac{1}{4}, \\x_1x_2 + x_1x_3 + x_2x_3 &= \frac{-2}{4} = -\frac{1}{2}, \\x_1x_2x_3 &= -\frac{4}{4} = -1.\end{aligned}$$

Пример 4. Найдем нормированный многочлен четвертой степени с действительными коэффициентами, имеющий двукратный корень 2 и простые корни 3, -1 .

Искомый многочлен имеет вид

$$f(x) = (x - 2)^2(x - 3)(x + 1).$$

Его коэффициенты могут быть найдены по формулам Виета, если положить $x_1 = x_2 = 2$, $x_3 = 3$, $x_4 = -1$. Считая $a_0 = 1$, имеем:

$$\begin{aligned} a_1 &= -(2 + 2 + 3 - 1) = -6, \\ a_2 &= 2 \cdot 2 + 2 \cdot 3 - 2 \cdot 1 + 2 \cdot 3 - 2 \cdot 1 - 3 \cdot 1 = 9, \\ a_3 &= -(2 \cdot 2 \cdot 3 - 2 \cdot 2 \cdot 1 - 2 \cdot 3 \cdot 1 - 2 \cdot 3 \cdot 1) = 4, \\ a_4 &= -2 \cdot 2 \cdot 3 \cdot 1 = -12. \end{aligned}$$

Таким образом,

$$f(x) = x^4 - 6x^3 + 9x^2 + 4x - 12.$$

Пример 5. Считая известным, что многочлен

$$f(x) = x^4 - 4x^3 + 3x - 1 \in \mathbf{R}[x]$$

имеет 4 действительных корня, вычислим сумму их квадратов.

Обозначим корни данного многочлена через x_1, x_2, x_3, x_4 . Воспользуемся тождеством

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = (x_1 + x_2 + x_3 + x_4)^2 - 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4).$$

По формулам (7)

$$\begin{aligned}x_1 + x_2 + x_3 + x_4 &= 4, \\x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 &= 0.\end{aligned}$$

Следовательно,

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 16.$$

Пример 6. Докажем «теорему Вильсона»: *при любом простом p имеет место сравнение*

$$(p-1)! \equiv -1 \pmod{p}.$$

Согласно малой теореме Ферма, все ненулевые элементы поля $\mathbf{Z}_p$ вычетов по модулю p являются корнями многочлена $x^{p-1} - \bar{1} \in \mathbf{Z}_p[x]$. Так как в поле $\mathbf{Z}_p$ имеется $p-1$ ненулевых элементов, то этот многочлен разлагается на линейные множители в кольце $\mathbf{Z}_p[x]$, причем все его корни простые. Их произведение есть вычет по модулю p числа $(p-1)!$, а по формуле Виета оно равно $-\bar{1}$. Отсюда и получаем теорему Вильсона.

5. Алгебраические сравнения по простому модулю. Пусть p — простое число. *Алгебраическим сравнением по модулю p* называется сравнение вида

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \equiv 0 \pmod{p}, \quad (8)$$

где $a_0, a_1, \dots, a_{n-1}, a_n$ — целые числа, а x — неизвестное, допустимые значения которого также целые. Из общих свойств сравнений (АТЧ III, § 1 гл. III) следует, что:

1) если коэффициенты сравнения (8) заменить любыми целыми числами, сравнимыми с ними по модулю p , то полученное сравнение будет эквивалентно сравнению (8);

2) если x_0 — решение сравнения (8), то и любое целое число, сравнимое с x_0 по модулю p , будет решением этого сравнения.

Сравнение (8) называется *тривиальным*, если все коэффициенты $a_0, a_1, \dots, a_{n-1}, a_n$ делятся на p . В этом случае оно выполняется для любых значений x . Нетривиальное алгебраическое сравнение можно, пользуясь свойством 1, привести к такому виду, в котором a_0 не делится на p . Для этого надо просто отбросить те первые несколько членов (если они есть), коэффициенты которых делятся на p . При условии, что a_0 не делится на p , число n называется *степенью* сравнения (8).

Для любого целого числа a будем обозначать через $\bar{a}$ класс вычетов по модулю p , содержащий a . Из определения операций над классами вычетов следует, что при любом $x_0 \in \mathbf{Z}$

$$\overline{a_0 x_0^n + a_1 x_0^{n-1} + \dots + a_{n-1} x_0 + a_n} = \overline{a_0} \overline{x_0^n} + \overline{a_1} \overline{x_0^{n-1}} + \dots + \overline{a_{n-1}} \overline{x_0} + \overline{a_n}. \quad (9)$$

Число x_0 является решением сравнения (8) тогда и только тогда, когда

$$\overline{a_0 x_0^n + a_1 x_0^{n-1} + \dots + a_{n-1} x_0 + a_n} = \overline{0}.$$

В силу (9), последнее равенство может быть переписано в виде

$$\overline{a_0} \overline{x_0^n} + \overline{a_1} \overline{x_0^{n-1}} + \dots + \overline{a_{n-1}} \overline{x_0} + \overline{a_n} = \overline{0},$$

а это означает, что класс вычетов $\overline{x_0}$ является решением алгебраического уравнения

$$\overline{a_0} x^n + \overline{a_1} x^{n-1} + \dots + \overline{a_{n-1}} x + \overline{a_n} = \overline{0} \quad (10)$$

над полем $\mathbf{Z}_p$ вычетов по модулю p .

Таким образом, алгебраическое сравнение по простому модулю p лишь формально отличается от алгебраического уравнения над полем $\mathbf{Z}_p$.

Будем называть *классом решений* сравнения (8) совокупность его решений, составляющих один класс вычетов по модулю p . Такой класс соответствует одному решению уравнения (10). Очевидно, что степень уравнения (10) равна степени сравнения (8). Из теоремы 3 § 1 получаем следующую теорему:

Т е о р е м а 2. *Число классов решений нетривиального алгебраического сравнения по простому модулю не превосходит его степени.*

С другой стороны, ясно, что число классов решений любого алгебраического сравнения не может быть больше p (числа всех классов вычетов по модулю p). Поэтому при $n \geq p$ теорема 2 ничего не дает. Однако в п. 6 § 1 было указано, как по любому многочлену $f(x) \in \mathbf{Z}_p[x]$ построить многочлен $f_0(x) \in \mathbf{Z}_p[x]$ степени не выше $p-1$, принимающий во всех точках те же значения, что и $f(x)$. Очевидно, что уравнение $f_0(x) = 0$ будет эквивалентно уравнению $f(x) = 0$. Пользуясь этим способом, можно любое алгебраическое сравнение заменить эквивалентным ему сравнением степени не выше $p-1$ (быть может, тривиальным). Например, сравнение

$$x^7 - x^5 + x^4 - x^3 - x - 1 \equiv 0 \pmod{3}$$

эквивалентно сравнению

$$x^2 + x + 1 \equiv 0 \pmod{3}$$

(см. пример, приведенный в п. 6 § 1).

Алгебраическое уравнение над конечным полем можно (по крайней мере, в принципе) решить путем поочередной подстановки в него всех элементов поля. Поэтому и решение алгебраического сравнения сводится к конечному перебору.

П р и м е р 7. Решим сравнение

$$8x^9 - 17x^8 + 31x^6 + 12x^5 - 7x^4 + 2x + 11 \equiv 0 \pmod{5}.$$

Переходим сразу к соответствующему алгебраическому уравнению над полем $\mathbf{Z}_5$:

$$\bar{3}x^9 + \bar{3}x^8 + \bar{1}x^6 + \bar{2}x^5 + \bar{3}x^4 + \bar{2}x + \bar{1} = 0.$$

Для удобства договоримся опускать черту в обозначениях классов вычетов. Заменяя левую часть полученного уравнения эквивалентным многочленом

$$3x + 3x^4 + x^2 + 2x + 3x^4 + 2x + 1 = x^4 + x^2 + 2x + 1,$$

приходим к уравнению

$$x^4 + x^2 + 2x + 1 = 0.$$

Пользуясь схемой Горнера, испытываем значения $x = 0, \pm 1, \pm 2$ (т. е. все значения, которые может принимать x):

	1	0	1	2	1
0					1
1	1	1	2	-1	0
2	1	2	0	2	0
-1	1	-1	2	0	1
-2	1	-2	0	2	2

Мы видим, что уравнение имеет два решения: 1 и 2. Решениями исходного сравнения, следовательно, будут числа вида $5k + 1$ и $5k + 2$.

Пример 8. Решим сравнение

$$x^{100} + 10x^{51} + 10x^{10} + 100x \equiv 0 \pmod{11}.$$

Переходим к уравнению над полем $\mathbf{Z}_{11}$:

$$x^{100} - x^{51} - x^{10} + x = 0.$$

Левая часть этого уравнения эквивалентна многочлену $x^{10} - x - x^{10} + x = 0$, так что уравнение эквивалентно тривиальному уравнению $0 = 0$. Его решениями являются все элементы поля $\mathbf{Z}_{11}$, а решениями исходного сравнения — все целые числа.

Вопросы для самопроверки

1. Приведите пример многочлена четвертой степени над полем действительных чисел, не имеющего корней в этом поле.

2. Приведите пример многочлена третьей степени над полем рациональных чисел, имеющего ровно один (простой) корень в этом поле.

3. Что называется кратностью корня многочлена?

4. Что такое простой корень?

5. Что такое корень кратности 0?

6. Какова кратность корня 0 многочлена x^n ?

7. Какова кратность корня -1 многочлена $(x + 1)^4 (x^4 - 2x^3 - 3x - 5)$?
8. Какое максимальное число корней с учетом их кратностей может иметь многочлен степени n ?
9. Что такое разложение многочлена на линейные множители?
10. В каком случае многочлен может быть разложен на линейные множители?
11. Какие корни имеет многочлен $x^3 (x + 2) (x - 3)^3 (x - 4)^2$? Укажите их кратности.
12. Докажите, что всякий многочлен $f(x) \in P[x]$ допускает не более одного разложения на линейные множители с точностью до перестановки множителей и умножения их на элементы поля P .
13. Запишите формулы Виета. В каком случае они имеют место?
14. Какой вид принимают формулы Виета для нормированного многочлена?
15. Что такое алгебраическое сравнение?
16. Что такое класс решений алгебраического сравнения?
17. Какова связь между алгебраическими сравнениями по простому модулю и алгебраическими уравнениями над соответствующим полем вычетов?
18. Какое максимальное число классов решений может иметь алгебраическое сравнение степени n ?
19. Сколько классов решений имеет тривиальное алгебраическое сравнение?

Упражнения

1. Определите кратность корня x_0 многочлена $f(x) \in R[x]$:
 - а) $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$, $x_0 = 2$;
 - б) $f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16$, $x_0 = -2$.
2. Определите кратность корня x_0 многочлена $f(x) \in \mathbb{Z}_p[x]$:
 - а) $f(x) = x^5 + 2x^4 - 2x^2 - 3x - 1$, $x_0 = 2$, $p = 7$;
 - б) $f(x) = 2x^4 + x^3 - 2x^2 - 1$, $x_0 = -2$, $p = 5$.
3. При помощи формул Виета найдите нормированный многочлен четвертой степени с комплексными коэффициентами, имеющий данные корни x_1, x_2, x_3, x_4 :
 - а) $x_1 = 1$, $x_2 = 2$, $x_3 = -3$, $x_4 = -4$;
 - б) $x_1 = x_2 = x_3 = -1$, $x_4 = i$;
 - в) $x_1 = x_2 = 1 + i$, $x_3 = x_4 = 2$.
4. Найдите сумму квадратов и произведение всех корней многочлена $f(x) \in \mathbb{C}[x]$:
 - а) $f(x) = 3x^5 - x^3 + x + 2$;
 - б) $f(x) = x^4 + (1 + i)x^3 + (2 + 3i)x^2 - x + (3 + i)$;
 - в) $f(x) = x^n + ax^{n-1} + b$, $n \geq 3$.

5. Найдите сумму чисел, обратных корням многочлена $f(x) \in \mathbb{C}[x]$:

а) $f(x) = 3x^3 + 2x^2 - 1$;

б) $f(x) = x^4 - x^2 - x - 1$.

6. Найдите площадь треугольника, длины сторон которого есть корни уравнения: $x^3 - 10x^2 + 31x - 29 = 0$.

(У к а з а н и е. Воспользуйтесь формулой Герона.)

7. Решите алгебраическое сравнение:

а) $6x^7 + 12x^6 + x^5 + 9x^4 + x^3 + 13x + 4 \equiv 0 \pmod{5}$;

б) $x^7 + x^5 + x^3 + x^2 \equiv 1 \pmod{3}$;

в) $x^{100} + 100x^2 \equiv 10 \pmod{11}$;

г) $x^6 + x^3 + 1 \equiv 0 \pmod{7}$.

ТЕОРИЯ ДЕЛИМОСТИ В КОЛЬЦЕ МНОГОЧЛЕНОВ

§ 1. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

1. Деление с остатком. Между кольцом многочленов от одной переменной над полем и кольцом целых чисел имеется глубокая аналогия. Эта аналогия касается свойств делимости: разложения на простые множители, строения идеалов и т. д. Ее причина состоит в том, что в обоих этих кольцах выполнимо «деление с остатком», благодаря чему они являются евклидовыми кольцами.

Напомним определение евклидова кольца (АТЧ III, п. 6 § 2 гл. II). Область целостности K называется *евклидовым кольцом*, если на $K \setminus \{0\}$ задана функция N , принимающая неотрицательные целые значения, и выполняется свойство (E):

для любых $a, b \in K, b \neq 0$, существуют такие $q, r \in K$, что $a = qb + r$ и $N(r) < N(b)$ или $r = 0$.

Процедура отыскания таких элементов q и r для заданных элементов a и b называется *делением с остатком* в кольце K . При этом q называется *неполным частным*, а r — *остатком* от деления a на b .

Для кольца многочленов от одной переменной над полем в качестве функции N можно взять степень. Свойство (E) вытекает тогда из следующей теоремы:

Теорема 1. Пусть P — произвольное поле, f и g — многочлены с коэффициентами из P , причем $g \neq 0$. Тогда существует, и притом единственная, пара многочленов $q, r \in P[x]$, удовлетворяющая условиям:

$$1) f = qg + r;$$

$$2) \text{ ст. } r < \text{ ст. } g.$$

(Напомним, что $\text{ст. } 0 = -\infty$, поэтому второе условие будет выполнено, в частности, если $r = 0$.)

Доказательство. Пусть

$$f = a_0x^n + a_1x^{n-1} + \dots + a_n,$$

$$g = b_0x^m + b_1x^{m-1} + \dots + b_m,$$

причем $a_0 \neq 0, b_0 \neq 0$.

Если $n < m$, то можно взять $q = 0, r = f$. Пусть теперь $n \geq m$. Положим тогда

$$f_1 = f - c_0x^{n-m}g,$$

где $c_0 = \frac{a_0}{b_0}$.

Очевидно, что ст. $f_1 \leq n - 1$. Пусть

$$f_1 = a'_0 x^{n-1} + a'_1 x^{n-2} + \dots + a'_{n-2} x + a'_{n-1}.$$

Положим

$$f_2 = f_1 - c_1 x^{n-m-1} g,$$

где $c_1 = \frac{a'_0}{b_0}$.

Очевидно, что ст. $f_2 \leq n - 2$. Продолжая этот процесс, получим последовательность многочленов $f_1, f_2, \dots$, причем ст. $f_k \leq n - k$. Последним будет многочлен f_{n-m+1} , степень которого меньше степени g . Имеем:

$$f_{n-m+1} = f - c_0 x^{n-m} g - c_1 x^{n-m-1} g - \dots - c_{n-m} g,$$

откуда

$$f = (c_0 x^{n-m} + c_1 x^{n-m-1} + \dots + c_{n-m}) g + f_{n-m+1}.$$

Многочлены

$$q = c_0 x^{n-m} + c_1 x^{n-m-1} + \dots + c_{n-m}, \quad r = f_{n-m+1}$$

удовлетворяют требованиям теоремы.

Докажем теперь единственность пары многочленов q, r , удовлетворяющей требованиям теоремы.

Предположим, что

$$f = q_1 g + r_1 = q_2 g + r_2,$$

причем ст. $r_1 < \text{ст. } g$ и ст. $r_2 < \text{ст. } g$. Тогда

$$(q_1 - q_2) g = r_2 - r_1.$$

Если $q_1 \neq q_2$, то ст. $(q_1 - q_2)g \geq \text{ст. } g$, в то время как ст. $(r_2 - r_1) < \text{ст. } g$. Следовательно, $q_1 = q_2$, но тогда и $r_1 = r_2$. Теорема доказана.

Таким образом, кольцо $P[x]$ является евклидовым кольцом. Кроме того, оно обладает тем свойством, что деление с остатком выполняется в нем однозначно (что не требуется в определении евклидова кольца).

Практически при делении многочленов с остатком результаты промежуточных вычислений удобно располагать так же, как это делается при делении целых чисел.

Пример 1. В кольце $R[x]$ разделим с остатком многочлен

$$f = 4x^5 - 2x^3 + x^2 + x + 2$$

на многочлен

$$g = 2x^3 - x^2 - x + 1.$$

Вычисления выполним по следующей схеме:

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

(В правом столбце под делителем последовательно выписываются члены неполного частного. В левом столбце выписываются многочлены $f, f_1, f_2, \dots$ и те кратные многочлены g , которые из них вычитаются в соответствии с доказательством теоремы.)

Таким образом,

$$q = 2x^2 + x + \frac{1}{2}, \quad r = \frac{1}{2}x^2 + \frac{1}{2}x + \frac{3}{2}.$$

Заметим, что деление в обычном смысле слова можно понимать как частный случай деления с остатком. А именно: многочлен f делится на многочлен g тогда и только тогда, когда при делении f на g с остатком получается остаток, равный нулю; в этом случае частное $\frac{f}{g}$ совпадает с неполным частным.

2. Идеалы. В одной из предыдущих глав курса алгебры и теории чисел (АТЧ III, § 2 гл. II) была изложена теория делимости в произвольных евклидовых кольцах. Посмотрим, как выглядят основные понятия и положения этой теории в частном случае кольца $P[x]$ многочленов над полем P .

Выясним прежде всего, что означают обратимость и ассоциированность в кольце $P[x]$. Так как при умножении многочленов степени складываются, то произведение двух многочленов может равняться 1 только в том случае, когда оба они имеют нулевую степень, т. е. являются элементами поля P , не равными нулю. Следовательно, обратимыми в кольце $P[x]$ могут быть только ненулевые элементы поля P . Очевидно, что всякий ненулевой элемент поля P обратим в $P[x]$, поскольку он обратим в P . Таким образом, обратимые элементы кольца $P[x]$ — это ненулевые элементы поля P . В соответствии с этим ассоциированные элементы — это многочлены, получающиеся друг из друга умножением на ненулевые элементы поля P .

Отметим, что среди многочленов, ассоциированных с данным ненулевым многочленом, имеется ровно один нормированный многочлен. А именно: если $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$, где $a_0 \neq 0$, то единственным нормированным многочленом, ассоциированным с $f(x)$, будет многочлен $\frac{1}{a_0}f(x) = x^n + \frac{a_1}{a_0}x^{n-1} + \dots + \frac{a_{n-1}}{a_0}x + \frac{a_n}{a_0}$.

Важнейшими понятиями теории делимости являются понятия *идеала* и *главного идеала* (АТЧ III, § 2 гл. II). В соответствии с общим определением, главным идеалом кольца $P[x]$, порождаемым многочленом f , называется идеал

$$(f) = \{uf \mid u \in P[x]\}.$$

Идеалы (f_1) и (f_2) совпадают тогда и только тогда, когда многочлены f_1 и f_2 ассоциированы.

Как всякое евклидово кольцо, кольцо $P[x]$ является кольцом *главных идеалов*. Это означает, что любой идеал I кольца $P[x]$ является главным, т. е. совпадает с идеалом (f) , где f — некоторый многочлен, называемый *образующим многочленом идеала I* .

Рассмотрим следующий пример. Пусть p — простое число. Обозначим через I ядро гомоморфизма, который каждому многочлену из кольца $\mathbb{Z}_p[x]$ сопоставляет определяемую им функцию. Это идеал кольца $\mathbb{Z}_p[x]$; он состоит из всех многочленов, определяющих нулевую функцию, т. е. эквивалентных нулевому многочлену (см. п. 6 § 1 гл. I). Согласно малой теореме Ферма, $x^p - x \in I$, так что образующий многочлен идеала I должен быть делителем многочлена $x^p - x$. С другой стороны, из теоремы 5 § 1 гл. I вытекает, что идеал I не содержит ненулевых многочленов степени, меньшей, чем p . Следовательно,

$$I = (x^p - x).$$

Два многочлена $f, g \in \mathbb{Z}_p[x]$ эквивалентны тогда и только тогда, когда $f - g \in I$, т. е. когда $f - g$ делится на $x^p - x$. В частности, каждый многочлен f эквивалентен остатку от его деления на $x^p - x$. Этот остаток и есть многочлен f_0 , способ построения которого был указан в п. 4 § 1 гл. I.

Пусть теперь $f_1, f_2, \dots, f_m$ — многочлены из кольца $P[x]$. Всевозможные «линейные комбинации»

$$u_1 f_1 + u_2 f_2 + \dots + u_m f_m \quad (u_1, u_2, \dots, u_m \in P[x]) \quad (1)$$

образуют идеал в кольце $P[x]$: сумма двух выражений вида (1) и произведение выражения вида (1) на любой многочлен также могут быть представлены в виде (1). Обозначим этот идеал через I и рассмотрим его образующий многочлен d . Многочлен d обладает следующими свойствами:

(Д1) d является делителем каждого из многочленов $f_1, f_2, \dots, f_m$, т. е. их общим делителем;

(Д2) d делится на всякий общий делитель многочленов $f_1, f_2, \dots, f_m$.

Свойство (Д1) следует из того, что многочлены $f_1, f_2, \dots, f_m$ принадлежат идеалу $I = (d)$, а свойство (Д2) — из возможности представления многочлена d в виде (1).

Любой многочлен d , обладающий свойствами (Д1) и (Д2), называется *наибольшим общим делителем* многочленов $f_1, f_2, \dots, f_m$.

Предыдущее рассуждение показывает, что наибольший общий делитель всегда существует (что совершенно не ясно из его определения). Можно показать, кроме того, что наибольший общий делитель единственен с точностью до ассоциированности. В самом деле, пусть d' и d'' — два наибольших общих делителя мно-

членов $f_1, f_2, \dots, f_m$. Из свойства (Д2) следует, что d' делится на d'' и точно так же d'' делится на d' , а это и означает, что d' и d'' ассоциированы.

Как мы видели выше, существует такой наибольший общий делитель многочленов $f_1, f_2, \dots, f_m$, который представляется в виде (1). Поскольку всякие два наибольших общих делителя ассоциированы, то и любой наибольший общий делитель d многочленов $f_1, f_2, \dots, f_m$ представляется в виде (1), т. е. принадлежит идеалу I . Отсюда следует, что и любой многочлен, который делится на d , тоже принадлежит идеалу I .

Итак, доказана следующая теорема:

Т е о р е м а 2. *Для любых многочленов $f_1, f_2, \dots, f_m \in P[x]$ существует наибольший общий делитель d . Он определен однозначно с точностью до ассоциированности. Любой многочлен h , делящийся на d (в частности, сам многочлен d), может быть представлен в виде*

$$h = u_1 f_1 + u_2 f_2 + \dots + u_m f_m, \quad (2)$$

где $u_1, u_2, \dots, u_m \in P[x]$.

Представление какого-либо многочлена h в виде (2) будем называть его *линейным выражением* через $f_1, f_2, \dots, f_m$.

За исключением тривиального случая $f_1 = f_2 = \dots = f_m = 0$, когда $d = 0$, среди наибольших общих делителей многочленов $f_1, f_2, \dots, f_m$ имеется ровно один нормированный многочлен. Его мы будем обозначать $(f_1, f_2, \dots, f_m)$. (Иногда используется обозначение НОД $\{f_1, f_2, \dots, f_m\}$.)

Многочлены $f_1, f_2, \dots, f_m$ называются *взаимно простыми* (в совокупности), если

$$(f_1, f_2, \dots, f_m) = 1,$$

т. е. если у них нет общих делителей, кроме элементов поля P .

Т е о р е м а 3. *Многочлены $f_1, f_2, \dots, f_m \in P[x]$ взаимно просты тогда и только тогда, когда существуют такие многочлены $u_1, u_2, \dots, u_m \in P[x]$, что*

$$u_1 f_1 + u_2 f_2 + \dots + u_m f_m = 1. \quad (3)$$

Д о к а з а т е л ь с т в о. Если $(f_1, f_2, \dots, f_m) = 1$, то существование многочленов $u_1, u_2, \dots, u_m$, удовлетворяющих условию (3), вытекает из последнего утверждения теоремы 2. Обратно, если выполнено условие (3), то всякий общий делитель многочленов $f_1, f_2, \dots, f_m$, будучи делителем левой части равенства (3), является делителем единицы, т. е. элементом поля P . Теорема доказана.

Из теоремы 2 следует, что если многочлены $f_1, f_2, \dots, f_m$ взаимно просты, то любой многочлен может быть представлен в виде (2) (поскольку любой многочлен делится на единицу).

В заключение отметим, что наибольший общий делитель многочленов $f_1, f_2, \dots, f_m$, за исключением случая, когда они все равны нулю, может быть определен как их общий делитель *н а и б о л ь*

шей степени. В самом деле, пусть $\tilde{d}$ — общий делитель наибольшей степени многочленов $f_1, f_2, \dots, f_m$. Их наибольший общий делитель должен делиться на $\tilde{d}$, но, так как $\text{ст. } d \leq \text{ст. } \tilde{d}$, многочлены d и $\tilde{d}$ ассоциированы и, значит, d является наибольшим общим делителем многочленов $f_1, f_2, \dots, f_m$.

3. Вычисление наибольшего общего делителя. Наибольший общий делитель двух многочленов $f, g \in P[x]$ может быть найден при помощи алгоритма Евклида, рассмотренного ранее для кольца целых чисел (АТЧ III, § 2 гл. I).

Алгоритм Евклида состоит в следующем. Сначала делят с остатком многочлен f на многочлен g , затем многочлен g — на остаток от первого деления, затем остаток от первого деления — на остаток от второго деления и т. д. до тех пор, пока не получится нулевой остаток. Это дает следующую цепочку равенств:

$$\begin{aligned} f &= q_1 g + r_1, \\ g &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\dots \dots \dots \\ r_{k-2} &= q_k r_{k-1} + r_k, \\ r_{k-1} &= q_{k+1} r_k, \end{aligned} \tag{4}$$

причем $\text{ст. } g > \text{ст. } r_1 > \text{ст. } r_2 > \dots > \text{ст. } r_k$. Последний ненулевой остаток (т. е. r_k) и есть наибольший общий делитель многочленов f и g . Это доказывается точно так же, как и для целых чисел.

На практике, если степени данных многочленов различны, удобнее в качестве f взять многочлен большей степени.

Пример 2. В кольце $R[x]$ найдем наибольший общий делитель многочленов

$$\begin{aligned} f &= x^4 + 3x^3 - x^2 - 4x - 3, \\ g &= 3x^3 + 10x^2 + 2x - 3. \end{aligned}$$

Делим f на g :

$$\begin{array}{r|l} x^4 + 3x^3 - x^2 - 4x - 3 & 3x^3 + 10x^2 + 2x - 3 \\ - x^4 + \frac{10}{3}x^3 + \frac{2}{3}x^2 - x & \frac{1}{3}x - \frac{1}{9} \\ \hline -\frac{1}{3}x^3 - \frac{5}{3}x^2 - 3x - 3 & \\ -\frac{1}{3}x^3 - \frac{10}{9}x^2 - \frac{2}{9}x + \frac{1}{3} & \\ \hline -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3} & \end{array}$$

Для удобства умножим полученный остаток на $-\frac{9}{5}$. При этом следующие остатки также умножатся на некоторые числа, отличные от нуля, что несущественно при нахождении наибольшего общего делителя. Выполним второе деление:

$$\begin{array}{r|l}
 -3x^3 + 10x^2 + 2x - 3 & x^2 + 5x + 6 \\
 \hline
 -3x^3 + 15x^2 + 18x & 3x - 5 \\
 \hline
 - & 5x^2 - 16x - 3 \\
 - & 5x^2 - 25x - 30 \\
 \hline
 & 9x + 27
 \end{array}$$

Полученный остаток разделим на 9 и выполним третье деление:

$$\begin{array}{r|l}
 -x^2 + 5x + 6 & x + 3 \\
 \hline
 -x^2 + 3x & x + 2 \\
 \hline
 & 2x + 6 \\
 - & 2x + 6 \\
 \hline
 & 0
 \end{array}$$

Поскольку остаток равен нулю, то

$$(f, g) = x + 3.$$

Алгоритм Евклида позволяет утверждать, что если f и g — многочлены с коэффициентами из поля P и L — какое-нибудь расширение поля P , то наибольший общий делитель многочленов f и g в кольце $P[x]$ равен их наибольшему общему делителю в кольце $L(x)$. В самом деле, отыскивая наибольший общий делитель с помощью алгоритма Евклида, мы в обоих случаях придем к одному и тому же результату (причем вычисления не будут выходить за пределы кольца $P[x]$).

Наибольший общий делитель нескольких многочленов $f_1, f_2, \dots, f_m$ может быть найден индуктивным способом на основании следующей формулы:

$$(f_1, f_2, \dots, f_{m-1}, f_m) = ((f_1, f_2, \dots, f_{m-1}), f_m). \quad (5)$$

Для того чтобы найти наибольший общий делитель многочленов $f_1, f_2, \dots, f_m$, следует, согласно этой формуле, найти сначала $d_2 = (f_1, f_2)$, затем $d_3 = (d_2, f_3)$ и т. д.; $d_m = (d_{m-1}, f_m)$ и будет искомым наибольшим общим делителем.

Докажем формулу (5). Согласно определению наибольшего общего делителя, делители многочлена $(f_1, f_2, \dots, f_{m-1})$ — это в точности общие делители многочленов $f_1, f_2, \dots, f_{m-1}$. Поэтому совокупность всех общих делителей многочленов $(f_1, f_2, \dots, f_{m-1})$ и f_m совпадает с совокупностью всех общих делителей многочленов $f_1, f_2, \dots, f_{m-1}$ и f_m ; отсюда и следует формула (5).

4. Вычисление коэффициентов линейного выражения наибольшего общего делителя. Согласно теореме 2, наибольший общий делитель d двух многочленов $f, g \in P[x]$, а также всякий многочлен, кратный d , может быть представлен в виде $uf + vg$, где $u, v \in P[x]$. Напомним, что такое представление мы называем линейным выражением данного многочлена через многочлены f и g .

Для нахождения линейного выражения наибольшего общего делителя d можно воспользоваться алгоритмом Евклида. В самом деле, первое из равенств (4) дает следующее линейное выражение многочлена r_1 через f и g :

$$r_1 = f - q_1 g.$$

Подставляя его во второе равенство, получаем линейное выражение многочлена r_2 :

$$r_2 = g - q_2 r_1 = -g_2 f + (1 + q_1 q_2) g.$$

Продолжая так дальше, получаем в конце концов линейное выражение наибольшего общего делителя $d = r_k$.

Пример 3. Найдем линейное выражение наибольшего общего делителя d многочленов f и g из примера 2.

Результаты делений с остатком, выполненных при решении примера 2, показывают, что

$$f = \left(\frac{1}{3}x - \frac{1}{9}\right)g - \frac{5}{9}(x^2 + 5x + 6),$$

$$g = (3x - 5)(x^2 + 5x + 6) + 9(x + 3).$$

Отсюда находим:

$$x^2 + 5x + 6 = -\frac{9}{5}f + \frac{1}{5}(3x - 1)g,$$

$$x + 3 = \frac{1}{9}g - \frac{1}{9}(3x - 5)(x^2 + 5x + 6) = \frac{1}{5}(3x - 5)f +$$

$$+ \frac{1}{9}g - \frac{1}{45}(3x - 5)(3x - 1)g = \frac{1}{5}(3x - 5)f - \frac{1}{5}(x^2 - 2x)g.$$

Таким образом,

$$u = \frac{1}{5}(3x - 5), \quad v = -\frac{1}{5}(x^2 - 2x).$$

Линейное выражение любого многочлена h , кратного d , может быть найдено, исходя из линейного выражения d . А именно: пусть $h = h_1 d$ и $d = uf + vg$. Тогда

$$h = h_1(uf + vg) = (h_1 u)f + (h_1 v)g.$$

На практике линейное выражение многочлена h удобнее искать не с помощью алгоритма Евклида, а методом неопределенных коэффициентов. Запишем искомые многочлены u и v в общем виде с неопределенными (неизвестными) коэффициентами. Приравнивая коэффициенты при одинаковых степенях x в равенстве $h = uf + vg$, получим систему уравнений для коэффициентов многочленов u и v . Легко видеть, что эти уравнения будут линейными.

Для применения этого метода необходимо заранее иметь оценки степеней многочленов u и v (иначе мы не будем знать, в каком общем виде их записать).

Теорема 4. Пусть многочлен h , кратный $d = (f, g)$, удовлетворяет условию

$$\text{ст. } h < \text{ст. } f + \text{ст. } g.$$

Тогда он допускает линейное выражение $h = uf + vg$, в котором

$$\text{ст. } u < \text{ст. } g, \quad \text{ст. } v < \text{ст. } f.$$

Доказательство. Пусть $h = u_0f + v_0g$ — какое-то линейное выражение многочлена h . Разделим u_0 с остатком на g :

$$u_0 = qg + u, \text{ ст. } u < \text{ст. } g.$$

Выражение $u_0f + v_0g$ может быть преобразовано следующим образом:

$$u_0f + v_0g = uf + (v_0 + gf)g = uf + vg,$$

где $v = v_0 + gf$. Итак, $h = uf + vg$, причем ст. $u < \text{ст. } g$. Так как $vg = h - uf$ и ст. $h < \text{ст. } f + \text{ст. } g$, то ст. $vg < \text{ст. } f + \text{ст. } g$. Отсюда следует, что ст. $v < \text{ст. } f$, и потому многочлены u и v удовлетворяют требованиям теоремы.

Пример 4. Найдем линейное выражение многочлена $h = x - 2$ через многочлены

$$f = x^2 + 2, \quad g = x^3 + x - 1.$$

Легко проверить, что многочлены f и g взаимно просты, так что искомое линейное выражение существует, причем многочлены u и v можно искать в виде

$$u = a_0x^2 + a_1x + a_2, \quad v = b_0x + b_1.$$

Приравнивая коэффициенты при одинаковых степенях x в равенстве

$$(a_0x^2 + a_1x + a_2)(x^2 + 2) + (b_0x + b_1)(x^3 + x - 1) = x - 2,$$

получаем следующие соотношения:

$$\begin{cases} a_0 & & + b_0 & = 0, \\ & a_1 & & + b_1 & = 0, \\ 2a_0 & + a_2 & + b_0 & = 0, \\ & 2a_1 & - b_0 & + b_1 & = 1, \\ & & 2a_2 & - b_1 & = -2. \end{cases}$$

Отсюда находим: $a_0 = 1$, $a_1 = 0$, $a_2 = -1$, $b_0 = -1$, $b_1 = 0$, т. е. $u = x^2 - 1$, $v = -x$.

Иногда при составлении линейных уравнений для коэффициентов многочленов u , v удобнее не приравнивать коэффициенты при одинаковых степенях x , а придавать x различные значения.

Пример 5. Найдем многочлены u , $v \in \mathbb{R}[x]$, удовлетворяющие условию $uf + vg = 1$, где

$$f = (x + 1)(x - 3), \quad g = x(x - 1).$$

Очевидно, что многочлены f , g взаимно просты (иначе у них был бы общий линейный делитель, а значит, и общий корень). Ищем u и v в виде $u = a_0x + a_1$, $v = b_0x + b_1$. В равенстве

$$(a_0x + a_1)(x + 1)(x - 3) + (b_0x + b_1)x(x - 1) = 1$$

придаем x последовательно значения 0, 1, 3, -1. При этом получаем:

$$-3a_1 = 1 \Rightarrow a_1 = -\frac{1}{3},$$

$$-4(a_0 + a_1) = 1 \Rightarrow a_0 = \frac{1}{12},$$

$$\left. \begin{aligned} 6(3b_0 + b_1) &= 1 \\ 2(-b_0 + b_1) &= 1 \end{aligned} \right\} \Rightarrow b_0 = -\frac{1}{12}, \quad b_1 = \frac{5}{12}.$$

Таким образом,

$$u = \frac{1}{12}(x - 4), \quad v = \frac{1}{12}(-x + 5).$$

5. Наименьшее общее кратное. Наименьшим общим кратным многочленов $f_1, f_2, \dots, f_m \in P[x]$ называется многочлен h , обладающий следующими свойствами:

(К1) h делится на каждый из многочленов $f_1, f_2, \dots, f_m$, т. е. является их общим кратным;

(К2) h делит любое общее кратное многочленов $f_1, f_2, \dots, f_m$.

Совокупность всех общих кратных многочленов $f_1, f_2, \dots, f_m$ есть не что иное, как пересечение главных идеалов, порождаемых этими многочленами, т. е. идеал $(f_1) \cap (f_2) \cap \dots \cap (f_m)$. Образующий многочлен этого идеала будет наименьшим общим кратным. В самом деле, он принадлежит этому идеалу и потому является общим кратным многочленов $f_1, f_2, \dots, f_m$. С другой стороны, всякое общее кратное, будучи элементом этого идеала, делится на него. Это рассуждение доказывает существование наименьшего общего кратного. Ясно также, что наименьшее общее кратное единственно с точностью до ассоциированности. В самом деле, если h' и h'' — два наименьших общих кратных многочленов $f_1, f_2, \dots, f_m$, то из свойства (К2) следует, что h' делит h'' и точно так же h'' делит h' . Это означает, что h' и h'' ассоциированы.

За исключением тривиального случая, когда один из многочленов $f_1, f_2, \dots, f_m$ равен нулю, идеал $(f_1) \cap (f_2) \cap \dots \cap (f_m)$ не является нулевым, так как содержит, например, многочлен $f_1 f_2 \dots f_m$. Поэтому, если исключить упомянутый случай, можно утверждать, что среди наименьших общих кратных многочленов $f_1, f_2, \dots, f_m$ имеется ровно один нормированный многочлен. Будем обозначать его через $[f_1, f_2, \dots, f_m]$. (Иногда используется обозначение НОК $\{f_1, f_2, \dots, f_m\}$.)

Для двух многочленов f, g наименьшее общее кратное $[f, g]$ связано с наибольшим общим делителем (f, g) соотношением

$$f, g = cf g \quad (c \in P, c \neq 0). \quad (6)$$

Эта формула может служить для нахождения наименьшего общего кратного двух многочленов.

Для доказательства формулы (6) положим $d = (f, g)$, $h = [f, g]$, $f = f_1 d$, $g = g_1 d$ и рассмотрим многочлен

$$h' = \frac{fg}{d} = f_1 g = f g_1. \quad (7)$$

Многочлен h' является общим кратным многочленов f, g и, следовательно, делится на h . Теперь рассмотрим многочлен $d' = \frac{fg}{h}$.

$$f = \frac{h}{g} d', \quad g = \frac{h}{f} d'$$

показывают, что d' — общий делитель многочленов f, g ; следовательно, d' делит d , т. е. $d = qd'$, где q — некоторый многочлен. Отсюда получаем:

$$h' = \frac{fg}{d} = \frac{fg}{qd'} = \frac{h}{q} \Rightarrow h = qh'.$$

Стало быть, h делится на h' . Таким образом, h и h' ассоциированы, т. е. $h = ch'$, где $c \in P$, $c \neq 0$. Из (7) получаем тогда, что $hd = cfg$, что и требовалось доказать.

Из формулы (6) следует, в частности, что *наименьшее общее кратное двух взаимно простых многочленов равно их произведению*.

Пример 6. В кольце $R[x]$ найдем наименьшее общее кратное многочленов

$$f = 2x^3 + x - 3, \quad g = x^2 + x - 2.$$

Находим $d = (f, g)$ при помощи алгоритма Евклида:

$$\begin{array}{r|l} \begin{array}{r} 2x^3 + x - 3 \\ - (2x^3 + 2x^2 - 4x) \\ \hline -2x^2 + 5x - 3 \\ - (-2x^2 - 2x + 4) \\ \hline 7x - 7 \end{array} & \begin{array}{r} x^2 + x - 2 \\ 2x - 2 \\ \hline x^2 + x - 2 \\ - (x^2 + x - 2) \\ \hline 0 \end{array} \end{array}$$

Итак, $d = x - 1$ и, значит,

$$[f, g] = \frac{fg}{d} = f \frac{g}{d} = (2x^3 + x - 3)(x + 2) = 2x^4 + 4x^3 + x^2 - x - 6.$$

6. Результат. Алгоритм Евклида позволяет найти наибольший общий делитель любых двух конкретных многочленов и, в частности, выяснить, являются ли они взаимно простыми. Однако он не дает в явном виде условия, которому должны удовлетворять коэффициенты двух многочленов для того, чтобы эти многочлены были (или, наоборот, не были) взаимно просты.

Аналогичная ситуация возникает в линейной алгебре. Метод Гаусса, позволяя решать конкретные системы линейных уравнений, не дает явного условия на коэффициенты системы, при котором данная система совместна или, скажем, определена. Такие условия могут быть получены при помощи понятия определителя.

В этом пункте мы найдем соотношение между коэффициентами двух многочленов, выполнение которого необходимо и достаточно для того, чтобы многочлены не были взаимно просты. Мы придем к понятию результата, которое будет применено в § 2 гл. III к решению системы двух алгебраических уравнений с двумя неизвестными.

Пусть

$$\begin{aligned} f &= a_0 x^n + a_1 x^{n-1} + \dots + a_n, \\ g &= b_0 x^m + b_1 x^{m-1} + \dots + b_m - \end{aligned}$$

два многочлена с коэффициентами из поля P , причем $a_0 \neq 0$, $b_0 \neq 0$, так что ст. $f = n$, ст. $g = m$.

Из формулы (6) следует, что *многочлены f и g не являются взаимно простыми тогда и только тогда, когда их наименьшее общее кратное имеет степень, меньшую, чем их произведение*. Наименьшее общее кратное h многочленов f и g представляется в виде $h = fu$ и одновременно в виде $h = gv$, где u и v — некоторые многочлены. Имеем:

$$\text{ст. } h = \text{ст. } f + \text{ст. } u = \text{ст. } g + \text{ст. } v.$$

Так как ст. $fg = \text{ст. } f + \text{ст. } g$, то из условия ст. $h < \text{ст. } fg$ следует, что

$$\text{ст. } u < \text{ст. } g = m, \text{ ст. } v < \text{ст. } f = n.$$

Таким образом, *если многочлены f и g не взаимно просты, то существуют такие многочлены u и v , что*

$$fu = gv, \text{ ст. } u < m, \text{ ст. } v < n. \quad (8)$$

Обратно, если существуют многочлены u и v , удовлетворяющие условиям (8), то многочлен $fu = gv$, являющийся общим кратным многочленов f и g , имеет степень, меньшую, чем степень произведения fg . Степень n и m общего кратного в этом случае тем более меньше степени fg , и, значит, многочлены f и g не являются взаимно простыми.

Итак, вопрос о взаимной простоте многочленов f и g сводится к вопросу о существовании многочленов u и v , удовлетворяющих условиям (8). Выясним, когда такие многочлены существуют. Запишем их в общем виде:

$$\begin{aligned} u &= u_1 x^{m-1} + u_2 x^{m-2} + \dots + u_m, \\ v &= v_1 x^{n-1} + v_2 x^{n-2} + \dots + v_n. \end{aligned}$$

Предположим для определенности, что $m \leq n$. Каждое из произведений fu , gv представляет собой многочлен степени не выше $n + m - 1$. Коэффициенты многочлена fu , записанные в столбец, имеют вид

$$\begin{array}{ccccccc} a_0 u_1, & & & & & & \\ a_1 u_1 + a_0 u_2, & & & & & & \\ \dots & & & & & & \\ a_{m-1} u_1 + a_{m-2} u_2 + \dots + a_1 u_{m-1} + a_0 u_m, & & & & & & \\ a_m u_1 + a_{m-1} u_2 + \dots + a_2 u_{m-1} + a_1 u_m, & & & & & & \\ \dots & & & & & & \\ a_n u_1 + a_{n-1} u_2 + \dots + a_{n-m+2} u_{m-1} + a_{n-m+1} u_m, & & & & & & \\ a_n u_2 + \dots + a_{n-m+3} u_{m-1} + a_{n-m+2} u_m, & & & & & & \\ \dots & & & & & & \\ & & & & a_n u_{m-1} + a_{n-1} u_m, & & \\ & & & & a_n u_m. & & \end{array}$$

Коэффициенты многочлена g_v имеют вид

$$\begin{array}{l} b_0 v_1, \\ b_1 v_1 + b_0 v_2, \\ \quad \ddots \\ b_m v_1 + b_{m-1} v_2 + \dots + b_0 v_{m+1}, \\ \quad \quad b_m v_2 + \dots \quad \quad \quad + b_0 v_{m+2}, \\ \quad \quad \quad \ddots \\ \quad \quad \quad b_m v_{n-m} + \dots + b_0 v_n, \\ \quad \quad \quad \quad \ddots \\ \quad \quad \quad \quad \quad b_m v_{n-1} + b_{m+1} v_n, \\ \quad \quad \quad \quad \quad \quad b_m v_n. \end{array}$$

Приравнявая коэффициенты многочленов f_u и g_v при одинаковых степенях x , получаем систему однородных линейных уравнений относительно неизвестных $u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n$. Число уравнений этой системы равно $n + m$, т. е. числу неизвестных. Если перенести все члены с $v_1, v_2, \dots, v_n$ в левую часть, то получится следующая матрица коэффициентов при неизвестных*:

$$\left(\begin{array}{ccccccc} a_0 & \dots & & & & & -b_0 \\ a_1 a_0 & & & & & & -b_1 \quad -b_0 \\ \cdot & \cdot & & & & & \\ \cdot & \cdot & & & & & \\ a_{m-1} a_{m-2} \dots a_0 & & & -b_{m-1} & -b_{m-2} \dots & & -b_0 \\ a_m & a_{m-1} \dots a_1 & & -b_m & -b_{m-1} \dots & & -b_1 -b_0 \\ a_{m+1} & a_m \dots a_2 & & & -b_m \dots & & -b_2 -b_1 -b_0 \\ & \cdot & \cdot & \cdot & \cdot & & \\ a_n & a_{n-1} \dots a_{n-m+1} & & & & -b_m & \dots & -b_0 \\ & a_n \dots a_{n-m+2} & & & & & -b_m & \dots & -b_1 \\ & & a_n a_{n-1} & & & & & & -b_m & -b_{m-1} \\ & & & a_n & & & & & & -b_m \end{array} \right)$$

Рассматриваемая система линейных уравнений имеет ненулевое решение тогда и только тогда, когда определитель этой матрицы равен нулю. При его вычислении можно для удобства умножить на -1 последние n столбцов и транспонировать матрицу. Полученный определитель

$$R(f, g) = \left[\begin{array}{c} a_0 a_1 \dots a_n \\ a_0 a_1 \dots a_n \\ \vdots \\ a_0 a_1 \dots a_n \\ b_0 b_1 \dots b_m \\ b_0 b_1 \dots b_m \\ \vdots \\ b_0 b_1 \dots b_m \end{array} \right] \left\{ \begin{array}{l} m \text{ строк} \\ n \text{ строк} \end{array} \right. \quad (9)$$

называется *результантом* многочленов f и g .

Итак, доказано следующее утверждение.

* Мы приводим запись матрицы в случае, когда $n > m$.

Теорема 5. Многочлены $f, g \in P[x]$ не являются взаимно простыми тогда и только тогда, когда их результат $R(f, g)$, определяемый формулой (9), равен нулю.

Пример 7. Вычислим результат многочленов

$$f = 2x^4 - 5x^2 - x - 1, \quad g = x^3 - 3x^2 + 1$$

(с действительными коэффициентами) и выясним, являются ли они взаимно простыми.

Искомый результат имеет вид

$$R(f, g) = \begin{vmatrix} 2 & 0 & 5 & -1 & -1 & 0 & 0 \\ 0 & 2 & 0 & 5 & -1 & -1 & 0 \\ 0 & 0 & 2 & 0 & 5 & -1 & -1 \\ 1 & -3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -3 & 0 & 1 \end{vmatrix}$$

Вычисляя этот определитель, находим, что $R(f, g) = 543 \neq 0$; следовательно, многочлены f и g взаимно просты.

З а м е ч а н и е. Если не предполагать, что коэффициенты a_0, b_0 отличны от нуля, то обращение в нуль определителя (9) остается не обязательным условием того, чтобы многочлены f и g не были взаимно просты. В самом деле, если f и g не взаимно просты, то существуют такие ненулевые многочлены u и v , что

$$fu = gv, \quad \text{ст. } u < \text{ст. } g, \quad \text{ст. } v < \text{ст. } f.$$

Поскольку мы не предполагаем, что $a_0 \neq 0$ и $b_0 \neq 0$, нельзя утверждать, что $\text{ст. } f = n$ и $\text{ст. } g = m$, но, во всяком случае,

$$\text{ст. } f \leq n, \quad \text{ст. } g \leq m.$$

Поэтому многочлены u и v тем более удовлетворяют условиям (8), а из существования таких многочленов так же, как и выше, следует, что определитель (9) равен нулю.

Вопросы для самопроверки

1. Что такое евклидово кольцо?
2. Почему кольцо многочленов над любым полем является евклидовым кольцом?
3. Докажите единственность деления с остатком в кольце многочленов.
4. Опишите все идеалы кольца многочленов $P[x]$, где P — произвольное поле.
5. Какие многочлены являются ассоциированными элементами кольца $P[x]$?
6. Пусть I — ненулевой идеал кольца $P[x]$. Докажите, что любые два ненулевые многочлена наименьшей степени в идеале I ассоциированы.

7. Что такое наибольший общий делитель многочленов $f_1, f_2, \dots, f_m \in P[x]$?
8. Докажите существование наибольшего общего делителя любых многочленов $f_1, f_2, \dots, f_m \in P[x]$.
9. Докажите, что наибольший общий делитель единствен с точностью до ассоциированности.
10. Докажите, что если многочлен d является общим делителем многочленов $f_1, f_2, \dots, f_m$ и представляется в виде $u_1 f_1 + u_2 f_2 + \dots + u_m f_m$, где $u_1, u_2, \dots, u_m$ — какие-то многочлены, то он является наибольшим общим делителем многочленов $f_1, f_2, \dots, f_m$.
11. Докажите, что наибольший общий делитель многочленов $f_1, f_2, \dots, f_m$ является их общим делителем наибольшей степени.
12. Докажите, что всякий общий делитель наибольшей степени многочленов $f_1, f_2, \dots, f_m$ является их наибольшим общим делителем.
13. Каково необходимое и достаточное условие того, чтобы многочлен h допускал линейное выражение через данные многочлены $f_1, f_2, \dots, f_m$?
14. Что такое взаимно простые многочлены?
15. В чем состоит критерий взаимной простоты многочленов $f_1, f_2, \dots, f_m$?
16. Для чего служит алгоритм Евклида?
17. Как найти наибольший общий делитель трех многочленов?
18. Что такое наименьшее общее кратное нескольких многочленов?
19. Докажите существование наименьшего общего кратного любых многочленов.
20. Докажите единственность (с точностью до ассоциированности) наименьшего общего кратного.
21. Докажите, что наименьшее общее кратное ненулевых многочленов $f_1, f_2, \dots, f_m \in P[x]$ является их ненулевым общим кратным наименьшей степени.
22. Докажите, что всякое ненулевое общее кратное наименьшей степени ненулевых многочленов $f_1, f_2, \dots, f_m \in P[x]$ является их наименьшим общим кратным.
23. Как связаны наибольший общий делитель и наименьшее общее кратное двух многочленов?
24. Докажите формулу $[f_1, f_2, \dots, f_{m-1}, f_m] = [[f_1, f_2, \dots, f_{m-1}], f_m]$.
25. Что такое результат двух многочленов?
26. В каком случае результат двух многочленов обращается в нуль?

Упражнения

1. Выполните деление с остатком в кольце $R[x]$:

а) $2x^4 - 3x^3 + 4x^2 - 5x + 6$ на $x^2 - 3x + 1$;

б) $x^3 - 3x^2 - x - 1$ на $3x^2 - 2x + 1$.

2. Найдите наибольший общий делитель многочленов в кольце $R[x]$:

а) $x^4 + x^3 - 3x^2 - 4x - 1$ и $x^3 + x^2 - x - 1$;

б) $x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$ и $x^5 + x^2 - x + 1$.

3. Найдите наибольший общий делитель многочленов в кольце $Z_p[x]$:

а) $x^5 + x^4 - x^3 + x - 1$ и $x^3 - x^2 + x - 1$, $p = 3$;

б) $x^6 + x^4 + x + 1$ и $x^5 + x^3 + x^2 + 1$, $p = 2$.

4. С помощью алгоритма Евклида найдите линейное выражение наибольшего общего делителя двух многочленов из кольца $R[x]$:

а) $x^4 + 2x^3 - x^2 - 4x - 2$ и $x^4 + x^3 - x^2 - 2x - 2$;

б) $3x^3 - 2x^2 + x + 2$ и $x^2 - x + 1$.

5. Способом неопределенных коэффициентов найдите линейное выражение многочлена h через взаимно простые многочлены f , $g \in R[x]$.

а) $f = x^4 - 4x^3 + 1$, $g = x^3 - 3x^2 + 1$, $h = 1$;

б) $f = x^4 - 2x^3 - 4x^2 + 6x + 1$, $g = x^3 - 5x - 3$, $h = x^4$;

в) $f = x^3$, $g = (x - 1)^2$, $h = 2x - 1$;

г) $f = (x - 1)(x - 2)$, $g = x(x + 1)(x + 2)$, $h = 1$.

6. В кольце $R[x]$ найдите наименьшее общее кратное многочленов:

а) $x^5 - 2x^4 + x^3 + 7x^2 - 12x + 10$ и $3x^4 - 6x^3 + 5x^2 + 2x - 2$;

б) $x^4 - 10x^2 + 1$ и $x^4 - 4\sqrt{2}x^3 + 6x^2 + 4\sqrt{2}x + 1$.

7. Вычислите результат двух многочленов с действительными коэффициентами и выясните, являются ли они взаимно простыми:

а) $x^3 - 3x^2 + 2x + 1$ и $2x^2 - x - 1$;

б) $2x^3 - 3x^2 - x + 2$ и $x^4 - 2x^2 - 3x + 4$.

§ 2. РАЗЛОЖЕНИЕ НА НЕПРИВОДИМЫЕ МНОЖИТЕЛИ

1. **Основная теорема.** Как и во всяком кольце главных идеалов, в кольце $P[x]$ многочленов над полем P каждый необратимый элемент может быть разложен на простые множители, причем это разложение единственно с точностью до перестановки множителей и замены их ассоциированными элементами (см. АТЧ III, п. 5 § 2 гл. II).

Напомним, что ненулевой элемент области целостности называется простым, если он необратим и не может быть разложен в произведение двух необратимых элементов. Простые элементы кольца $P[x]$ по традиции называются *неприводимыми многочленами*. Поскольку необратимые элементы кольца $P[x]$, отличные от нуля, — это многочлены положительной степени, то неприводимый многочлен — это такой многочлен положительной степени, который не может быть разложен в произведение двух многочленов положительной степени. (Многочлен, который может быть разложен в произведение двух многочленов положительной степени, называется *приводимым*). Можно также сказать, что *неприводимый*

многочлен — это такой многочлен положительной степени, который не может быть разложен в произведение двух многочленов меньшей степени. В самом деле, если в разложении $f = gh$ оба множителя g, h имеют положительную степень, то каждый из них имеет степень, меньшую, чем степень f , и обратно.

Учитывая это определение и смысл понятия «ассоциированность» для многочленов, приходим к следующей теореме.

Теорема 1. *Всякий многочлен $f \in P[x]$, не являющийся элементом поля P , может быть разложен в произведение неприводимых многочленов:*

$$f = p_1 p_2 \dots p_m, \quad (1)$$

причем если $f = q_1 q_2 \dots q_l$ — другое такое разложение, то $l = m$ и при подходящей нумерации множителей имеют место равенства $q_i = c_i p_i$ ($i = 1, 2, \dots, m$), где $c_i \in P$, $c_i \neq 0$.

Например, многочлен

$$f = 3x^4 + 5x^3 + 4x^2 + x - 1$$

следующим образом разлагается на неприводимые множители в кольце $R[x]$:

$$f = (3x - 1)(x + 1)(x^2 + x + 1).$$

Равенство

$$f = (2x^2 + 2x + 2)(3x + 3)\left(\frac{1}{2}x - \frac{1}{6}\right)$$

также задает разложение многочлена f на неприводимые множители, оно получается из первого разложения путем перестановки множителей и умножения их на числа $\frac{1}{6}$, 3 и 2 соответственно.

Если вынести за скобки старшие коэффициенты всех неприводимых множителей какого-либо разложения многочлена $f \in P[x]$, то многочлен f представится в виде

$$f = ap_1 p_2 \dots p_m (a \in P, a \neq 0), \quad (2)$$

где $p_1, p_2, \dots, p_m$ — н о р м и р о в а н н ы е неприводимые многочлены. Такое представление многочлена f будем называть его *нормированным разложением на неприводимые множители*.

Очевидно, что множитель a в формуле (2) совпадает со старшим коэффициентом многочлена f и что нормированное разложение на неприводимые множители единственно с точностью до перестановки множителей.

В приведенном выше примере нормированное разложение на неприводимые множители имеет вид

$$f = 3\left(x - \frac{1}{3}\right)(x + 1)(x^2 + x + 1).$$

2. Кратность неприводимого делителя. Пусть p — какой-нибудь неприводимый делитель многочлена $f \in P[x]$. Может случиться,

что f делится не только на p , но и на p^2 или даже на более высокую степень p . Наибольшее из таких чисел k , что f делится на p^k , называется *кратностью неприводимого делителя p многочлена f* . Иными словами, кратность равна k , если f делится на p^k , но не делится на p^{k+1} . Если p — неприводимый многочлен, не являющийся делителем многочлена f , то удобно считать, что p — неприводимый делитель кратности 0.

Сравнивая определение кратности неприводимого делителя с определением кратности корня, данным в п. 2 § 2 гл. I, мы видим, что *кратность корня x_0 многочлена $f \in P[x]$ есть не что иное, как кратность неприводимого делителя $x - x_0$ этого многочлена*. (Многочлен $x - x_0$, очевидно, неприводим, так как не может быть разложен в произведение двух многочленов положительной степени.)

Т е о р е м а 2. *Кратность неприводимого делителя p многочлена f равна числу множителей, ассоциированных с p , в любом разложении многочлена f на неприводимые множители.*

В частности, неприводимый многочлен p является делителем многочлена f тогда и только тогда, когда разложение многочлена f на неприводимые множители содержит хотя бы один множитель, ассоциированный с p . Поэтому неприводимые делители многочлена f называют также его *неприводимыми множителями*.

Д о к а з а т е л ь с т в о. Предположим, что p — неприводимый делитель кратности k многочлена f . Тогда

$$f = p^k f_1, \quad (3)$$

где f_1 не делится на p . Разложим многочлен f_1 на неприводимые множители:

$$f_1 = q_1 q_2 \dots q_l.$$

В этом разложении не будет множителей, ассоциированных с p . Для многочлена f мы получим тогда разложение на неприводимые множители:

$$f = p^k q_1 q_2 \dots q_l,$$

в котором будет ровно k множителей, ассоциированных с p . В силу теоремы 2 столько же множителей, ассоциированных с p , будет в любом разложении многочлена f на неприводимые множители.

(Если ст. $f_1 = 0$, то равенство (3) уже дает разложение многочлена f на неприводимые множители и в нем имеется ровно k множителей, ассоциированных с p .)

3. Неприводимые многочлены. Неприводимые многочлены играют роль, аналогичную роли простых чисел в арифметике. Естественно поставить вопрос: какие же существуют неприводимые многочлены? Ответ на этот вопрос зависит от поля P , однако некоторые общие соображения все же можно высказать.

Прежде всего, *любой многочлен первой степени неприводим*, так как произведение двух многочленов положительной степени

всегда имеет степень ≥ 2 . Следовательно, разложение на линейные множители, рассмотренное в п. 3 § 2 гл. I, является частным случаем разложения на неприводимые множители.

По теореме Безу многочлен, имеющий корень x_0 , делится на $x - x_0$. Степень частного при этом, очевидно, будет на единицу меньше степени самого многочлена. Поэтому *всякий многочлен степени ≥ 2 , имеющий корень в поле P , приводим*. В главе IV будет доказано, что всякий многочлен положительной степени над полем C комплексных чисел имеет корень в C . Отсюда будет следовать, что в кольце $C[x]$ неприводимы только многочлены первой степени и, значит, разложение на неприводимые множители является в этом случае разложением на линейные множители.

В общем случае только часть неприводимых множителей в разложении многочлена f будет первой степени (или же таких множителей не будет вовсе). Из теоремы 2 следует, что *множитель $x - x_0$ присутствует в нормированном разложении многочлена f на неприводимые множители тогда и только тогда, когда x_0 — корень многочлена f ; при этом кратность множителя $x - x_0$ равна кратности корня x_0* . Таким образом, число множителей первой степени в разложении многочлена f на неприводимые множители равно числу его корней (с учетом кратностей).

Какие же все-таки существуют неприводимые многочлены, кроме многочленов первой степени? Для выяснения этого вопроса сопоставим прежде всего следующие два свойства многочлена $f \in P[x]$:

(I) f приводим;

(II) f имеет корень (в поле P).

Выше уже отмечалось, что из (II) следует (I). Обратное, вообще говоря, неверно. Например, многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим в кольце $R[x]$, но, очевидно, не имеет действительных корней. Однако для многочленов степеней 2 и 3 из (I) следует (II), потому что если такой многочлен f разлагается в произведение двух многочленов положительной степени, то один из них непременно должен быть первой степени и, значит, многочлен f имеет корень. Таким образом, *многочлен степени 2 или 3 неприводим тогда и только тогда, когда он не имеет корней (в поле P)*.

Например, в кольце $R[x]$ неприводим многочлен $x^2 + 1$ и вообще всякий многочлен второй степени, не имеющий действительных корней. В кольце $Q[x]$ неприводим, например, многочлен $x^3 - 2$, поскольку единственный действительный корень этого многочлена иррационален.

В главе IV будет доказано, что в кольце $R[x]$ неприводимы только многочлены первой степени и многочлены второй степени, не имеющие действительных корней. Для кольца $Q[x]$ ситуация совершенно иная: в этом кольце существуют неприводимые многочлены любой степени (см. гл. V).

Если поле P конечно, то для любого n существует лишь конечное число многочленов степени не выше n с коэффициентами

из P , и поэтому неприводимые многочлены не выше любой заданной степени могут быть найдены путем перебора, аналогично тому как находятся простые числа, не превосходящие заданного числа.

Пример 1. Перечислим все неприводимые многочлены степени не выше 4 в кольце $\mathbb{Z}_2[x]$ и докажем, что в этом кольце существуют неприводимые многочлены пятой степени.

Прежде всего, неприводимы два многочлена первой степени:

$$x, x + 1.$$

Из многочленов выше первой степени нужно рассматривать только такие, которые не имеют корней в поле $\mathbb{Z}_2$. В поле $\mathbb{Z}_2$ имеется всего два элемента: 0 и 1*. Условие $f(0) \neq 0$ означает, что свободный член многочлена f отличен от нуля. Условие $f(1) \neq 0$ означает, что число отличных от нуля членов многочлена f нечетно. Для многочленов второй и третьей степени отсутствие корней, как мы знаем, обеспечивает неприводимость. Таким образом, из многочленов второй и третьей степени неприводимы следующие:

$$x^2 + x + 1, x^3 + x^2 + 1, x^3 + x + 1.$$

Многочлены более высокой степени могут уже быть приводимыми, не имея корней; однако в этом случае все их неприводимые множители выше первой степени. В частности, из многочленов четвертой степени, не имеющих корней, приводим только один многочлен, который является квадратом неприводимого многочлена второй степени. Этот многочлен

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

Оставшиеся три многочлена

$$x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1$$

неприводимы.

Из многочленов пятой степени, не имеющих корней, приводимы только два многочлена, которые разлагаются в произведение неприводимого многочлена второй степени и одного из неприводимых многочленов третьей степени. Число многочленов пятой степени, не имеющих корней, равно 8. В самом деле, коэффициент при x^5 и свободный член каждого такого многочлена равны 1; коэффициенты при x^4 , x^3 и x^2 могут быть заданы произвольно восемью различными способами, после чего коэффициент при x однозначно определяется из условия, что число всех ненулевых коэффициентов нечетно. Следовательно, число неприводимых многочленов пятой степени равно $8 - 2 = 6$.

Так же, как доказывается бесконечность множества простых чисел, может быть доказана бесконечность множества нормированных неприводимых многочленов над любым полем P . Предположим, что таких многочленов имеется конечное число, и пусть $p_1, p_2, \dots, p_n$ — все эти многочлены. Рассмотрим многочлен $f =$

* Мы опускаем черту в обозначениях элементов поля $\mathbb{Z}_2$.

$= p_1 p_2 \dots p_n + 1$. Всякий многочлен положительной степени должен делиться на какой-нибудь неприводимый многочлен, однако многочлен f не делится ни на один из многочленов $p_1, p_2, \dots, p_n$. Полученное противоречие показывает, что сделанное допущение о конечности множества неприводимых многочленов неверно. Заметим, что доказанное утверждение представляет интерес только для конечного поля P , поскольку если поле P бесконечно, то имеется бесконечно много нормированных неприводимых многочленов первой степени.

Можно показать, что точное число нормированных неприводимых многочленов степени n над конечным полем из q элементов равно

$$\frac{1}{n} \left(q^n - \sum_i \frac{n}{q^{p_i}} + \sum_{i < j} \frac{n}{q^{p_i p_j}} - \dots + (-1)^s \frac{n}{q^{p_1 p_2 \dots p_s}} \right),$$

где $p_1, p_2, \dots, p_s$ — различные простые множители числа n .

4. Отыскание наибольшего общего делителя и наименьшего общего кратного при помощи разложения на неприводимые множители. Зная разложение многочлена f на неприводимые множители, легко найти все его делители. А именно: пусть

$$f = ap_1^{k_1} p_2^{k_2} \dots p_s^{k_s} \quad (a \in P, a \neq 0) \quad (4)$$

нормированное разложение многочлена f на неприводимые множители. Тогда всякий делитель d многочлена f имеет вид

$$d = cp_1^{m_1} p_2^{m_2} \dots p_s^{m_s} \quad (0 \leq m_i \leq k_i, c \in P, c \neq 0). \quad (5)$$

В самом деле, пусть $f = f_1 d$. Разложив f_1 и d на нормированные неприводимые множители, получим разложение на нормированные неприводимые множители самого многочлена f . В силу теоремы 1, оно должно совпадать с разложением (4). Отсюда следует, что в разложение многочлена d могут входить только неприводимые многочлены $p_1, p_2, \dots, p_s$, причем кратность множителя p_i не должна быть больше k_i .

Если известны разложения многочленов f и g на неприводимые множители, то наибольший общий делитель $d = (f, g)$ может быть найден так же, как для целых чисел (АТЧ III, п. 2 § 5 гл. I), по следующему правилу: в его разложение на неприводимые множители входят те и только те неприводимые многочлены, которые участвуют в разложении f и в разложении g , причем кратность каждого такого множителя p в разложении d равна минимуму из кратностей p в разложениях f и g . Если добавить к разложениям f и g множители в нулевых степенях таким образом, чтобы формально в обоих разложениях участвовали одни и те же неприводимые многочлены, то это правило может быть представлено следующим образом. Пусть

$$f = ap_1^{k_1} p_2^{k_2} \dots p_s^{k_s}, \quad g = bp_1^{l_1} p_2^{l_2} \dots p_s^{l_s} \quad (a, b \in P, a, b \neq 0); \quad (6)$$

тогда

$$(f, g) = d = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}, \quad (7)$$

где $m_i = \min \{k_i, l_i\}$.

Для того чтобы обосновать это правило, заметим прежде всего, что многочлен d , определенный формулой (7), делит f и g . С другой стороны, из приведенного выше описания делителей многочлена f и аналогичного описания делителей многочлена g ясно, что всякий их общий делитель h содержит в своем разложении только неприводимые множители $p_1, p_2, \dots, p_s$, причем с кратностями, не превосходящими $m_1, m_2, \dots, m_s$ соответственно, и, следовательно, h делит d . Таким образом, d — действительно наибольший общий делитель многочленов f и g .

Пример 2. В кольце $R[x]$ найдем наибольший общий делитель d многочленов.

$$f = x(x+1)^3(x-1)^2(x^2+1), \quad g = (x+1)^2(x-1)^4(x-3)(x^2+1)^2.$$

Согласно сформулированному выше правилу (и учитывая, что многочлен x^2+1 неприводим в кольце $R[x]$) находим:

$$d = (x+1)^2(x-1)^2(x^2+1).$$

Вышеописанный способ нахождения наибольшего общего делителя многочленов f и g может быть применен и тогда, когда известно разложение на неприводимые множители лишь одного из них, скажем, многочлена f . В самом деле, пусть разложение многочлена f на неприводимые множители имеет вид (4). Для определения наибольшего общего делителя $d = (f, g)$ достаточно знать, с какими кратностями участвуют в разложении g известные неприводимые многочлены $p_1, p_2, \dots, p_s$, а это легко выяснить с помощью теоремы 2.

Пример 3. В кольце $Q[x]$ найдем наибольший общий делитель многочленов

$$f = (x^3-2)^2(x^2+1)(x+1)^2, \quad g = x^9-3x^3-2.$$

Многочлен f задан своим разложением на неприводимые множители. Испытывая их поочередно, убеждаемся, что g делится на x^3-2 — на x^3-2 , но не делится на $(x^3-2)^2$, не делится на x^2+1 и делится на $(x+1)^2$. Следовательно,

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

Заметим, что в предыдущем примере наибольший общий делитель не изменится, если мы будем рассматривать f и g как элементы кольца $R[x]$ или $C[x]$ (см. п. 7 § 1).

Аналогично можно найти наименьшее общее кратное двух многочленов. Если многочлены f и g заданы формулами (6), то

$$[f, g] = p_1^{M_1} p_2^{M_2} \dots p_s^{M_s},$$

где $M_i = \max \{k_i, l_i\}$.

Следует, однако, иметь в виду, что, в отличие от целых чисел, найти разложение многочлена на неприводимые множители, как правило, гораздо труднее, чем найти наибольший общий делитель двух многочленов при помощи алгоритма Евклида. Поэтому разо-

бранный в этом пункте способ нахождения наибольшего общего делителя и наименьшего общего кратного двух многочленов имеет ограниченное применение.

5. Производная многочлена. В курсе математического анализа доказывается, что производная многочлена есть снова многочлен, причем если

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad (8)$$

то

$$f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}. \quad (9)$$

В применении к многочленам с коэффициентами из произвольного поля P определение производной, даваемое в математическом анализе, теряет смысл, так как оно опирается на понятие предела. Остается другой, формальный путь: принять формулу (9) за о п р е д е л е н и е производной, подобно тому как в п. 2 § 1 мы приняли формулы (4), (6) и (7) за определение суммы и произведения многочленов.

Итак, для многочлена $f(x) \in P[x]$, задаваемого формулой (8), мы определяем его *производную* $f'(x)$ по формуле (9). Коэффициент ka_k при x^{k-1} в этой формуле следует понимать как

$$\underbrace{a_k + a_k + \dots + a_k}_{k \text{ раз}} = \underbrace{(1 + 1 + \dots + 1)}_{k \text{ раз}} a_k$$

(см. АТЧ III, п. 4 § 1 гл. II).

Если характеристика поля P равна нулю (АТЧ III, п. 6 § 1 гл. II), то

$$\underbrace{1 + 1 + \dots + 1}_{k \text{ раз}} \neq 0$$

для любого $k > 0$ и, значит, $ka_k \neq 0$ при $a_k \neq 0$. В этом случае *производная многочлена степени $n \geq 1$ является многочленом степени $n - 1$.*

Напротив, если характеристика поля P положительна, степень многочлена при дифференцировании может уменьшиться больше чем на единицу. Может даже случиться, что производная многочлена положительной степени будет нулевым многочленом. Например, пусть

$$f(x) = x^6 + x^3 + \bar{1} \in \mathbb{Z}_3[x].$$

Тогда

$$f'(x) = (\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1})x^5 + (\bar{1} + \bar{1} + \bar{1})x^2 = 0.$$

Докажем некоторые свойства дифференцирования многочленов.

1°. *Множитель c , принадлежащий кольцу K , можно вынести за знак дифференцирования.*

Пусть многочлен $f(x)$ задается формулой (8). Тогда

$$(cf(x))' = ca_1 + 2ca_2x + \dots + nca_nx^{n-1} = cf'(x),$$

что и требовалось доказать.

2°. Производная суммы нескольких многочленов равна сумме их производных.

Достаточно доказать это свойство для суммы двух многочленов. Пусть

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots + b_mx^m. \end{aligned}$$

Тогда

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_p + b_p)x^p,$$

где $p = \max\{n, m\}$, и

$$\begin{aligned} (f(x) + g(x))' &= (a_1 + b_1) + 2(a_2 + b_2)x + \dots + p(a_p + b_p)x^{p-1} = \\ &= (a_1 + 2a_2x + \dots + pa_px^{p-1}) + (b_1 + 2b_2x + \dots + pb_px^{p-1}) = \\ &= f'(x) + g'(x). \end{aligned}$$

(Как обычно, считается, что $a_k = 0$ при $k > n$ и $b_k = 0$ при $k > m$.)

3°. Для производной произведения двух многочленов справедлива формула

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

Многочлен $f(x)g(x)$ равен сумме всевозможных произведений uv , где u — член многочлена $f(x)$, v — член многочлена $g(x)$. Запишем это следующим образом:

$$f(x)g(x) = \sum uv.$$

Согласно свойству 2° имеем:

$$(f(x)g(x))' = \sum (uv)'.$$

В то же время

$$f'(x)g(x) = \sum u'v \text{ и } f(x)g'(x) = \sum uv'.$$

Поэтому достаточно проверить, что $(uv)' = u'v + uv'$ для любых u, v , т. е. доказать свойство 3° для о д н о ч л е н о в. При этом свойство 1° позволяет свести проверку к случаю одночленов с коэффициентами, равными единице. В этом случае проверка проводится следующим образом:

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

Наше утверждение доказано.

Как и в математическом анализе, из свойства 3° выводится следующая формула дифференцирования произведения любого числа множителей:

$$\begin{aligned} (f_1(x)f_2(x)\dots f_n(x))' &= f_1'(x)f_2(x)\dots f_n(x) + \\ &+ f_1(x)f_2'(x)\dots f_n(x) + \dots + f_1(x)f_2(x)\dots f_n'(x). \end{aligned} \quad (10)$$

Частным случаем этой формулы является формула дифференцирования степени:

$$(f(x)^n)' = n f(x)^{n-1} f(x)'. \quad (11)$$

Таким образом, определенная нами операция дифференцирования многочленов над произвольным полем обладает некоторыми свойствами дифференцирования функций действительной переменной.

Можно определить дифференцирование многочленов аксиоматически, потребовав выполнения свойств 1^0 — 3^0 и свойства $x' = 1$. Из этих четырех свойств так же, как в курсе математического анализа, выводится формула (9).

Производная от производной многочлена $f(x)$ называется его второй производной и обозначается через $f''(x)$. Производная от второй производной называется третьей производной и т. д. Для m -й производной используется обозначение $f^{(m)}(x)$. Так как при каждом дифференцировании степень многочлена понижается, то $(n+1)$ -я производная любого многочлена степени n равна нулю.

6. Изменение кратности неприводимого делителя при дифференцировании многочлена. Введенное в предыдущем пункте понятие производной многочлена над произвольным полем может быть применено к исследованию кратности неприводимых делителей.

Во всех оставшихся пунктах этого параграфа мы будем предполагать, что P — поле нулевой характеристики. При этом предположении справедливо следующее утверждение:

Теорема 3. Если p — неприводимый делитель кратности $k \geq 1$ многочлена $f \in P[x]$, то p является неприводимым делителем кратности $k-1$ производной f' многочлена f . (В частности, если $k=1$, то f' не делится на p .)

Доказательство. Многочлен f может быть представлен в виде $f = p^k h$, где h не делится на p . Дифференцируя это равенство, получаем:

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

Докажем, что многочлен, стоящий в скобках, не делится на p . Так как второе слагаемое делится на p , то достаточно доказать, что $kp'h$ не делится на p .

Поскольку характеристика поля P равна нулю, p' — ненулевой многочлен, степень которого (на единицу) меньше степени p . Следовательно, p' не делится на p . Так как p — неприводимый многочлен и h тоже не делится на p , то и произведение $p'h$ не делится на p . Многочлен $kp'h$ равен произведению многочлена $p'h$ на ненулевой элемент $\underbrace{1 + 1 + \dots + 1}_{k \text{ раз}}$ поля P и, значит, также

не делится на p .

Таким образом, f' делится на p^{k-1} , но не делится на p^k . Это и означает, что p является неприводимым делителем кратности $k-1$ многочлена f' . Теорема доказана.

Неприводимый делитель p многочлена f называется *кратным*, если его кратность больше единицы.

С л е д с т в и е 1. *Многочлен $f \in P[x]$ не имеет кратных неприводимых делителей тогда и только тогда, когда он взаимно прост со своей производной.*

Д о к а з а т е л ь с т в о. Если многочлен f имеет кратный неприводимый делитель p , то из предыдущей теоремы следует, что p делит f' и, стало быть, $(f, f') \neq 1$. Обратно, если $(f, f') \neq 1$, то f и f' имеют хотя бы один общий неприводимый делитель p . При этом p должен быть *к р а т н ы м* делителем многочлена f , так как иначе, согласно той же теореме, он не был бы делителем производной.

Следствие 1 позволяет сделать вывод, что *многочлен $f \in P[x]$, не имеющий кратных неприводимых делителей, сохраняет это свойство при любом расширении поля P* (хотя сами неприводимые делители, вообще говоря, будут другими). В самом деле, наибольший общий делитель не меняется при расширении поля (см. п. 3 § 1), так что если $(f, f') = 1$ в кольце $P[x]$, то это же остается верным и в кольце $L[x]$, где L — любое расширение поля P .

Применяя теорему 3 к неприводимому делителю вида $x - x_0$, получаем такое следствие:

С л е д с т в и е 2. *Если x_0 — корень кратности $k \geq 1$ многочлена $f \in P[x]$, то x_0 будет корнем кратности $k - 1$ производной f' этого многочлена.*

В частности, x_0 — *к р а т н ы й* корень (т. е. $k > 1$) тогда и только тогда, когда $f'(x_0) = 0$.

Например, число 2 является корнем многочлена

$$f(x) = x^3 - 2x^2 - 4x + 8 \in \mathbf{R}[x].$$

Имеем:

$$f'(x) = 3x^2 - 4x - 4,$$

откуда $f'(2) = 0$. Это означает, что число 2 является кратным корнем многочлена $f(x)$.

7. Выделение кратных неприводимых множителей. Пусть разложение многочлена $f \in P[x]$ на неприводимые множители имеет вид

$$f = ap_1^{k_1} p_2^{k_2} \dots p_s^{k_s} \quad (a \in P, a \neq 0), \quad (12)$$

где $p_1, p_2, \dots, p_s$ — *н е а с с о ц и и р о в а н н ы е* неприводимые многочлены, причем числа $k_1, k_2, \dots, k_s$ отличны от нуля. По теореме 2, многочлены $p_1, p_2, \dots, p_s$ являются неприводимыми делителями многочлена f кратностей $k_1, k_2, \dots, k_s$ соответственно. Теорема 3 позволяет утверждать, что $p_1, p_2, \dots, p_s$ — неприводимые делители производной f' многочлена f кратностей $k_1 - 1, k_2 - 1, \dots, k_s - 1$ соответственно. (Если $k_i = 1$ для какого-то i , то p_i — неприводимый делитель производной f' кратности 0, т. е. p_i вообще не является делителем f' .) Отсюда следует, что наибольший общий делитель многочленов f и f' имеет вид

$$(f, f') = bp_1^{k_1-1} p_2^{k_2-1} \dots p_s^{k_s-1} \quad (b \in P, b \neq 0). \quad (13)$$

Например, если $f = ap_1p_2^3p_3p_4^2$, то

$$(f, f') = bp_2^2p_4.$$

Таким образом, неприводимые множители многочлена (f, f') — это в точности кратные неприводимые множители многочлена f . Существенно то, что многочлен (f, f') может быть найден без разложения f на неприводимые множители, а именно при помощи алгоритма Евклида. Для определения всех кратных неприводимых множителей многочлена f достаточно разложить на неприводимые множители многочлен (f, f') , степень которого меньше степени f .

Процедура отыскания наибольшего общего делителя многочленов f и f' называется *выделением кратных неприводимых множителей многочлена f* .

Из формул (12) и (13) следует, что многочлен

$$\tilde{f} = \frac{f}{(f, f')} \quad (14)$$

имеет следующее разложение на неприводимые множители:

$$\tilde{f} = cp_1p_2 \dots p_s \quad (c \in P, c \neq 0). \quad (15)$$

Иными словами, $\tilde{f}$ имеет те же неприводимые множители, что и f , но все однократные. Нахождение многочлена $\tilde{f}$ называется *освобождением многочлена f от кратных неприводимых множителей*.

Пример 4. Выделим кратные неприводимые множители многочлена

$$f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1 \in R[x].$$

Дифференцируя f и вынося $2x$ за скобки, получаем:

$$f' = 2xg,$$

где $g = 4x^6 - 3x^4 - 5x^3 + 3x + 1$.

Так как f не делится на x , то $(f, f') = (f, g)$. С помощью алгоритма Евклида находим, что $(f, g) = x^4 - x^3 - x + 1$. Таким образом,

$$(f, f') = x^4 - x^3 - x + 1 = (x^3 - 1)(x - 1) = (x^2 + x + 1)(x - 1)^2.$$

Отсюда следует, что кратными неприводимыми множителями многочлена f являются $x^2 + x + 1$ (кратности 2) и $x - 1$ (кратности 3). Разделив f на $(x^2 + x + 1)^2(x - 1)^3$, можно получить полное разложение f на неприводимые множители:

$$f = (x^2 + x + 1)^3(x - 1)^3(x + 1).$$

Так как корни многочлена соответствуют его неприводимым множителям первой степени, то корни многочлена (f, f') — это в точности кратные корни многочлена f . Поэтому выделение кратных неприводимых множителей является в то же время *выделением кратных корней*.

Пример 5. Найдем кратные корни многочлена

$$f = x^4 + 8x^3 - x^2 - 68x - 84.$$

Имеем:

$$\begin{aligned} f' &= 2(2x^3 + 12x^2 - x - 34), \\ (f, f') &= x + 2. \end{aligned}$$

Многочлен $x + 2$ имеет корень $x_0 = -2$. Это и есть кратный корень многочлена f (кратности 2). (Остальные корни можно найти, разделив f на $(x + 2)^2$.)

Если производную f' многочлена f удастся разложить на неприводимые множители (например, если удастся найти ее корни), то наибольший общий делитель f и f' может быть найден способом, описанным в п. 4.

Пример 6. Выясним, при каких a многочлен

$$f = x^3 + x^2 - 8x + a \in \mathbf{R}[x]$$

имеет кратный корень.

Имеем: $f' = 3x^2 + 2x - 8$;

корни f' суть $x_1 = -2$, $x_2 = \frac{4}{3}$. Подставляя эти значения в f ,

находим, что $f(x_1) = 0$ при $a = -12$, а $f(x_2) = 0$ при $a = \frac{176}{27}$.

Это и будут искомые значения a . (При $a = -12$ многочлен f имеет двукратный корень -2 ; при $a = \frac{176}{27}$ — двукратный корень $\frac{4}{3}$.)

8. Дискриминант. Будем по-прежнему предполагать, что характеристика поля равна нулю. В тех случаях, когда достаточно бывает выяснить только сам факт наличия или отсутствия у многочлена кратных неприводимых множителей, можно воспользоваться результатом (см. п. 6 § 1). В самом деле, многочлен f имеет кратные неприводимые множители тогда и только тогда, когда f и f' не взаимно просты, необходимым и достаточным условием чего, в свою очередь, является условие $R(f, f') = 0$. Элемент поля P , определяемый равенством

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f'), \quad (16)$$

называется *дискриминантом* многочлена f . Из наших рассуждений следует такое утверждение:

Теорема 4. *Многочлен $f \in P[x]$ имеет кратный неприводимый множитель тогда и только тогда, когда его дискриминант равен нулю.*

Вычислим в общем виде дискриминанты многочленов второй и третьей степени.

Для многочлена второй степени

$$\bar{f} = a_0 x^2 + a_1 x + a_2$$

дискриминант имеет вид

$$D(\bar{f}) = -a_0^{-1} \begin{vmatrix} a_0 & a_1 & a_2 \\ 2a_0 & a_1 & 0 \\ 0 & 2a_0 & a_1 \end{vmatrix} = -4a_0 a_2 + a_1^2. \quad (17)$$

Это выражение совпадает с тем, что в школьной алгебре называют дискриминантом квадратного трехчлена.

Для многочлена третьей степени

$$f = a_0x^3 + a_1x^2 + a_2x + a_3$$

дискриминант имеет вид

$$D(f) = -a_0^{-1} \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ 3a_0 & 2a_1 & a_2 & 0 & 0 \\ 0 & 3a_0 & 2a_1 & a_2 & 0 \\ 0 & 0 & 3a_0 & 2a_1 & a_2 \end{vmatrix} =$$

$$= -27a_0^2a_3^2 + 18a_0a_1a_2a_3 - 4a_1^3a_3 - 4a_0a_2^3 + a_1^2a_2^2. \quad (18)$$

Пример 7. Решим пример 6 при помощи дискриминанта.

Так как кратный неприводимый множитель многочлена третьей степени может быть только первой степени, то наличие такого множителя у данного многочлена f равносильно наличию у него кратного корня в поле P . По формуле (18) находим дискриминант:

$$D(f) = -27a^2 - 148a + 2112.$$

Приравнявая его нулю, находим два значения a : $a_1 = -12$, $a_2 = \frac{176}{27}$.

Вопросы для самопроверки

1. Что такое неприводимый многочлен?
2. Что такое нормированное разложение многочлена на неприводимые множители?
3. Что такое кратность неприводимого делителя многочлена?
4. Как определить кратность данного неприводимого делителя многочлена f , зная разложение многочлена f на неприводимые множители?
5. Докажите, что многочлен третьей степени, не имеющий корня в данном поле, неприводим.
6. Приведите пример приводимого многочлена четвертой степени в кольце $\mathbf{R}[x]$, не имеющего действительных корней.
7. Какова в общем случае связь между разложением на неприводимые множители и корнями многочлена?
8. Как найти все делители многочлена, если известно его разложение на неприводимые множители? Дайте строгое обоснование этого способа.
9. Как найти наибольший общий делитель нескольких многочленов, если известно разложение каждого из них на неприводимые множители?
10. Как найти наибольший общий делитель двух многочленов, если известно разложение одного из них на неприводимые множители?

11. Как определяется производная многочлена?
12. Докажите формулу дифференцирования произведения двух многочленов.
13. Докажите, что при дифференцировании многочлена над полем нулевой характеристики кратность каждого неприводимого делителя уменьшается на единицу. Где в этом доказательстве используется, что характеристика поля равна нулю?
14. Пусть x_0 — корень многочлена $f(x) \in P[x]$, где P — поле нулевой характеристики. Докажите, что кратность корня x_0 равна k тогда и только тогда, когда $f'(x_0) = f''(x_0) = \dots = f^{(k-1)}(x_0) = 0, f^{(k)}(x_0) \neq 0$.
15. Сформулируйте критерий того, что данный многочлен над полем нулевой характеристики не имеет кратных неприводимых множителей.
16. Что такое выделение кратных неприводимых множителей?
17. Как, не зная корней многочлена f , построить многочлен, имеющий те же корни, что и f , но все однократные?

Упражнения

1. Перечислите все нормированные неприводимые многочлены степени не выше 3 в кольце $\mathbf{Z}_3[x]$ и докажите существование неприводимых многочленов четвертой степени.
2. Сколько нормированных неприводимых многочленов третьей степени имеется в кольце $\mathbf{Z}_5[x]$?
3. В кольце $\mathbf{Q}[x]$ найдите наибольший общий делитель многочленов:
 - а) $x^3(x^3 - 2)^2(x^2 - 3)$ и $x(x^2 + 1)^2(x^3 - 2)$;
 - б) $(x^4 - 4)(x^2 - 2)$ и $(x^2 + 2)^2(x^4 + 4)$.
4. В кольце $\mathbf{C}[x]$ найдите наибольший общий делитель многочленов:
 - а) $(x - 1)^2(x - 2)^2(x + i)$ и $x^5 - 2x^3 + 2x^2 - 3x + 2$;
 - б) $x^6 - 1$ и $x^{14} - x + 1$.
5. Выделите кратные неприводимые множители многочлена:
 - а) $f = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8$;
 - б) $f = x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$.
6. Найдите кратные корни многочлена $f \in \mathbf{C}[x]$:
 - а) $f = x^5 - 10x^3 - 20x^2 - 15x - 4$;
 - б) $f = x^7 - 3x^6 + 5x^5 - 7x^4 + 7x^3 - 5x^2 + 3x - 1$.
7. Определите, при каких значениях a многочлен $f \in \mathbf{R}[x]$ имеет кратный корень:
 - а) $f = x^3 - 3x + a$;
 - б) $f = x^3 - 8x^2 + (13 - a)x - (6 + 2a)$.

§ 3. МНОГОЧЛЕНЫ НАД КОЛЬЦОМ С ОДНОЗНАЧНЫМ РАЗЛОЖЕНИЕМ НА ПРОСТЫЕ МНОЖИТЕЛИ

1. Деление с остатком многочленов над кольцом. В § 1, 2 этой главы рассматривались многочлены над полем. Полученные там результаты перестают быть справедливыми для многочленов над произвольной областью целостности. Это объясняется прежде всего тем, что в кольце многочленов над произвольной областью целостности деление с остатком не всегда выполнимо. Рассмотрим этот вопрос более подробно.

Пусть

$$\begin{aligned} f &= a_0x^n + a_1x^{n-1} + \dots + a_n, \\ g &= b_0x^m + b_1x^{m-1} + \dots + b_m \quad — \end{aligned}$$

многочлены с коэффициентами из области целостности K , причем $a_0 \neq 0$, $b_0 \neq 0$. Обозначим через P поле отношений кольца K (см. АТЧ III, п. 5 § 3 гл. II). Рассматривая f и g как элементы кольца $P[x]$, мы можем выполнить деление f на g с остатком, т. е. найти такие многочлены q , $r \in P[x]$, что $f = qg + r$ и ст. $r <$ ст. g . Известно также, что такая пара многочленов q , r единственна. Отсюда следует, что если указанное деление с остатком выполнимо в кольце $K[x]$, то его результат будет тот же, что и в кольце $P[x]$, т. е. получится то же неполное частное q и тот же остаток r (но только в этом случае $q, r \in K[x]$).

В общем случае многочлены q и r могут и не принадлежать кольцу $K[x]$: например, при $n \geq m$, для того чтобы $q, r \in K[x]$, необходимо, чтобы элемент a_0 делился на b_0 в кольце K . Однако если f делится на b_0^{n-m+1} (при $n \geq m$), то деление на b_0 , которое в процессе деления с остатком будет выполнено $n - m + 1$ раз, не выведет за пределы кольца K . (Если $n < m$, то $q = 0$, $r = f$, так что деление с остатком выполнимо в кольце $K[x]$.) В частности, деление с остатком выполнимо в кольце $K[x]$, если b_0 — обратимый элемент кольца K .

Из-за ограниченной возможности деления с остатком теория делимости в кольце многочленов над произвольной областью целостности не может быть построена так, как это было сделано в кольце многочленов над полем. Тем не менее оказывается, что если в кольце K имеет место однозначное разложение на простые множители (как, например, в кольце $\mathbb{Z}$ целых чисел), то и кольцо $K[x]$ обладает этим свойством (хотя, вообще говоря, не является кольцом главных идеалов). Доказательству этого факта и посвящен настоящий параграф.

Можно показать, что кольцо $K[x]$ является кольцом главных идеалов только в том случае, когда K — поле. В самом деле, если K — не поле, то существует необратимый элемент $a \in K$. Рассмотрим совокупность I многочленов с коэффициентами из K , свободный член которых делится на a . Легко видеть, что это идеал кольца $K[x]$. Он содержит многочлены a и x . Если бы идеал I был главным, то многочлен d , его порождающий, был бы общим делителем a и x . Всякий де-

датель многочлена a есть многочлен нулевой степени, т. е. элемент кольца K . Таким образом, d — элемент кольца K . Так как он принадлежит идеалу I , то он делится на a ; но тогда и x делится на a , что очевидно не соответствует действительности. Следовательно, идеал I не является главным.

2. Факториальные кольца. В кольце целых чисел, а также в кольце многочленов над полем и вообще в любом кольце главных идеалов имеет место однозначное разложение на простые множители. Как мы увидим ниже, существуют кольца, обладающие этим свойством, но не являющиеся кольцами главных идеалов, например кольцо многочленов с целыми коэффициентами. Ввиду этого оказывается полезным ввести общее понятие кольца с однозначным разложением на простые множители и исследовать свойства делимости в таких кольцах.

Область целостности K называется **факториальным кольцом**, если в ней всякий необратимый элемент может быть разложен на простые множители, причем это разложение единственно с точностью до перестановки множителей и замены их ассоциированными элементами.

Ряд свойств делимости, имеющих место для колец главных идеалов, остается справедливым и для произвольных факториальных колец. Рассмотрим некоторые из этих свойств.

1°. Простыми делителями необратимого элемента a являются, с точностью до ассоциированности, те и только те простые элементы, которые входят в его разложение на простые множители.

Очевидно, что простые элементы, входящие в разложение элемента a на простые множители, являются его делителями. Обратное, пусть p — простой делитель элемента a и пусть $a = pb$. Если b — обратимый элемент, то a — простой элемент, ассоциированный с p . Если b — необратимый элемент, то, разложив b на простые множители и домножив это разложение на p , получим разложение элемента a на простые множители, один из которых равен p . Ввиду единственности разложения на простые множители в кольце K элемент p или ассоциированный с ним элемент должен входить во всякое разложение a на простые множители.

2°. Если произведение $a_1 a_2 \dots a_n$ делится на простой элемент p , то хотя бы один из элементов $a_1, a_2, \dots, a_n$ делится на p .

В самом деле, разложим на простые множители каждый из элементов $a_1, a_2, \dots, a_n$ (кроме тех, которые обратимы). Произведение этих разложений даст разложение на простые множители элемента $a_1 a_2 \dots a_n$. В силу свойства 1° оно должно содержать множитель, ассоциированный с p . Этот множитель входит в разложение одного из элементов $a_1, a_2, \dots, a_n$, который, стало быть, делится на p .

Элементы $a_1, a_2, \dots, a_n$ факториального кольца называются **взаимно простыми (в совокупности)**, если они не имеют общего необратимого делителя. Так как у всякого необратимого элемента есть простой делитель, то взаимная простота элементов $a_1, a_2, \dots, a_n$ может также пониматься как отсутствие у них общего простого делителя, а в силу свойства 1° это равносильно тому, что

в разложениях этих элементов на простые множители нет общего (с точностью до ассоциированности) множителя.

3. Примитивные многочлены. Пусть K — факториальное кольцо. Многочлен $f \in K[x]$ называется *примитивным*, если его коэффициенты взаимно просты или, что то же самое, если он не делится в кольце $K[x]$ ни на какой необратимый элемент кольца K .

Например, многочлен $6x^2 + 10x - 15 \in \mathbb{Z}[x]$ примитивен, а многочлен $6x^2 + 10x + 4$ не примитивен, так как он делится на 2.

Докажем ряд лемм о примитивных многочленах.

Лемма 1 (лемма Гаусса). *Произведение примитивных многочленов кольца $K[x]$ есть примитивный многочлен.*

Доказательство. Достаточно доказать, что произведение двух примитивных многочленов $f, g \in K[x]$ есть примитивный многочлен. Предположим, что это не так. Тогда коэффициенты многочлена fg имеют общий простой делитель, скажем, p .

Пусть

$$\begin{aligned} f &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \\ g &= b_0 + b_1x + b_2x^2 + \dots + b_mx^m. \end{aligned}$$

Так как многочлен f примитивен, то не все его коэффициенты делятся на p . Пусть k — наибольшее из таких чисел, что a_k не делится на p . Это означает, что a_k не делится на p , а все коэффициенты $a_{k+1}, a_{k+2}, \dots, a_n$ делятся на p . Аналогично, пусть l — такое число, что b_l не делится на p , а $b_{l+1}, b_{l+2}, \dots, b_m$ делятся на p .

Рассмотрим коэффициент при x^{k+l} многочлена fg . Он имеет вид

$$c_{k+l} = a_kb_l + (a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \dots) + (a_{k-1}b_{l+1} + a_{k-2}b_{l+2} + \dots).$$

Первое выражение, заключенное в скобки, делится на p , так как $a_{k+1}, a_{k+2}, \dots$ делятся на p . Аналогично, второе выражение, заключенное в скобки, делится на p , так как $b_{l+1}, b_{l+2}, \dots$ делятся на p . Что касается произведения a_kb_l , то в силу свойства 2^о факториальных колец оно не делится на p . Следовательно, и c_{k+l} не делится на p , что противоречит нашему предположению. Тем самым лемма доказана.

Лемма 2. *Всякий многочлен $f \in K[x]$ может быть представлен в виде $f = a\tilde{f}$, где $a \in K$, а $\tilde{f}$ — примитивный многочлен.*

Доказательство. Разложим коэффициенты многочлена f на простые множители в кольце K и вынесем за скобки «общую часть» a этих разложений. Например, многочлен

$$f = 756x^2 - 240x + 156 = 2^2 \cdot 3^3 \cdot 7x^2 - 2^4 \cdot 3 \cdot 5x + 2^2 \cdot 3 \cdot 13$$

представим в виде

$$f = 2^2 \cdot 3 (3^2 \cdot 7x^2 - 2^2 \cdot 5x + 13) = 12 (63x^2 - 20x + 13).$$

В общем случае получим $f = a\tilde{f}$, где коэффициенты многочлена $\tilde{f}$ уже не имеют общих простых множителей и, следовательно, взаимно просты. Лемма доказана.

Введем теперь в рассмотрение поле отношений кольца K . Обозначим его через P .

Л е м м а 3. *Всякий многочлен $f \in P[x]$ может быть представлен в виде $f = c\tilde{f}$, где $c \in P$, а $\tilde{f}$ — примитивный многочлен из кольца $K[x]$.*

Д о к а з а т е л ь с т в о. Пусть

$$f = \frac{a_0}{b_0} x^n + \frac{a_1}{b_1} x^{n-1} + \dots + \frac{a_{n-1}}{b_{n-1}} x + \frac{a_n}{b_n},$$

где $a_i, b_i \in K$ ($i = 0, 1, \dots, n$). Обозначим через b какое-нибудь общее кратное элементов $b_0, b_1, \dots, b_n$ в кольце K (например, их произведение). Очевидно, что $bf \in K[x]$. По лемме 2 многочлен bf может быть представлен в виде $bf = a\tilde{f}$, где $a \in K$, а $\tilde{f}$ — примитивный многочлен из кольца $K[x]$. Имеем тогда: $f = \frac{a}{b}\tilde{f}$, что и является искомым представлением многочлена f .

Например, если K есть кольцо целых чисел и

$$f = \frac{7}{3}x^2 + \frac{14}{5}x + \frac{21}{2},$$

то представление многочлена f , о котором говорится в лемме 2, получается в результате следующих преобразований:

$$f = \frac{1}{30}(70x^2 + 84x + 315) = \frac{7}{30}(10x^2 + 12x + 45).$$

Л е м м а 4. *Если примитивные многочлены $f, g \in K[x]$ ассоциированы в кольце $P[x]$, то они ассоциированы и в кольце $K[x]$.*

Д о к а з а т е л ь с т в о. Пусть $f = \frac{a}{b}g$, где $a, b \in K$, $a \neq 0$, $b \neq 0$. Можно предположить, что a и b не имеют общих простых множителей, так как иначе дробь $\frac{a}{b}$ могла бы быть сокращена. Докажем, что при этом предположении элементы a и b должны быть обратимы в кольце K . Рассуждая от противного, допустим, например, что элемент a не обратим. Обозначим через p какой-нибудь его простой множитель. Тогда из равенства $bf = ag$ следует, что все коэффициенты многочлена bf делятся на p , но так как b не делится на p , то все коэффициенты многочлена f должны в этом случае делиться на p , а это противоречит примитивности многочлена f . Стало быть, a — обратимый элемент. Аналогично доказывается обратимость элемента b . Из обратимости a и b следует, что $\frac{a}{b}$ также обратимый элемент кольца K и, значит, многочлены f и g ассоциированы в кольце $K[x]$.

4. Разложение на простые множители. Обратимся к вопросу о разложении на простые множители в кольце $K[x]$, где K — факториальное кольцо.

Сделаем некоторые предварительные замечания. Очевидно, что произведение двух многочленов $f, g \in K[x]$ может быть ненулевым элементом кольца K (в частности, единицей) только в том случае, когда $f, g \in K$. Отсюда следует, что обратимыми элементами в кольце $K[x]$ являются только обратимые элементы кольца K . По той же причине простые элементы кольца K являются простыми элементами и в кольце $K[x]$.

Как и в предыдущем пункте, мы будем рассматривать отношения кольца K , которое будем обозначать через P . Согласно теореме 1 § 2, кольцо $P[x]$ факториально. Мы будем использовать это обстоятельство, сравнивая разложения на множители в кольце $K[x]$ и в кольце $P[x]$.

Имеет место следующая важная теорема:

Теорема 1. Пусть $f \in K[x]$ — многочлен положительной степени. Если он не может быть разложен в произведение двух многочленов положительной степени в кольце $K[x]$, то он не допускает такого разложения и в кольце $P[x]$, т. е. является неприводимым многочленом в $P[x]$.

Доказательство. Будем рассуждать от противного. Предположим, что $f = f_1 f_2$, где f_1 и f_2 — многочлены положительной степени с коэффициентами из поля P . По лемме 3, $f_1 = c_1 \tilde{f}_1$, $f_2 = c_2 \tilde{f}_2$, где $c_1, c_2 \in P$, а $\tilde{f}_1, \tilde{f}_2$ — примитивные многочлены из кольца $K[x]$. Имеем тогда:

$$f = (c_1 c_2) \tilde{f}_1 \tilde{f}_2. \quad (1)$$

С другой стороны, многочлен f по лемме 2 может быть представлен в виде

$$f = a \tilde{f}, \quad (2)$$

где $a \in K$, а $\tilde{f}$ — примитивный многочлен. Сопоставляя равенства (1) и (2), мы видим, что примитивный многочлен $\tilde{f}$ ассоциирован в кольце $P[x]$ с произведением $\tilde{f}_1 \tilde{f}_2$, которое по лемме 1 также является примитивным многочленом. Согласно лемме 3, многочлены $\tilde{f}$ и $\tilde{f}_1 \tilde{f}_2$ ассоциированы и в кольце $K[x]$, т. е. $\tilde{f} = b \tilde{f}_1 \tilde{f}_2$, где b — обратимый элемент кольца K . Подставляя это выражение в равенство (2), находим, что

$$f = a b \tilde{f}_1 \tilde{f}_2 = (a b \tilde{f}_1) \tilde{f}_2.$$

Это равенство противоречит предположению о том, что многочлен f не может быть разложен в произведение двух многочленов положительной степени в кольце $K[x]$. Тем самым теорема доказана.

Докажем теперь основную теорему этого параграфа.

Теорема 2. Если K — факториальное кольцо, то кольцо $K[x]$ также факториально.

Доказательство. Нужно доказать, что всякий необратимый элемент кольца $K[x]$ может быть разложен в произведение простых элементов этого кольца и что это разложение единственно с точностью до перестановки множителей и замены их ассоциированными элементами.

1°. Установим возможность разложения на простые множители любого необратимого элемента $f \in K[x]$. Если ст. $f = 0$, то f есть необратимый элемент кольца K и возможность его разложения на простые множители вытекает из факториальности кольца K . Поэтому будем считать, что ст. $f > 0$.

Предположим сначала, что f — примитивный многочлен. Рассмотрим всевозможные его разложения на множители положительной степени в кольце $K[x]$ (мы не исключаем и разложения, состоящего из одного множителя). Поскольку в любом таком разложении число множителей не превосходит степени f , то должно существовать разложение, содержащее наибольшее число множителей. Пусть оно имеет вид

$$\tilde{f} = p_1 p_2 \dots p_k. \quad (3)$$

Ни один из многочленов $p_1, p_2, \dots, p_k$ не может быть разложен в кольце $K[x]$ в произведение двух многочленов положительной степени, так как иначе многочлен $\tilde{f}$ мог бы быть разложен в произведение $k+1$ многочленов положительной степени. Кроме того, ни один из них не делится на необратимый элемент кольца K , так как в противном случае многочлен $\tilde{f}$ также делился бы на необратимый элемент кольца K , т. е. не был бы примитивен. Отсюда следует, что $p_1, p_2, \dots, p_k$ — простые элементы кольца $K[x]$ и разложение (3) является разложением многочлена $\tilde{f}$ на простые множители.

Если многочлен f не примитивен, то, по лемме 2, он представляется в виде $f = \tilde{a}\tilde{f}$, где $\tilde{a}$ — необратимый элемент кольца K , а $\tilde{f}$ — примитивный многочлен. Разложив $\tilde{a}$ и $\tilde{f}$ на простые множители, мы получим разложение на простые множители многочлена f .

2°. Докажем теперь единственность разложения на простые множители в кольце $K[x]$.

Предположим, что многочлен $f \in K[x]$ допускает два разложения на простые множители:

$$\tilde{f} = a_1 a_2 \dots a_s p_1 p_2 \dots p_k, \quad (4)$$

$$\tilde{f} = b_1 b_2 \dots b_t q_1 q_2 \dots q_l, \quad (5)$$

где $a_1, a_2, \dots, a_s, b_1, b_2, \dots, b_t$ — простые элементы нулевой степени, т. е. простые элементы кольца K , а $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ — простые элементы положительной степени.

Из теоремы 1 следует, что многочлены $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ неприводимы в кольце $P[x]$. Поэтому равенства (4) и (5) можно рассматривать как два разложения многочлена $\tilde{f}$ на неприводимые множители в кольце $P[x]$ (при этом число неприводимых множителей в первом разложении равно k , во втором — l).

Поскольку в кольце $P[x]$ разложение на неприводимые множители единственно, то $k = l$ и при подходящей нумерации многочлены q_i и p_i ($i = 1, 2, \dots, k$) ассоциированы в кольце $P[x]$.

Кроме того, многочлены $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_k$, будучи простыми элементами кольца $K[x]$, не могут делиться на необратимые элементы кольца K , т. е. являются **примитивными** многочленами. Если учесть это обстоятельство, лемма 4 позволит сделать вывод, что *многочлены p_i и q_i ($i = 1, 2, \dots, k$) ассоциированы в кольце $K[x]$* . Отсюда, в свою очередь, следует, что произведения $a_1 a_2, \dots, a_s$ и $b_1 b_2, \dots, b_t$ являются ассоциированными элементами кольца K . В силу единственности разложения на простые множители в кольце K имеем $s = t$ и при подходящей нумерации *элементы a_i и b_i ($i = 1, 2, \dots, k$) ассоциированы в кольце K и тем самым — в кольце $K[x]$* . На этом доказательство теоремы заканчивается.

Вопросы для самопроверки

1. Всегда ли выполнимо деление с остатком в кольце многочленов над областью целостности, не являющейся полем?
2. Что такое факториальное кольцо?
3. Докажите, что если произведение нескольких элементов факториального кольца делится на простой элемент p , то хотя бы один из множителей делится на p .
4. В каком случае элементы $a_1, a_2, \dots, a_k$ факториального кольца называются взаимно простыми?
5. Что такое примитивный многочлен в кольце $K[x]$, где K — факториальное кольцо?
6. В чем состоит лемма Гаусса?
7. Докажите, что если $f, g \in \mathbb{Z}[x]$, причем g — примитивный многочлен, и $h \in \mathbb{Q}[x]$ — такой многочлен, что $f = gh$, то $h \in \mathbb{Z}[x]$. Покажите на примере, что предположение о примитивности многочлена g здесь существенно.
8. Докажите, что множество простых элементов кольца $\mathbb{Z}[x]$ есть объединение множества простых чисел и множества примитивных многочленов, неприводимых в кольце $\mathbb{Q}[x]$.
9. Докажите, что кольцо $\mathbb{Z}[x]$ факториально.
10. Докажите, что элементы 2 и x кольца $\mathbb{Z}[x]$ взаимно просты.
11. Докажите, что многочлены с четным свободным членом образуют идеал в кольце $\mathbb{Z}[x]$. Является ли этот идеал главным?

§ 4. ПОЛЕ РАЦИОНАЛЬНЫХ ДРОБЕЙ

1. Определение. В § 1, 2 этой главы мы занимались изучением свойств делимости в кольце $P[x]$ многочленов над полем P . Можно поставить вопрос о таком расширении кольца $P[x]$, в котором деление выполнялось бы без ограничений (за исключением деления на нуль), т. е. о **вложении кольца $P[x]$ в поле**. Поскольку кольцо $P[x]$ является областью целостности, такое вложение возможно. А именно, кольцо $P[x]$ может быть вложено в свое **поле отношений**.

Поле отношений кольца $P[x]$ (где P — произвольное поле) называется *полем рациональных дробей* (от x) над P и обозначается $P(x)$. Согласно определению поля отношений (см. АТЧ III, п. 5 § 3 гл. II), элементы поля $P(x)$ — это классы эквивалентных «дробей» — символов вида

$$\frac{f}{g} \quad (f, g \in P[x], g \neq 0). \quad (1)$$

Дроби $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ считаются эквивалентными, если $f_1 g_2 = f_2 g_1$. Сложение и умножение дробей (1) определяется, как сложение и умножение обычных дробей, а сложение и умножение классов производится путем сложения или соответственно умножения любых их представителей. Многочлен $f \in P[x]$ отождествляется с классом дробей, эквивалентных $\frac{f}{1}$, и тем самым кольцо $P[x]$ оказывается вложенным в поле $P(x)$.

2. Несократимые рациональные дроби. Рассмотрим произвольную рациональную дробь $\frac{f}{g}$. Обозначим через d наибольший общий делитель многочленов f и g , и пусть $f = f_1 d$, $g = g_1 d$. Тогда $\frac{f}{g} \sim \frac{f_1}{g_1}$ (так как $f g_1 = f_1 g = f_1 g_1 d$). Дробь $\frac{f_1}{g_1}$ обладает тем свойством, что ее числитель и знаменатель взаимно просты. Такая рациональная дробь называется *несократимой*.

Пусть теперь $\frac{f_2}{g_2}$ — л ю б а я дробь, эквивалентная дроби $\frac{f}{g}$. Из равенства

$$f_1 g_2 = f_2 g_1 \quad (2)$$

следует, что $f_1 g_2$ делится на g_1 . Так как f_1 и g_1 взаимно просты, то g_2 делится на g_1 . Пусть $g_2 = g_1 h$. Сокращая равенство (2) на g_1 , получаем тогда, что $f_2 = f_1 h$. Таким образом, любая рациональная дробь $\frac{f_2}{g_2}$, эквивалентная дроби $\frac{f}{g}$, имеет вид $\frac{f_1 h}{g_1 h}$, где $\frac{f_1}{g_1}$ — несократимая дробь, эквивалентная $\frac{f}{g}$, а h — некоторый многочлен.

Если $\frac{f_2}{g_2}$ — также несократимая дробь, то из равенств $f_2 = f_1 h$, $g_2 = g_1 h$ следует, что $h \in P$. Таким образом, несократимая дробь, эквивалентная дроби $\frac{f}{g}$, единственна с точностью до умножения числителя и знаменателя на ненулевой элемент поля P .

3. Рациональные функции. Определим значение рациональной дроби $\frac{f}{g}$ в точке $x_0 \in P$ как $\frac{f(x_0)}{g(x_0)}$. При этом будем предполагать, что $g(x_0) \neq 0$; в противном случае будем считать, что дробь $\frac{f}{g}$ не определена в точке x_0 . Тем самым по каждой рациональной дроби определяется функция, значения которой принадлежат полю P , а область определения есть поле P , за исключением конечного числа точек (корней знаменателя).

Если $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$, то из равенства $f_1 g_2 = f_2 g_1$ следует, что

$$f_1(x_0) g_2(x_0) = f_2(x_0) g_1(x_0)$$

и при условии, что $g_1(x_0) \neq 0$ и $g_2(x_0) \neq 0$,

$$\frac{f_1(x_0)}{g_1(x_0)} = \frac{f_2(x_0)}{g_2(x_0)}.$$

Это равенство показывает, что функции, определяемые эквивалентными рациональными дробями, совпадают в их общей области определения.

Из описания всех рациональных дробей, эквивалентных данной дроби (см. п. 2), следует, что если знаменатель несократимой рациональной дроби обращается в нуль в точке x_0 , то и знаменатель любой эквивалентной ей дроби будет в этой точке обращаться в нуль. Иными словами, из всех дробей, эквивалентных данной, несократимая дробь задает функцию, имеющую наибольшую область определения. Функция, определяемая несократимой рациональной дробью, называется *рациональной функцией*.

Предоставляем читателю проверить, что сумма (соответственно произведение) рациональных дробей $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ определяет функцию, равную сумме (соответственно произведению) функций, определяемых дробями $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$, на том множестве, где обе эти функции определены.

Если поле P бесконечно, то из равенства (в общей области определения) функций, определяемых двумя рациональными дробями, следует равенство самих дробей. Доказательство этого утверждения мы также предоставляем читателю.

Глава III

МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

§ 1. КОЛЬЦО МНОГОЧЛЕНОВ ОТ n ПЕРЕМЕННЫХ

1. Построение кольца многочленов. Подобно тому как в § 1 главы I было построено кольцо многочленов от одной переменной, можно построить кольцо многочленов от любого числа переменных.

Пусть K — произвольная область целостности. Многочленом от $x_1, x_2, \dots, x_n$ с коэффициентами из K назовем формальное выражение вида

$$\sum_{(k_1, k_2, \dots, k_n)} a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad (1)$$

где $a_{k_1 k_2 \dots k_n}$ — элементы кольца K , а $(k_1, k_2, \dots, k_n)$ пробегает некоторое конечное множество наборов неотрицательных целых чисел; при этом для сокращения записи условимся не писать формальных множителей $x_i^{k_i}$ в тех случаях, когда $k_i = 0$. Так, многочленами от x_1, x_2, x_3 с коэффициентами из $\mathbb{Z}$ будут, например, выражения

$$2x_2^3 x_3 + 3 + 0x_1 x_2 x_3 + (-1)x_1^2 x_3$$

и

$$1x_1^2 + 4x_1 x_2^3.$$

Будем называть всякое формальное слагаемое $a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$, входящее в состав многочлена (1), его *членом* (в частности, $a_{0,0,\dots,0}$ назовем *свободным членом*), а элемент $a_{k_1 k_2 \dots k_n}$ кольца K — *коэффициентом при $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$* ; если член вида $a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ отсутствует, то будем считать, что коэффициент $a_{k_1 k_2 \dots k_n}$ при $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ равен нулю. Так, в первом из приведенных выше примеров $a_{0,3,1} = 2$, $a_{0,0,0} = 3$, $a_{1,1,1} = a_{1,1,0} = 0$ и т. д.; во втором примере $a_{k_1 k_2 k_3} = 0$ при $k_3 > 0$.

Для обозначения многочленов от $x_1, x_2, \dots, x_n$ будем пользоваться символами $f(x_1, x_2, \dots, x_n)$, $g(x_1, x_2, \dots, x_n)$ и т. п.

Многочлены $f_1(x_1, x_2, \dots, x_n)$ и $f_2(x_1, x_2, \dots, x_n)$ будем считать *равными*, если для любых $k_1, k_2, \dots, k_n$ коэффициент при $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ многочлена $f_1(x_1, x_2, \dots, x_n)$ равен коэффициенту при $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ многочлена $f_2(x_1, x_2, \dots, x_n)$. Равенство будет записываться обычным образом:

$$f_1(x_1, x_2, \dots, x_n) = f_2(x_1, x_2, \dots, x_n).$$

Из определения равенства многочленов следует, что порядок членов в записи многочлена несуществен и что приписывание или отбрасывание членов с нулевыми коэффициентами не меняет многочлена (имея это в виду, обычно таких членов не пишут), например:

$$2x_2^3x_3 + 3 + 0x_1x_2x_3 + (-1)x_1^2x_3 = 3 + 2x_2^3x_3 + (-1)x_1^2x_3.$$

Определим теперь сложение и умножение многочленов. Пусть даны два многочлена:

$$f(x_1, x_2, \dots, x_n) = \sum_{(k_1, k_2, \dots, k_n)} a_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}. \quad (2)$$

$$g(x_1, x_2, \dots, x_n) = \sum_{(k_1, k_2, \dots, k_n)} b_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}. \quad (3)$$

Определим сумму этих многочленов по формуле

$$\begin{aligned} & f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n) = \\ &= \sum_{(k_1, k_2, \dots, k_n)} (a_{k_1 k_2 \dots k_n} + b_{k_1 k_2 \dots k_n}) x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \end{aligned} \quad (4)$$

где суммирование в правой части распространяется на все наборы $(k_1, k_2, \dots, k_n)$, для которых $a_{k_1 k_2 \dots k_n} \neq 0$ или $b_{k_1 k_2 \dots k_n} \neq 0$.

Далее, определим произведение многочленов по формуле

$$\begin{aligned} & f(x_1, x_2, \dots, x_n) g(x_1, x_2, \dots, x_n) = \\ &= \sum_{(k_1, k_2, \dots, k_n)} c_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \end{aligned} \quad (5)$$

где

$$c_{k_1 k_2 \dots k_n} = \sum_{\substack{(l_1, l_2, \dots, l_n) \\ 0 \leq l_i \leq k_i}} a_{l_1 l_2 \dots l_n} b_{k_1 - l_1, k_2 - l_2, \dots, k_n - l_n}, \quad (6)$$

а суммирование в правой части формулы (5) распространяется на все наборы $(k_1, k_2, \dots, k_n)$, для которых $c_{k_1 k_2 \dots k_n} \neq 0$ (таких наборов имеется лишь конечное число).

Например, пусть

$$f(x_1, x_2, x_3) = 3x_2 + 1x_1x_2^2x_3^2 + (-2)x_1^2x_2^3x_3^4,$$

$$g(x_1, x_2, x_3) = 2x_1 + (-1)x_1^2x_2x_3^2 + 1x_1^3x_2^2x_3^4.$$

Тогда $f(x_1, x_2, x_3) g(x_1, x_2, x_3)$ определяется по формуле (5), где

$$c_{1,1,0} = a_{0,1,0} b_{1,0,0} = 3 \cdot 2 = 6,$$

$$c_{2,2,2} = a_{0,1,0} b_{2,1,2} + a_{1,2,2} b_{1,0,0} = 3 \cdot (-1) + 1 \cdot 2 = -1,$$

$$\begin{aligned} c_{3,3,4} &= a_{0,1,0} b_{3,2,4} + a_{1,2,2} b_{2,1,2} + a_{2,3,4} b_{1,0,0} = 3 \cdot 1 + \\ &+ 1 \cdot (-1) + (-2) \cdot 2 = -2, \end{aligned}$$

$$c_{4,4,6} = a_{1,2,2} b_{3,2,4} + a_{2,3,4} b_{2,1,2} = 1 \cdot 1 + (-2) \cdot (-1) = 3,$$

$$c_{5,5,8} = a_{2,3,4} b_{3,2,4} = (-2) \cdot 1 = -2,$$

а остальные коэффициенты произведения равны нулю, так что

$$\begin{aligned} f(x_1, x_2, x_3) g(x_1, x_2, x_3) = & 6x_1x_2 + (-1)x_1^2x_2^2x_3^2 + \\ & + (-2)x_1^3x_2^3x_3 + 3x_1^4x_2^4x_3^6 + (-2)x_1^5x_2^5x_3^8. \end{aligned}$$

З а м е ч а н и е. Роль букв $x_1, x_2, \dots, x_n$ в записи многочленов могут играть любые другие буквы. В тех случаях, когда ясно, какие буквы исполняют эту роль (и, в частности, каково число этих букв), обозначения многочленов $f(x_1, x_2, \dots, x_n), g(x_1, x_2, \dots, x_n)$ могут сокращаться до $f, g, \dots$

Отметим теперь некоторые свойства определенных выше операций над многочленами.

1⁰. Коммутативность сложения так же, как для многочленов от одной переменной, вытекает из коммутативности сложения в кольце K .

2⁰. Ассоциативность сложения следует из ассоциативности сложения в кольце K .

3⁰. Существование нуля. Роль нулевого элемента играет многочлен, все коэффициенты которого равны нулю. Этот многочлен называется *нулевым* и обозначается символом 0.

4⁰. Существование противоположного элемента. Многочленом, противоположным многочлену $f(x_1, x_2, \dots, x_n)$, будет многочлен $\bar{f}(x_1, x_2, \dots, x_n)$, коэффициенты которого противоположны соответствующим коэффициентам многочлена $f(x_1, x_2, \dots, x_n)$.

5⁰. Дистрибутивность умножения относительно сложения можно проверить так же, как для многочленов от одной переменной, пользуясь дистрибутивностью в кольце K .

Свойства 1⁰—5⁰ означают, что *многочлены от $x_1, x_2, \dots, x_n$ с коэффициентами из K образуют кольцо относительно определенных нами операций*. Это кольцо называется *кольцом многочленов от $x_1, x_2, \dots, x_n$ над K* и обозначается $K[x_1, x_2, \dots, x_n]$.

Многочлены, не содержащие $x_1, x_2, \dots, x_n$, т. е. состоящие из одного свободного члена, мы будем отождествлять с элементами кольца K , основываясь на том, что их сложение и умножение, как видно из определений, производится так же, как в кольце K . При таком соглашении кольцо K является подкольцом кольца $K[x_1, x_2, \dots, x_n]$.

Многочлен вида $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ называется *одночленом*. Из определения сложения многочленов видно, что произвольный многочлен (1) равен сумме одночленов $a_{k_1k_2\dots k_n}x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$. Это позволяет рассматривать символ «+» в записи многочлена как знак сложения.

Из определения умножения многочленов легко увидеть, что *произведение двух одночленов есть одночлен*, а именно:

$$(ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n})(bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}) = abx_1^{k_1+l_1}x_2^{k_2+l_2}\dots x_n^{k_n+l_n}. \quad (7)$$

Одночлены, отличающиеся лишь коэффициентами, называются *подобными*. Сумма подобных одночленов есть также одночлен, а именно:

$$ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n} + bx_1^{k_1} x_2^{k_2} \dots x_n^{k_n} + \dots + cx_1^{k_1} x_2^{k_2} \dots x_n^{k_n} = \\ = (a + b + \dots + c) x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}. \quad (8)$$

Будем рассматривать каждый многочлен как сумму его членов. Тогда из свойства дистрибутивности умножения многочленов относительно сложения вытекает следующее правило умножения многочленов: для вычисления произведения $f(x_1, x_2, \dots, x_n) g(x_1, x_2, \dots, x_n)$ нужно каждый член многочлена $f(x_1, x_2, \dots, x_n)$ умножить на каждый член многочлена $g(x_1, x_2, \dots, x_n)$ по формуле (7) и результаты сложить, выполнив приведение подобных членов по формуле (8). Практически многочлены перемножают именно этим способом.

Продолжим рассмотрение свойств операций над многочленами.

6°. Коммутативность умножения. Сформулированное выше правило умножения многочленов позволяет так же, как и для многочленов от одной переменной, свести доказательство коммутативности умножения к тому случаю, когда оба множителя являются одночленами. Что касается умножения одночленов, то его коммутативность видна из формулы (7), так как умножение в кольце K коммутативно.

7°. Ассоциативность умножения можно доказать аналогично, исходя из ассоциативности умножения в кольце K .

8°. Существование единицы. Роль единицы играет многочлен $1 \in K$.

Таким образом, $K[x_1, x_2, \dots, x_n]$ — коммутативное ассоциативное кольцо с единицей. В п. 3 мы покажем, что в нем нет делителей нуля, откуда будет следовать, что оно является областью целостности.

Можно заметить, что если в произвольный многочлен $f(x_1, x_2, \dots, x_n)$ подставить вместо букв $x_1, x_2, \dots, x_n$ многочлены $1x_1, 1x_2, \dots, 1x_n$ и фактически произвести все операции, формально указанные в записи многочлена $f(x_1, x_2, \dots, x_n)$, то получится тот же многочлен $f(x_1, x_2, \dots, x_n)$. Это позволяет придавать записи многочлена содержательный смысл. (Вспомним, что выше мы уже дали содержательное толкование символу «+»). Имея это в виду, мы можем при записи многочлена не писать коэффициентов, равных 1 (за исключением свободного члена), а также вместо $+(-a)x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ писать $-ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$, понимая «—» как знак вычитания.

2. Степень и лексикографическое упорядочение. Степенью (точнее, степенью по совокупности переменных) ненулевого одночлена $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ называется число $k_1 + k_2 + \dots + k_n$. Очевидно, что степень произведения двух одночленов равна сумме их степеней.

Степенью (по совокупности переменных) ненулевого многочлена называется максимальная из степеней его членов. Например, степень многочлена $x_1^2 x_2^2 x_3 + 3x_3^4 - x_1 x_2^3 + x_1^3 x_2^3$ равна 6. Степень нулевого многочлена считается равной $-\infty$.

Многочлен называется *однородным степени m* , если все его члены имеют степень m . Например, многочлен $x_1^4 - x_1 x_2^3 + 2x_2^2 x_3^2$ является однородным степени 4.

Очевидно, что:

(01) сумма двух однородных многочленов одинаковой степени есть однородный многочлен той же степени;

(02) произведение однородных многочленов степеней m_1 и m_2 есть однородный многочлен степени $m_1 + m_2$.

Если в выражении многочлена сгруппировать члены одинаковой степени, то получится представление данного многочлена в виде суммы однородных многочленов различных степеней. Легко понять, что такое представление единственно. Составляющие его однородные многочлены называются *однородными компонентами* данного многочлена.

Пр и м е р 1. Однородными компонентами многочлена

$$f(x_1, x_2, x_3) = x_1^5 x_2 - x_1 x_3^2 - x_1^2 x_2^2 + x_1 x_2 x_3 + 2x_2^4 x_3^2 + x_1^2 x_2^2 x_3^2$$

будут многочлены

$$\begin{aligned} & x_1^5 x_2 + 2x_2^4 x_3^2 + x_1^2 x_2^2 x_3^2 \quad (\text{однородная компонента степени 6}), \\ & -x_1^2 x_2^2 \quad (\text{однородная компонента степени 4}), \\ & -x_1 x_3^2 + x_1 x_2 x_3 \quad (\text{однородная компонента степени 3}). \end{aligned}$$

При $n = 1$ члены многочлена однозначно упорядочиваются по убыванию (или по возрастанию) степени. При $n > 1$ такое упорядочение, вообще говоря, не однозначно, так как могут быть члены одинаковой степени, но с различными наборами показателей.

Для однозначного упорядочения членов многочлена от любого числа переменных используется так называемое *лексикографическое упорядочение* ненулевых одночленов. Одночлен $u = ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ считается *старше* одночлена $v = bx_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$ (а одночлен v — *младше* одночлена u), если либо $k_1 > l_1$, либо $k_1 = l_1$, но $k_2 > l_2$, либо $k_1 = l_1$, $k_2 = l_2$, но $k_3 > l_3$ и т. д. В этом случае пишут: $u > v$ (или $v < u$).

Например, $-x_1 x_2^2 > 2x_1 x_2 x_3^4$. Как показывает этот пример, лексикографическое упорядочение не согласовано с упорядочением по степеням, т. е. лексикографически старший член может иметь меньшую степень.

Очевидно, что если $u > v$ и $v > w$, то $u > w$, т. е. отношение « $>$ » является отношением порядка. Название «лексикографическое упорядочение» объясняется тем, что если рассматривать наборы показателей одночленов как «слова», составленные из букв «алфавита» 0, 1, 2, ..., то расположение одночленов в порядке лек-

сикографического возрастания будет обычным алфавитным расположением, какое употребляется в словарях (лексиконах).

Пример 2. Расположив в порядке лексикографического убывания члены многочлена

$$f(x_1, x_2, x_3) = x_2^4 + x_1x_2x_3 + 3x_1x_2 - x_2x_3 + 2x_2x_3^2,$$

получим:

$$f(x_1, x_2, x_3) = x_1x_2x_3 + 3x_1x_2 + x_2^4 + 2x_2x_3^2 - x_2x_3.$$

Очевидно, что среди членов любого ненулевого многочлена $f(x_1, x_2, \dots, x_n)$ имеется член, который старше всех остальных. Он называется *старшим членом* многочлена $f(x_1, x_2, \dots, x_n)$. Так, в приведенном выше примере старшим членом является $x_1x_2x_3$.

Важнейшее свойство лексикографического упорядочения состоит в следующем:

(Л1) если $u > v$ и w — любой ненулевой одночлен, то $uw > vw$.

Для того чтобы это доказать, достаточно заметить, что при умножении на w к показателям степени переменной x_i в одночленах u и v добавляется одно и то же число (равное показателю степени x_i в одночлене w) и, следовательно, знак неравенства (или равенства) между ними сохраняется.

Из (Л1) выводится такое свойство:

(Л2) если $u > v$ и $w > t$, то $uw > vt$.

В самом деле, согласно (Л1) из $u > v$ следует, что $uw > vw$ и аналогично из $w > t$ вытекает, что $vw > vt$. Следовательно, $uw > vt$.

3. Отсутствие делителей нуля в кольце многочленов. Лексикографическое упорядочение позволяет, в частности, установить отсутствие делителей нуля в кольце многочленов от n переменных над областью целостности K . Пусть f и g — два ненулевых многочлена, u и w — их старшие члены. Произведение fg равно сумме всевозможных произведений членов многочлена f на члены многочлена g . В эту сумму будет входить и произведение uw , причем из отсутствия делителей нуля в кольце K следует, что коэффициент одночлена uw (равный произведению коэффициентов одночленов u и w) отличен от нуля. Покажем, что все другие произведения будут младше, чем uw . Если v — какой-либо член многочлена f , отличный от u , то $u > v$ и по свойству (Л1) $uw > vw$. Аналогично, если t — какой-либо член многочлена g , отличный от w , то $uw > ut$. Наконец, при тех же предположениях по свойству (Л2) имеем: $uw > vt$. Таким образом, среди произведений членов многочлена f на члены многочлена g не будет одночленов, подобных uw . Отсюда следует, что $fg \neq 0$.

Таким образом, доказана следующая теорема:

Теорема 1. *Кольцо многочленов от n переменных над областью целостности также является областью целостности.*

Одновременно установлена и такая теорема:

Теорема 2. *Старший член произведения двух ненулевых*

многочленов от n переменных равен произведению их старших членов.

Докажем еще одну теорему.

Теорема 3. *Степень произведения двух ненулевых многочленов от n переменных равна сумме их степеней.*

Доказательство. Пусть $f(x_1, x_2, \dots, x_n)$ — многочлен степени k , $g(x_1, x_2, \dots, x_n)$ — многочлен степени l . Представим каждый из этих многочленов в виде суммы однородных многочленов. Обозначим через $f_k(x_1, x_2, \dots, x_n)$ (соответственно через $g_l(x_1, x_2, \dots, x_n)$) однородную компоненту степени k (соответственно l) многочлена $f(x_1, x_2, \dots, x_n)$ (соответственно $g(x_1, x_2, \dots, x_n)$). Произведение $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ равно сумме всевозможных произведений однородных компонент многочлена $f(x_1, x_2, \dots, x_n)$ на однородные компоненты многочлена $g(x_1, x_2, \dots, x_n)$. Среди таких произведений есть произведение $f_k(x_1, x_2, \dots, x_n)g_l(x_1, x_2, \dots, x_n)$, отличное от нуля (по теореме 1) и имеющее степень $k + l$; все остальные произведения имеют меньшую степень. Следовательно, степень многочлена $f(x_1, x_2, \dots, x_n)g(x_1, x_2, \dots, x_n)$ равна $k + l$.

4. Выделение одной переменной. Если в выражении (1) многочлена $f(x_1, x_2, \dots, x_n)$ сгруппировать члены, содержащие переменную x в одинаковой степени, и в каждой такой группе членов вынести эту степень x_n за скобки, то многочлен $f(x_1, x_2, \dots, x_n)$ представится в виде

$$f(x_1, x_2, \dots, x_n) = \sum_k f_k(x_1, x_2, \dots, x_{n-1}) x_n^k. \quad (9)$$

Например,

$$2x_1^2 x_3^2 + x_1 x_2 x_3 + 3x_1^2 - x_3 + 2x_2 x_3^2 = (2x_1^2 + 2x_2) x_3^2 + (x_1 x_2 - 1) x_3 + 3x_1^2.$$

Таким образом, каждый многочлен от переменных $x_1, x_2, \dots, x_n$ с коэффициентами из кольца K можно рассматривать как многочлен от одной переменной x_n с коэффициентами из кольца $K[x_1, x_2, \dots, x_{n-1}]$. При этом сложение и умножение, производимые в кольце $K[x_1, x_2, \dots, x_n]$, приводят к тем же результатам, что и в кольце $K[x_1, x_2, \dots, x_{n-1}][x_n]$.

В самом деле, пусть

$$f(x_1, x_2, \dots, x_n) = \sum_k f_k(x_1, x_2, \dots, x_{n-1}) x_n^k,$$

$$g(x_1, x_2, \dots, x_n) = \sum_k g_k(x_1, x_2, \dots, x_{n-1}) x_n^k.$$

Из свойств операций в кольце $K[x_1, x_2, \dots, x_n]$ следует, что

$$\begin{aligned} & f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n) = \\ &= \sum_k (f_k(x_1, x_2, \dots, x_{n-1}) + g_k(x_1, x_2, \dots, x_{n-1})) x_n^k, \end{aligned}$$

$$f(x_1, x_2, \dots, x_n) g(x_1, x_2, \dots, x_n) = \sum_k h_k(x_1, x_2, \dots, x_{n-1}) x_n^k,$$

где

$$h_k(x_1, x_2, \dots, x_{n-1}) = \sum_l f_l(x_1, x_2, \dots, x_{n-1}) g_{k-l}(x_1, x_2, \dots, x_{n-1}).$$

Это согласуется с правилами сложения и умножения в кольце $K[x_1, x_2, \dots, x_{n-1}][x_n]$.

Итак, кольцо многочленов от $x_1, x_2, \dots, x_n$ с коэффициентами из кольца K можно рассматривать как кольцо многочленов от x_n с коэффициентами из кольца $K[x_1, x_2, \dots, x_{n-1}]$.

Этим можно воспользоваться, чтобы дать другое доказательство теоремы 1. А именно теорема 1 может быть доказана индукцией по n . При $n = 1$ доказываемое утверждение составляет содержание теоремы 1 § 1 гл. I. Переход от $n - 1$ к n осуществляется на основе той же теоремы. Для этого надо применить ее к кольцу многочленов от одной переменной над кольцом $K[x_1, x_2, \dots, x_{n-1}]$, которое по предположению индукции является областью целостности.

5. Многочлены как функции. Каждый многочлен от n переменных с коэффициентами из кольца K определяет функцию на $K^n = \underbrace{K \times K \times \dots \times K}_{n \text{ раз}}$ со значениями в K . А именно, значением

многочлена $f(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$, задаваемого выражением (1), в точке $(x_{01}, x_{02}, \dots, x_{0n}) \in K^n$ называется элемент кольца K , определяемый по формуле

$$f(x_{01}, x_{02}, \dots, x_{0n}) = \sum_{(k_1, k_2, \dots, k_n)} a_{k_1 k_2 \dots k_n} x_{01}^{k_1} x_{02}^{k_2} \dots x_{0n}^{k_n}. \quad (10)$$

Аналогично тому, как это было сделано для многочленов от одной переменной, можно проверить, что функция, определяемая суммой (соответственно произведением) двух многочленов, равна сумме (соответственно произведению) функций, определяемых этими многочленами.

Теорема 4. Если кольцо K бесконечно, то из равенства функций, определяемых двумя многочленами, следует равенство самих многочленов.

Доказательство проведем индукцией по числу переменных. Для многочленов от одной переменной утверждение теоремы было доказано в § 1 гл. I.

Предположим теперь, что утверждение теоремы справедливо для многочленов от $n - 1$ переменной, и докажем, что тогда оно справедливо для многочленов от n переменных. Пусть $f(x_1, x_2, \dots, x_n)$, $g(x_1, x_2, \dots, x_n)$ — многочлены от n переменных $x_1, x_2, \dots, x_n$, определяющие одинаковые функции, т. е. принимающие одинаковые значения во всех точках пространства K^n . Представим $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ как многочлены от x_n с коэффициентами из кольца $K[x_1, x_2, \dots, x_{n-1}]$:

$$f(x_1, x_2, \dots, x_n) = \sum_k f_k(x_1, x_2, \dots, x_{n-1}) x_n^k,$$

$$g(x_1, x_2, \dots, x_n) = \sum_k g_k(x_1, x_2, \dots, x_{n-1}) x_n^k.$$

Дадим переменным $x_1, x_2, \dots, x_{n-1}$ произвольные значения $x_{01}, x_{02}, \dots, x_{0,n-1}$. Пусть

$$f_k(x_{01}, x_{02}, \dots, x_{0,n-1}) = a_k,$$

$$g_k(x_{01}, x_{02}, \dots, x_{0,n-1}) = b_k.$$

Многочлены

$$F(x_n) = \sum_k a_k x_n^k, \quad G(x_n) = \sum_k b_k x_n^k,$$

как следует из нашего предположения, принимают одинаковые значения при всех значениях x_n . В самом деле, при любом $x_{0n} \in K$

$$\begin{aligned} F(x_{0n}) &= f(x_{01}, x_{02}, \dots, x_{0,n-1}, x_{0n}) = \\ &= g(x_{01}, x_{02}, \dots, x_{0,n-1}, x_{0n}) = G(x_{0n}). \end{aligned}$$

Теорема 4 § 1 гл. I позволяет заключить, что $F(x_n) = G(x_n)$, т. е.

$$f_k(x_{01}, x_{02}, \dots, x_{0,n-1}) = g_k(x_{01}, x_{02}, \dots, x_{0,n-1})$$

при любом k . Так как $x_{01}, x_{02}, \dots, x_{0,n-1}$ — произвольные элементы кольца K , то в силу предположения индукции

$$f_k(x_1, x_2, \dots, x_{n-1}) = g_k(x_1, x_2, \dots, x_{n-1})$$

при любом k ; но тогда

$$f(x_1, x_2, \dots, x_n) = g(x_1, x_2, \dots, x_n),$$

что и требовалось доказать.

Таким образом, если кольцо K бесконечно, то отображение, которое каждому многочлену из кольца $K[x_1, x_2, \dots, x_n]$ сопоставляет определяемую им функцию, является и з о м о р ф и з м о м кольца $K[x_1, x_2, \dots, x_n]$ на некоторое кольцо функций, определяемых на K^n и принимающих значения в K .

Если кольцо K конечно, утверждение теоремы 4 неверно (для $n = 1$ это отмечалось в § 1 гл. I). Однако при некоторых дополнительных предположениях оно может быть верным. Например, в случае, когда $K = \mathbb{Z}_p$ — кольцо вычетов по простому модулю p , утверждение теоремы 4 будет верно в предположении, что степени обоих многочленов по каждой из переменных не превосходят $p - 1$. При этом данное выше доказательство остается в силе, если только вместо теоремы 4 § 1 гл. I воспользоваться теоремой 5 того же параграфа.

С другой стороны, для всякого многочлена $f(x_1, x_2, \dots, x_n) \in \mathbb{Z}_p[x_1, x_2, \dots, x_n]$ легко построить многочлен $f_0(x_1, x_2, \dots, x_n)$, имеющий по каждой переменной степень не выше $p - 1$ и определяющий ту же функцию, что и $f(x_1, x_2, \dots, x_n)$. Для многочленов от одной переменной способ построения такого многочлена был указан в п. 6 § 1 гл. I. В общем случае многочлен $f_0(x_1, x_2, \dots, x_n)$ строится следующим образом: каждый член $ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ многочлена $f(x_1, x_2, \dots, x_n)$ заменяется членом $ax_1^{r_1} x_2^{r_2} \dots x_n^{r_n}$, где $r_1, r_2, \dots, r_n$ определяются из условий

$$k_i = q_i(p - 1) + r_i, \quad 1 \leq r_i \leq p - 1,$$

Например, если

$$f(x_1, x_2, x_3) = x_1^{10} x_2^2 x_3 + 2x_2^{10} x_3^8 - x_1^6 x_2^4 x_3^5 \in Z_5[x_1, x_2, x_3],$$

то

$$f_0(x_1, x_2, x_3) = x_1^2 x_2^4 x_3 + 2x_2^2 x_3^4 - x_1^2 x_2^4 x_3 = 2x_2^2 x_3^4.$$

Заметим, что многочлен $f_0(x_1, x_2, \dots, x_n)$ есть единственный многочлен имеющий по каждой переменной степень не выше $p-1$ и определяющий ту же функцию, что и $f(x_1, x_2, \dots, x_n)$. Действительно, любые два таких многочлена определяют одну и ту же функцию и, по предыдущему, равны.

В качестве приложения докажем так называемую теорему Шевалле. Пусть имеется алгебраическое сравнение с n неизвестными:

$$f(x_1, x_2, \dots, x_n) \equiv 0 \pmod{p}, \quad (11)$$

где p — простое число, $f(x_1, x_2, \dots, x_n)$ — многочлен с целыми коэффициентами, не имеющий свободного члена. Любой набор целых чисел, делящихся на p , будет решением этого сравнения; такие решения будем называть тривиальными. Теорема Шевалле состоит в том, что если степень многочлена $f(x_1, x_2, \dots, x_n)$ (по совокупности переменных) меньше, чем n , то сравнение (11) имеет нетривиальное решение. Например, сравнение $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{p}$ в силу этой теоремы при любом p имеет нетривиальное решение.

Для доказательства теоремы Шевалле представим рассматриваемое сравнение в виде уравнения

$$\bar{f}(x_1, x_2, \dots, x_n) = 0 \quad (12)$$

над полем Z_p (ср. п. 5 § 2 гл. I). Здесь $\bar{f}(x_1, x_2, \dots, x_n)$ обозначает многочлен, получаемый из $f(x_1, x_2, \dots, x_n)$ заменой всех коэффициентов их классами вычетов по модулю p . Из условия теоремы следует, что $\bar{f}(\bar{0}, \bar{0}, \dots, \bar{0}) = \bar{0}$ и что ст. $\bar{f}(x_1, x_2, \dots, x_n) = m < n$. Нужно доказать, что уравнение (12) имеет ненулевое решение.

Предположим, что уравнение (12) имеет только нулевое решение. Тогда многочлен $1 - \bar{f}(x_1, x_2, \dots, x_n)^{p-1}$ определяет ту же функцию, что и многочлен $(1 - x_1^{p-1})(1 - x_2^{p-1}) \dots (1 - x_n^{p-1})$, поскольку в точке $(\bar{0}, \bar{0}, \dots, \bar{0})$ оба многочлена принимают значение $\bar{1}$, а во всех остальных точках обращаются в нуль. Заметим, что многочлен $(1 - x_1^{p-1})(1 - x_2^{p-1}) \dots (1 - x_n^{p-1})$ имеет по каждой переменной степень $p-1$. Следовательно, он должен получаться из многочлена $1 - \bar{f}(x_1, x_2, \dots, x_n)^{p-1}$ с помощью описанной выше процедуры. Однако это невозможно, поскольку указанная процедура, как легко видеть, не увеличивает степени по совокупности переменных, а степень многочлена $1 - \bar{f}(x_1, x_2, \dots, x_n)^{p-1}$, равная $m(p-1)$, меньше, чем степень многочлена $(1 - x_1^{p-1})(1 - x_2^{p-1}) \dots (1 - x_n^{p-1})$, равная $n(p-1)$. Полученное противоречие доказывает теорему.

6. Разложение на неприводимые множители. Переходя к изучению свойств делимости в кольце многочленов от n переменных, мы будем теперь рассматривать многочлены над полем.

Из теоремы 2 § 3 гл. II следует следующая теорема:

Теорема 5. Кольцо многочленов от n переменных над полем P является факториальным кольцом.

Доказательство. Проведем индукцию по n . Для $n=1$ факториальность была доказана в § 2 гл. II. Предположим теперь, что кольцо $P[x_1, x_2, \dots, x_{n-1}]$ факториально, и докажем, исходя из этого, факториальность кольца $P[x_1, x_2, \dots, x_n]$. В п. 5 было показано, что кольцо $P[x_1, x_2, \dots, x_n]$ можно представить как кольцо

многочленов от одной переменной x_n над кольцом $P[x_1, x_2, \dots, x_{n-1}]$. Его факториальность следует тогда из теоремы 2 § 3 гл. II, согласно которой кольцо многочленов от одной переменной над факториальным кольцом также факториально.

Как и при $n = 1$, простые элементы кольца $P[x_1, x_2, \dots, x_n]$ называются *неприводимыми многочленами*. Обратимыми элементами кольца $P[x_1, x_2, \dots, x_n]$, как следует, например, из теоремы 3, являются только многочлены нулевой степени, т. е. ненулевые элементы поля P . Ввиду этого неприводимый многочлен может быть определен как такой многочлен положительной степени, который не разлагается в произведение двух многочленов положительной степени.

Так как при умножении многочленов степени складываются (теорема 3), то всякий многочлен первой степени («линейный многочлен») неприводим. Существуют, однако, и другие неприводимые многочлены. Более того, при $n \geq 2$ неприводимы в некотором смысле «почти все» многочлены.

Пример 3. Докажем неприводимость многочлена

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$$

в кольце $\mathbb{C}[x_1, x_2, x_3]$.

Рассмотрим $f(x_1, x_2, x_3)$ как многочлен $F(x_3)$ с коэффициентами из кольца $K = \mathbb{C}[x_1, x_2]$. Так как его старший коэффициент равен 1, то он не делится ни на какой необратимый элемент кольца K . Поэтому если многочлен $F(x_3)$ не является простым элементом кольца $K[x_3]$, то он разлагается в произведение линейного и квадратного многочленов, причем произведение их старших коэффициентов равно 1. Можно считать, что линейный множитель имеет вид $x_3 - g$, где $g \in K$. По теореме Безу, g_3 является тогда корнем многочлена $F(x_3)$, т. е. $g^3 = -x_1^3 - x_2^3$. Докажем, что в кольце K не существует элемента g , удовлетворяющего этому условию. В самом деле, так как при возведении в куб степень многочлена утраивается, такой элемент g должен был бы быть многочленом первой степени от x_1 и x_2 , т. е. многочленом вида $ax_1 + bx_2 + c$ ($a, b, c \in P$); однако равенство $-x_1^3 - x_2^3 = (ax_1 + bx_2 + c)^3$ не имеет места ни при каких a, b, c , что следует, например, из сравнения коэффициентов при $x_1^2 x_2$.

7. Выделение линейных множителей. Для многочленов от нескольких переменных имеет место следующее обобщение теоремы Безу.

Теорема 6. Пусть P — бесконечное поле. Многочлен $f(x_1, x_2, \dots, x_n) \in P[x_1, x_2, \dots, x_n]$ делится на линейный многочлен

$$p(x_1, x_2, \dots, x_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n + b \quad (13)$$

тогда и только тогда, когда он обращается в нуль во всякой точке пространства P^n , в которой обращается в нуль многочлен $p(x_1, x_2, \dots, x_n)$.

При $n = 1$ и $p(x_1) = x_1 - x_0$, где $x_0 \in P$, утверждение этой теоремы совпадает с теоремой Безу, поскольку многочлен $x_1 - x_0$ обращается в нуль в точке x_0 и только в этой точке,

Доказательство. Рассмотрим сначала частный случай, когда $p(x_1, x_2, \dots, x_n) = x_n$. Представим $f(x_1, x_2, \dots, x_n)$ в виде многочлена от x_n :

$$f(x_1, x_2, \dots, x_n) = \sum_{k=0}^m f_k(x_1, x_2, \dots, x_{n-1})x_n^k.$$

Очевидно, что $f(x_1, x_2, \dots, x_n)$ делится на x_n тогда и только тогда, когда $f_0(x_1, x_2, \dots, x_{n-1}) = 0$. Так как поле P бесконечно, то по теореме 4 многочлен $f_0(x_1, x_2, \dots, x_{n-1})$ является нулевым тогда и только тогда, когда $f_0(x_{01}, x_{02}, \dots, x_{0,n-1}) = 0$ для любых $x_{01}, x_{02}, \dots, x_{0,n-1} \in P$. Очевидно, что

$$f_0(x_{01}, x_{02}, \dots, x_{0,n-1}) = f(x_{01}, x_{02}, \dots, x_{0,n-1}, 0).$$

Это равенство показывает, что обращение в нуль многочлена $f_0(x_1, x_2, \dots, x_{n-1})$ во всех точках пространства P^{n-1} равносильно обращению в нуль многочлена $f(x_1, x_2, \dots, x_n)$ во всех точках пространства P^n с нулевой координатой x_n . Тем самым для рассматриваемого частного случая теорема доказана.

Обратимся к общему случаю. Предположим для определенности, что в выражении (13) коэффициент a_n не равен нулю. Сделаем обратимую линейную замену переменных:

$$y_1 = x_1, y_2 = x_2, \dots, y_{n-1} = x_{n-1}, y_n = p(x_1, x_2, \dots, x_n)$$

$$\left(\text{при этом } x_n = -\frac{a_1}{a_n} y_1 - \frac{a_2}{a_n} y_2 - \dots - \frac{a_{n-1}}{a_n} y_{n-1} + \frac{1}{a_n} y_n - \frac{b}{a_n} \right).$$

Пусть $g(y_1, y_2, \dots, y_n)$ — многочлен от $y_1, y_2, \dots, y_n$, получаемый после такой замены из многочлена $f(x_1, x_2, \dots, x_n)$. Так как $p(x_1, x_2, \dots, x_n) = y_n$, то вопрос о делимости многочлена $f(x_1, x_2, \dots, x_n)$ на $p(x_1, x_2, \dots, x_n)$ равносильен вопросу о делимости многочлена $g(y_1, y_2, \dots, y_n)$ на y_n . Тем самым доказательство теоремы сведено к рассмотренному выше частному случаю.

В случае, когда $P = \mathbb{C}$, теорема, аналогичная теореме 6, справедлива для любого неприводимого многочлена $p(x_1, x_2, \dots, x_n)$. Однако доказательство этой теоремы значительно более сложно, и мы не будем здесь его приводить.

Пример 4. Пусть $f(x), g(x) \in P[x]$ — нормированные многочлены, разлагающиеся на линейные множители. Докажем следующую формулу для результата этих многочленов (см. п. 6 § 1 гл. II):

$$R(f, g) = \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j), \quad (14)$$

где $x_1, x_2, \dots, x_n$ (соответственно $y_1, y_2, \dots, y_m$) — корни многочлена $f(x)$ (соответственно $g(x)$).

Пусть

$$\begin{aligned} f(x) &= x^n + a_1 x^{n-1} + \dots + a_n = (x - x_1)(x - x_2) \dots (x - x_n), \\ g(x) &= x^m + b_1 x^{m-1} + \dots + b_m = (x - y_1)(x - y_2) \dots (x - y_m). \end{aligned} \quad (15)$$

Согласно определению результата,

$$R(f, g) = \begin{vmatrix} 1 & a_1 & \dots & a_n \\ & 1 & a_1 & \dots & a_n \\ & & \ddots & \ddots & \ddots \\ & & & 1 & a_1 & \dots & a_n \\ 1 & b_1 & \dots & b_m \\ & 1 & b_1 & \dots & b_m \\ & & \ddots & \ddots & \ddots & \ddots \\ & & & 1 & b_1 & \dots & b_m \end{vmatrix} \quad (16)$$

(элементы матрицы, которые здесь не выписаны, равны нулю).

Выразим по формулам Виета коэффициенты многочленов $f(x)$ и $g(x)$ через их корни и подставим эти выражения в определитель (16). Будем рассматривать $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ как независимые переменные. Тогда при раскрытии определителя (16) результат представится как многочлен от этих переменных. Если в какой-то член определителя из 1-й строки входит элемент из столбца с номером k_1 , из 2-й строки — элемент из столбца с номером k_2 и т. д., причем все эти элементы относятся к числу выписанных в формуле (16), то степень этого члена равна

$$(k_1 - 1) + (k_2 - 2) + \dots + (k_m - m) + (k_{m+1} - 1) + (k_{m+2} - 2) + \dots + (k_{m+n} - n) = (k_1 + k_2 + \dots + k_{m+n}) - (1 + 2 + \dots + m) - (1 + 2 + \dots + n).$$

Так как $(k_1, k_2, \dots, k_{m+n})$ есть перестановка из чисел $1, 2, \dots, m+n$, то

$$k_1 + k_2 + \dots + k_{m+n} = 1 + 2 + \dots + (m+n) = \frac{(m+n)(m+n+1)}{2}.$$

Следовательно, степень каждого ненулевого члена определителя равна

$$\frac{(m+n)(m+n+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} = mn,$$

т. е. $R(f, g)$ — однородный многочлен степени mn от переменных $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$.

Дадим теперь переменным $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ какие-то значения. Если для некоторых i, j значение x_i будет равно значению y_j , то многочлены $f(x)$ и $g(x)$, определяемые по формулам (15), будут иметь общий корень и, стало быть, не будут взаимно простыми. По теореме 5 § 1 гл. II их результат в этом случае будет равен нулю. Теорема 6 этого параграфа позволяет сделать отсюда вывод*, что $R(f, g)$ делится на $x_i - y_j$ (как многочлен от $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$). Так как число различных разностей $x_i - y_j$ равно nm , то разложение многочлена $R(f, g)$ на неприводимые множители в кольце $P[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ имеет вид

$$R(f, g) = c \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j), \quad (17)$$

где $c \in P$. Для вычисления коэффициента c положим все x_i равными 1, а все y_j равными 0. При этом, согласно (15), имеем:

$$f(x) = (x-1)^n, \quad g(x) = x^m,$$

результат легко вычисляется по формуле (16) и оказывается равным 1. Произведение, стоящее в правой части равенства (17), в этом случае также равно 1. Следовательно, $c = 1$.

Аналогично можно вывести следующую формулу для дискриминанта многочлена (см. п. 8 § 2 гл. II):

$$D(f) = \prod_{\substack{i, j=1 \\ i > j}}^n (x_i - x_j)^2. \quad (18)$$

Вопросы для самопроверки

1. Дайте определение кольца многочленов от n переменных над произвольной областью целостности.

* В формулировке теоремы 6 требуется, чтобы поле P было бесконечно. Однако если поле P конечно, то его можно расширить до бесконечного поля (например, до поля $P(x)$ рациональных дробей), и тогда наше рассуждение будет справедливо.

2. Докажите ассоциативность умножения в кольце многочленов от n переменных.
3. Что такое степень многочлена от n переменных?
4. Что такое однородный многочлен?
5. Как определяется лексикографическое упорядочение одночленов?
6. Докажите отсутствие делителей нуля в кольце многочленов от n переменных.
7. Чему равна степень произведения двух многочленов от n переменных?
8. Докажите, что если произведение двух многочленов является однородным многочленом, то каждый из них также однороден.
9. Что такое выделение одной переменной в многочлене от n переменных?
10. Докажите, что функция, определяемая произведением двух многочленов от n переменных, равна произведению определяемых ими функций.
11. Пусть P — поле нулевой характеристики. Могут ли различные многочлены из кольца $P[x_1, x_2, \dots, x_n]$ определять одну и ту же функцию?
12. Пусть P — произвольное поле. Докажите, что кольцо $P[x_1, x_2, \dots, x_n]$ факториально.
13. Докажите, что все неприводимые множители однородного многочлена из кольца $P[x_1, x_2, \dots, x_n]$ также являются однородными многочленами.

Упражнения

1. Найдите однородные компоненты многочлена из кольца $R[x_1, x_2, x_3]$:
 - а) $(x_1^2 + x_2)(x_2^2 + x_3)(x_3^2 + x_1)$;
 - б) $(x_1^4 - x_2x_3 + 1)^2$.
2. Расположите в порядке лексикографического убывания члены многочлена из кольца $R[x_1, x_2, x_3]$:
 - а) $x_1^2x_2^2x_3^2 - x_1^3 + x_2^4 + 2x_1^2x_3^4$;
 - б) $(x_1^2 - x_2x_3)(x_2^2 - x_3x_1)(x_3^2 - x_1x_2)$.
3. Докажите неприводимость следующих многочленов в кольце $C[x_1, x_2, \dots, x_n]$:
 - а) $x_1^2 + x_2^2 + \dots + x_n^2, n \geq 3$;
 - б) $x_1^3 + x_2^6 + x_3^9$.

§ 2. СИММЕТРИЧЕСКИЕ МНОГОЧЛЕНЫ

1. Основные определения. В этом параграфе мы будем рассматривать многочлены над произвольной областью целостности K .

Многочлен $f(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$ называется *симметрическим*, если он не меняется при любой перестановке переменных, т. е. если

$$f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = f(x_1, x_2, \dots, x_n)$$

для любой перестановки $(i_1, i_2, \dots, i_n)$ чисел $1, 2, \dots, n$. Например, многочлен $x_1^2 x_2^2 + x_2^2 x_3^2 + x_3^2 x_1^2 + 2x_1 + 2x_2 + 2x_3$ является симметрическим. Многочлен $f(x_1, x_2, x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$ не является симметрическим, так как

$$f(x_1, x_3, x_2) = x_1^2 x_3 + x_3^2 x_2 + x_2^2 x_1 \neq f(x_1, x_2, x_3).$$

Строение симметрических многочленов можно представить себе, исходя из следующих соображений. Пусть $(i_1, i_2, \dots, i_n)$ — произвольная перестановка чисел $1, 2, \dots, n$. Если симметрический многочлен $f(x_1, x_2, \dots, x_n)$ содержит член $ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$, то он должен также содержать член $ax_{i_1}^{k_1} x_{i_2}^{k_2} \dots x_{i_n}^{k_n}$. Обозначим через $S(x_1^{k_1} x_2^{k_2} \dots x_n^{k_n})$ сумму различных одночленов, которые получают-ся из $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ всевозможными перестановками переменных. Очевидно, что это будет симметрический многочлен. Из предыдущего следует, что *любой симметрический многочлен есть линейная комбинация многочленов вида*

$$S(x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}).$$

В частности, отсюда вытекает, что *всякий симметрический многочлен является суммой однородных симметрических многочленов*.

Особую роль среди симметрических многочленов, как мы увидим в дальнейшем, играют так называемые *элементарные симметрические многочлены*:

$$\begin{aligned}\sigma_1(x_1, x_2, \dots, x_n) &= x_1 + x_2 + \dots + x_n, \\ \sigma_2(x_1, x_2, \dots, x_n) &= x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n, \\ &\dots \\ \sigma_n(x_1, x_2, \dots, x_n) &= x_1 x_2 \dots x_n,\end{aligned}\tag{1}$$

которые мы будем обозначать просто $\sigma_1, \sigma_2, \dots, \sigma_n$. По определению, k -й элементарный симметрический многочлен есть сумма всевозможных произведений по k различных переменных. Полезно вспомнить, что, согласно формулам Виета, коэффициенты нормированного многочлена $f(x)$ от одной переменной с точностью до знака равны элементарным симметрическим многочленам от его корней (точнее говоря, значениям, которые принимают элементарные симметрические многочлены, если вместо переменных подставить корни многочлена $f(x)$).

Другую важную серию симметрических многочленов составляют так называемые *степенные суммы*

$$s_k = s_k(x_1, x_2, \dots, x_n) = x_1^k + x_2^k + \dots + x_n^k.\tag{2}$$

Заметим, что используя введенное выше обозначение S , можно записать:

$$\sigma_k = S(x_1 x_2 \dots x_k), \quad s_k = S(x_1^k).$$

2. Основная теорема о симметрических многочленах. Легко понять, что сумма, разность и произведение симметрических многочленов также являются симметрическими многочленами. Например, пусть h есть произведение симметрических многочленов f и g . Для любой перестановки $(i_1, i_2, \dots, i_n)$ имеем:

$$\begin{aligned} h(x_{i_1}, x_{i_2}, \dots, x_{i_n}) &= f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) g(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = \\ &= f(x_1, x_2, \dots, x_n) g(x_1, x_2, \dots, x_n) = h(x_1, x_2, \dots, x_n); \end{aligned}$$

следовательно, $h(x_1, x_2, \dots, x_n)$ — симметрический многочлен. Очевидно также, что элементы кольца K (многочлены нулевой степени) являются симметрическими многочленами.

Таким образом, симметрические многочлены образуют подкольцо в кольце $K[x_1, x_2, \dots, x_n]$, причем это подкольцо содержит кольцо K . Следовательно, если $F(X_1, X_2, \dots, X_m)$ — произвольный многочлен с коэффициентами из кольца K и $f_1, f_2, \dots, f_m$ — любые симметрические многочлены от $x_1, x_2, \dots, x_n$, то $F(f_1, f_2, \dots, f_m)$ также будет симметрическим многочленом от $x_1, x_2, \dots, x_n$. Естественно поставить вопрос, нельзя ли найти такие симметрические многочлены $f_1, f_2, \dots, f_m$, чтобы всякий симметрический многочлен можно было выразить через них указанным выше образом. Оказывается, что в качестве таких многочленов $f_1, f_2, \dots, f_m$ можно взять элементарные симметрические многочлены $\sigma_1, \sigma_2, \dots, \sigma_n$ (при этом $m = n$). А именно, имеет место следующая теорема:

Теорема 1. *Всякий симметрический многочлен $f(x_1, x_2, \dots, x_n)$ может быть представлен в виде многочлена от элементарных симметрических многочленов.*

Другими словами, можно найти такой многочлен $F(X_1, X_2, \dots, X_n)$ от n переменных с коэффициентами из кольца K , что

$$F(\sigma_1, \sigma_2, \dots, \sigma_n) = f.$$

Доказательство этой теоремы будет проведено в следующем пункте, а сейчас рассмотрим некоторые примеры. Легко видеть, что

$$\begin{aligned} \sigma_1^2 &= (x_1 + x_2 + \dots + x_n)^2 = x_1^2 + x_2^2 + \dots + x_n^2 + \\ &+ 2(x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n) = S(x_1^2) + 2S(x_1 x_2), \end{aligned}$$

откуда

$$S(x_1^2) = \sigma_1^2 - 2\sigma_2. \quad (3)$$

Далее,

$$\sigma_1 \sigma_2 = S(x_1^2 x_2) + 3S(x_1 x_2 x_3),$$

так что

$$S(x_1^2 x_2) = \sigma_1 \sigma_2 - 3\sigma_3. \quad (4)$$

Наконец, из равенства $S(x_1^2) \sigma_1 = S(x_1^3) + S(x_1^2 x_2)$ находим, что

$$S(x_1^3) = \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3. \quad (5)$$

Формулы (3), (4) и (5) позволяют выразить через элементарные симметрические многочлены любой симметрический многочлен, степень которого не выше 3. (При этом предполагается, что $n \geq 3$; если $n = 2$, то следует считать $\sigma_3 = 0$.)

Пример 1. Выразим через $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ многочлен

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4).$$

Прежде всего убедимся, что многочлен f симметрический. Легко заметить, что он является произведением всевозможных выражений $\varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3 + \varepsilon_4 x_4$, в каждом из которых:

а) среди коэффициентов $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ два равны 1, а остальные два равны -1 ;

б) $\varepsilon_1 = 1$.

Пусть (i_1, i_2, i_3, i_4) — любая перестановка чисел 1, 2, 3, 4. Тогда многочлен $f(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4})$ будет произведением всевозможных выражений $\varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3 + \varepsilon_4 x_4$, удовлетворяющих условию а) и, вместо условия б), условию $\varepsilon_{i_1} = 1$. Если $i_1 = 1$, то многочлен $f(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4})$ будет произведением тех же множителей, что и $f(x_1, x_2, x_3, x_4)$; если $i_1 \neq 1$, то два множителя будут отличаться знаком от соответствующих множителей многочлена $f(x_1, x_2, x_3, x_4)$. В любом случае

$$f(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}) = f(x_1, x_2, x_3, x_4).$$

Таким образом, f — симметрический многочлен.

Коэффициенты многочлена f при $x_1^3, x_1^2 x_2$ и $x_1 x_2 x_3$ равны соответственно 1, -1 и 2. Следовательно,

$$f = S(x_1^3) - S(x_1^2 x_2) + 2S(x_1 x_2 x_3).$$

По формулам (4) и (5) находим, что

$$f = \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3 - \sigma_1 \sigma_2 + 3\sigma_3 + 2\sigma_3 = \sigma_1^3 - 4\sigma_1 \sigma_2 + 8\sigma_3.$$

3. Доказательство основной теоремы.

Лемма 1. Пусть $u = ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ — лексикографически старший член симметрического многочлена $f(x_1, x_2, \dots, x_n)$. Тогда

$$k_1 \geq k_2 \geq \dots \geq k_n. \quad (6)$$

Доказательство. Рассуждая от противного, предположим, что $k_i < k_{i+1}$ для некоторого i . Наряду с членом u многочлен

$f(x_1, x_2, \dots, x_n)$ должен содержать член, получающийся из него перестановкой x_i и x_{i+1} , т. е. член

$$u' = ax_1^{k_1} x_2^{k_2} \dots x_{i+1}^{k_{i+1}} x_i^{k_i} \dots x_n^{k_n}.$$

Легко видеть, что $u' > u$ (первые $i - 1$ показателей совпадают, а i -й показатель у u' больше, чем у u). Это противоречит тому, что u — старший член многочлена f .

Л е м м а 2. Для любого одночлена $u = ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ ($a \neq 0$), показатели которого удовлетворяют неравенствам (6), существует многочлен вида

$$a\sigma_1^{l_1} \sigma_2^{l_2} \dots \sigma_n^{l_n},$$

старший член которого совпадает с u .

Д о к а з а т е л ь с т в о. Старший член многочлена σ_k равен $x_1 x_2 \dots x_k$. В силу теоремы 2 § 1, старший член произведения нескольких многочленов от $x_1, x_2, \dots, x_n$ равен произведению их старших членов. Следовательно, старший член многочлена $a\sigma_1^{l_1} \sigma_2^{l_2} \dots \sigma_n^{l_n}$ равен

$$ax_1^{l_1} (x_1 x_2)^{l_2} \dots (x_1 x_2 \dots x_n)^{l_n} = ax_1^{l_1 + l_2 + \dots + l_n} x_2^{l_2} \dots x_n^{l_n}.$$

Приравнивая его одночлену u , получаем следующую систему уравнений для определения показателей $l_1, l_2, \dots, l_n$:

$$\begin{cases} l_1 + l_2 + \dots + l_n = k_1 \\ l_2 + \dots + l_n = k_2 \\ \dots \\ l_n = k_n \end{cases} \quad (7)$$

Вычтем из 1-го уравнения 2-е, из 2-го — 3-е и т. д., кончая $(n-1)$ -м уравнением. В результате получим эквивалентную систему из следующих уравнений:

$$\begin{aligned} l_i &= k_i - k_{i+1} \quad (i = 1, 2, \dots, n-1), \\ l_n &= k_n. \end{aligned} \quad (8)$$

Отсюда видно, что набор чисел $(k_1 - k_2, k_2 - k_3, \dots, k_{n-1} - k_n, k_n)$ является единственным решением системы (7). Из условия леммы следует, что все эти числа неотрицательны и, значит, могут быть показателями одночлена. Таким образом, в качестве искомого многочлена можно взять

$$h = a\sigma_1^{k_1 - k_2} \sigma_2^{k_2 - k_3} \dots \sigma_{n-1}^{k_{n-1} - k_n} \sigma_n^{k_n}. \quad (9)$$

Перейдем непосредственно к доказательству теоремы 1. Пусть $f(x_1, x_2, \dots, x_n)$ — произвольный симметрический многочлен. Требуется найти такой многочлен $F(X_1, X_2, \dots, X_n)$ от n переменных, чтобы

$$F(\sigma_1, \sigma_2, \dots, \sigma_n) = f. \quad (10)$$

Если $f = 0$, то можно взять $F = 0$, и доказательство закончено. Пусть $f \neq 0$, и пусть $u = ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ — старший член

многочлена f . Согласно лемме 1, выполняются неравенства (6). По лемме 2, существует такой одночлен $h_1(X_1, X_2, \dots, X_n)$, что старший член многочлена $h_1(\sigma_1, \sigma_2, \dots, \sigma_n)$ равен u . Рассмотрим разность

$$f_1 = f - h_1(\sigma_1, \sigma_2, \dots, \sigma_n).$$

Если $f_1 = 0$, то

$$f = h_1(\sigma_1, \sigma_2, \dots, \sigma_n),$$

и доказательство закончено.

Если f_1 — ненулевой многочлен, то, во всяком случае, его старший член u_1 младше, чем u . Существует такой одночлен $h_2(X_1, X_2, \dots, X_n)$, что старший член многочлена $h_2(\sigma_1, \sigma_2, \dots, \sigma_n)$ равен u_1 .

Положим

$$f_2 = f_1 - h_2(\sigma_1, \sigma_2, \dots, \sigma_n) = f - h_1(\sigma_1, \sigma_2, \dots, \sigma_n) - h_2(\sigma_1, \sigma_2, \dots, \sigma_n).$$

Если $f_2 = 0$, то

$$f = h_1(\sigma_1, \sigma_2, \dots, \sigma_n) + h_2(\sigma_1, \sigma_2, \dots, \sigma_n),$$

и доказательство закончено. Если f_2 — ненулевой многочлен, то его старший член u_2 младше, чем u_1 . Продолжая этот процесс, получаем последовательность многочленов $f, f_1, f_2, \dots$, старшие члены которых удовлетворяют неравенствам

$$u > u_1 > u_2 > \dots \quad (11)$$

Покажем, что описанный выше процесс должен оборваться, т. е. на некотором шаге должен получиться нулевой многочлен. Из неравенств (11) и определения лексикографического упорядочения следует, что показатели степеней x_1 в одночленах $u, u_1, u_2, \dots$ образуют невозрастающую последовательность. Так как все они неотрицательны, то существует такой номер m_1 , что при всех $m \geq m_1$ показатель степени x_1 в одночлене u_m один и тот же. При лексикографическом сравнении этих одночленов показатель степени x_1 уже не будет играть роли и, следовательно, показатели степени x_2 в этих одночленах образуют невозрастающую последовательность. Начиная с некоторого номера m_2 и эти показатели будут равны между собой. Продолжая это рассуждение, находим такой номер $m_n = M$, что при всех $m \geq M$ все соответствующие показатели одночленов u_m равны. При этом условии неравенство $u_M > u_{M+1}$ невозможно. Следовательно, $f_{M+1} = 0$.

Согласно построению многочленов $f_1, f_2, \dots$, имеем:

$$f_{M+1} = f - h_1(\sigma_1, \sigma_2, \dots, \sigma_n) - h_2(\sigma_1, \sigma_2, \dots, \sigma_n) - \dots - h_{M+1}(\sigma_1, \sigma_2, \dots, \sigma_n),$$

и, значит,

$$f = h_1(\sigma_1, \sigma_2, \dots, \sigma_n) + h_2(\sigma_1, \sigma_2, \dots, \sigma_n) + \dots + h_{M+1}(\sigma_1, \sigma_2, \dots, \sigma_n) = F(\sigma_1, \sigma_2, \dots, \sigma_n),$$

где $F = h_1 + h_2 + \dots + h_{M+1}$. Теорема доказана.

4. Теорема единственности. Естественно задаться вопросом, однозначно ли выражение данного симметрического многочлена f через многочлены $\sigma_1, \sigma_2, \dots, \sigma_n$, т. е. однозначно ли определен многочлен F , удовлетворяющий условию (10). Оказывается, что ответ на этот вопрос положителен.

Т е о р е м а 2. *Всякий симметрический многочлен $f(x_1, x_2, \dots, x_n)$ единственным образом представляется в виде многочлена от элементарных симметрических многочленов.*

Докажем вначале одну лемму.

Л е м м а 3. *Пусть*

$$U(\sigma_1, \sigma_2, \dots, \sigma_n) = a\sigma_1^{l_1}\sigma_2^{l_2}\dots\sigma_n^{l_n},$$

$$V(\sigma_1, \sigma_2, \dots, \sigma_n) = b\sigma_1^{m_1}\sigma_2^{m_2}\dots\sigma_n^{m_n}.$$

Если старшие члены многочленов $U(\sigma_1, \sigma_2, \dots, \sigma_n)$ и $V(\sigma_1, \sigma_2, \dots, \sigma_n)$ (от $x_1, x_2, \dots, x_n$) пропорциональны, то $l_i = m_i$ при $i = 1, 2, \dots, n$.

Д о к а з а т е л ь с т в о. Если $k_1, k_2, \dots, k_n$ — показатели старшего члена многочлена $U(\sigma_1, \sigma_2, \dots, \sigma_n)$, то $l_1, l_2, \dots, l_n$ удовлетворяют уравнениям (7). Этим же уравнениям удовлетворяют и $m_1, m_2, \dots, m_n$. При доказательстве леммы 2 мы видели, что система уравнений (7) имеет единственное решение. Следовательно, $l_i = m_i$ ($i = 1, 2, \dots, n$).

Д о к а з а т е л ь с т в о т е о р е м ы 2. Предположим, что F и G — два различных многочлена от n переменных такие, что

$$f = F(\sigma_1, \sigma_2, \dots, \sigma_n) = G(\sigma_1, \sigma_2, \dots, \sigma_n).$$

Положим $H = F - G$, тогда $H \neq 0$, но

$$H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0. \quad (12)$$

Пусть $U_1, U_2, \dots, U_s$ — все члены многочлена H . Обозначим через u_i ($i = 1, 2, \dots, s$) старший член многочлена $U_i(\sigma_1, \sigma_2, \dots, \sigma_n)$. По лемме 3, среди одночленов $u_1, u_2, \dots, u_s$ нет пропорциональных. Выберем из них старший. Пусть это будет u_1 . По построению, одночлен u_1 старше всех остальных членов многочлена $U_i(\sigma_1, \sigma_2, \dots, \sigma_n)$ ($i = 1, 2, \dots, s$). Поэтому после приведения подобных членов в сумму

$$U_1(\sigma_1, \sigma_2, \dots, \sigma_n) + U_2(\sigma_1, \sigma_2, \dots, \sigma_n) + \dots + U_s(\sigma_1, \sigma_2, \dots, \sigma_n)$$

член u_1 сохранится. Отсюда следует, что эта сумма не равна нулю, что противоречит равенству (12). Тем самым теорема доказана.

5. Практические указания. Следуя доказательству теоремы 1, можно найти выражение любого конкретного симметрического многочлена через $\sigma_1, \sigma_2, \dots, \sigma_n$. Однако на практике удобнее применять другой способ, который мы сейчас изложим.

Для облегчения вычислений целесообразно представить данный симметрический многочлен в виде суммы однородных симметрических многочленов и каждый из них в отдельности выразить через $\sigma_1, \sigma_2, \dots, \sigma_n$, после чего сложить полученные выражения.

Для однородного симметрического многочлена $f(x_1, x_2, \dots, x_n)$ выражение через $\sigma_1, \sigma_2, \dots, \sigma_n$ может быть найдено следующим образом. Пусть степень многочлена f равна k . Тогда многочлены $f_1, f_2, \dots$, о которых идет речь в доказательстве теоремы 1, также будут однородными симметрическими многочленами степени k . Их старшие члены $u_1, u_2, \dots$ удовлетворяют неравенствам (11). Исходя из этого, можно указать возможные наборы показателей одночленов $u_1, u_2, \dots$. Это будут наборы $(k_1, k_2, \dots, k_n)$ целых неотрицательных чисел, удовлетворяющие следующим условиям:

- 1) $k_1 \geq k_2 \geq \dots \geq k_n$;
- 2) $k_1 + k_2 + \dots + k_n = k$;
- 3) одночлен $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ младше старшего члена многочлена f .

Для каждого из таких наборов $(k_1, k_2, \dots, k_n)$, а также для набора показателей старшего члена многочлена f нужно выписать по формулам (8) одночлен от $\sigma_1, \sigma_2, \dots, \sigma_n$, старший член которого как многочлена от $x_1, x_2, \dots, x_n$ равен $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$. Из доказательства теоремы 1 следует, что многочлен f будет линейной комбинацией найденных таким образом одночленов от $\sigma_1, \sigma_2, \dots, \sigma_n$. Коэффициенты этой линейной комбинации могут быть определены из системы линейных уравнений, которые получаются, если придавать переменным $x_1, x_2, \dots, x_n$ конкретные значения. (Коэффициент при одночлене от $\sigma_1, \sigma_2, \dots, \sigma_n$, соответствующем старшему члену самого многочлена f , равен, очевидно, коэффициенту этого старшего члена.)

Пример 2. Выразим через элементарные симметрические многочлены многочлен

$$f(x_1, x_2, x_3, x_4) = S(x_1^3 x_2).$$

Данный многочлен f — однородный многочлен четвертой степени; его старшим членом является одночлен $x_1^3 x_2$. Согласно вышеприведенному алгоритму, нужно найти всевозможные наборы (k_1, k_2, k_3, k_4) целых неотрицательных чисел, удовлетворяющие условиям:

- 1) $k_1 \geq k_2 \geq k_3 \geq k_4$;
- 2) $k_1 + k_2 + k_3 + k_4 = 4$;
- 3) одночлен $x_1^{k_1} x_2^{k_2} x_3^{k_3} x_4^{k_4}$ младше, чем $x_1^3 x_2$.

Выпишем эти наборы вместе с набором показателей старшего члена многочлена f в следующую таблицу:

3	1	0	0	$\sigma_1^2 \sigma_2$
2	2	0	0	σ_2^2
2	1	1	0	$\sigma_1 \sigma_3$
1	1	1	1	σ_4

В правом столбце указаны соответствующие одночлены от $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, показатели которых вычислены по формулам (8).

Многочлен f представляется в виде

$$f = \sigma_1^2 \sigma_2 + a \sigma_2^2 + b \sigma_1 \sigma_3 + c \sigma_4.$$

Для определения коэффициентов a, b, c будем придавать различные значения переменным x_1, x_2, x_3, x_4 и вычислять, какие значения при этом принимают левая и правая части равенства. Все вычисления расположим в таблицу, в первых четырех столбцах которой указаны значения, придаваемые переменным, в следующих пяти столбцах — значения, которые при этом принимают $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ и f , а в последнем столбце выписаны соответствующие уравнения для коэффициентов a, b, c .

x_1	x_2	x_3	x_4	σ_1	σ_2	σ_3	σ_4	f	
1	1	0	0	2	1	0	0	2	$2 = 4 + a$
1	1	1	0	3	3	1	0	6	$6 = 27 + 9a + 3b$
1	1	-1	-1	0	-2	0	1	-4	$-4 = 4a + c$

После преобразований получаем следующую систему уравнений:

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

откуда $a = -2, b = -1, c = 4$.

Таким образом,

$$f = \sigma_1^2 \sigma_2 - 2\sigma_2^2 - \sigma_1 \sigma_3 + 4\sigma_4.$$

Пример 3. Выразим через элементарные симметрические многочлены многочлен

$$f(x_1, x_2, x_3) = (x_1 x_2 + x_3)(x_1 x_3 + x_2)(x_2 x_3 + x_1).$$

Раскрыв скобки, представим многочлен f в виде суммы однородных многочленов:

$$\begin{aligned} f &= x_1^2 x_2^2 x_3^2 + (x_1^3 x_2 x_3 + x_1 x_2^3 x_3 + x_1 x_2 x_3^3) + \\ &+ (x_1^2 x_2^2 + x_1^2 x_3^2 + x_2^2 x_3^2) + x_1 x_2 x_3. \end{aligned}$$

Имеем:

$$\begin{aligned} x_1^2 x_2^2 x_3^2 &= \sigma_3^2, \\ x_1^3 x_2 x_3 + x_1 x_2^3 x_3 + x_1 x_2 x_3^3 &= (x_1^2 + x_2^2 + x_3^2) \sigma_3 = \\ &= (\sigma_1^2 - 2\sigma_2) \sigma_3 = \sigma_1^2 \sigma_3 - 2\sigma_2 \sigma_3, \\ x_1^2 x_2^2 + x_1^2 x_3^2 + x_2^2 x_3^2 &= \sigma_2^2 - 2(x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2) = \\ &= \sigma_2^2 - 2\sigma_1 \sigma_3, \\ x_1 x_2 x_3 &= \sigma_3. \end{aligned}$$

(Ввиду простоты получившихся многочленов их выражения через $\sigma_1, \sigma_2, \sigma_3$ находятся непосредственно.) Следовательно,

$$f = \sigma_3^2 + \sigma_1^2 \sigma_3 - 2\sigma_2 \sigma_3 + \sigma_2^2 - 2\sigma_1 \sigma_3 + \sigma_3.$$

6. Некоторые приложения. Пусть $h(x)$ — многочлен степени n с коэффициентами из поля P , имеющий n корней $c_1, c_2, \dots, c_n$ в этом поле. По формулам Виета значения элементарных симметрических многочленов от n переменных в точке $(c_1, c_2, \dots, c_n)$ выражаются через коэффициенты многочлена. Пользуясь этим обстоятельством и теоремой 1, можно найти значение любого симметрического многочлена в точке $(c_1, c_2, \dots, c_n)$, не зная самих корней $c_1, c_2, \dots, c_n$.

В частности, любой многочлен $f(x)$ с числовыми коэффициентами, как мы покажем в § 2 гл. IV, имеет n корней в поле $\mathbb{C}$ комплексных чисел. Указанный выше способ позволяет вычислить любой симметрический многочлен от этих корней.

Пример 4. Найдем $c_1^3 + c_2^3 + c_3^3$, где c_1, c_2, c_3 — комплексные корни многочлена $2x^3 + x^2 + 1$.

По формуле (5)

$$x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \quad (13)$$

С другой стороны, по формулам Виета находим:

$$\sigma_1(c_1, c_2, c_3) = -\frac{1}{2},$$

$$\sigma_2(c_1, c_2, c_3) = 0,$$

$$\sigma_3(c_1, c_2, c_3) = -\frac{1}{2}.$$

Придавая переменным x_1, x_2, x_3 в равенстве (13) значения c_1, c_2, c_3 , получаем:

$$c_1^3 + c_2^3 + c_3^3 = \left(-\frac{1}{2}\right)^3 + 3\left(-\frac{1}{2}\right) = -\frac{13}{8}.$$

Пример 5. Пусть c_1, c_2, c_3, c_4 — корни многочлена

$$f(x) = x^4 + px^2 + qx + r \in \mathbb{C}[x].$$

Найдем многочлен третьей степени, корнями которого являются числа

$$a_1 = c_1c_2 + c_3c_4, \quad a_2 = c_1c_3 + c_2c_4, \quad a_3 = c_1c_4 + c_2c_3.$$

Запишем искомый многочлен в виде

$$g(x) = x^3 + ax^2 + bx + c.$$

Согласно формулам Виета,

$$a = -(a_1 + a_2 + a_3),$$

$$b = a_1a_2 + a_1a_3 + a_2a_3,$$

$$c = -a_1a_2a_3.$$

Рассмотрим многочлены

$$h_1 = x_1x_2 + x_3x_4, \quad h_2 = x_1x_3 + x_2x_4, \quad h_3 = x_1x_4 + x_2x_3.$$

Это всевозможные выражения вида $x_i x_j + x_k x_l$, где i, j, k, l — различные индексы. Поэтому при любой перестановке переменных $x_1, x_2,$

x_3, x_4 многочлены h_1, h_2, h_3 только переставляются между собой. Следовательно, выражения $h_1 + h_2 + h_3$, $h_1h_2 + h_1h_3 + h_2h_3$, $h_1h_2h_3$ являются симметрическими многочленами от x_1, x_2, x_3, x_4 .

Непосредственные вычисления показывают, что

$$h_1 + h_2 + h_3 = \sigma_2,$$

$$h_1h_2 + h_1h_3 + h_2h_3 = S(x_1^2x_2x_3) = \sigma_1\sigma_3 - 4\sigma_4,$$

$$h_1h_2h_3 = S(x_1^3x_2x_3x_4) + S(x_1^2x_2^2x_3^2) = S(x_1^2)\sigma_4 +$$

$$+ \sigma_3^2 - 2S(x_1^2x_2^2x_3x_4) = (\sigma_1^2 - 2\sigma_2)\sigma_4 + \sigma^2 - 2\sigma_2\sigma_4 =$$

$$= \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4.$$

Придавая в этих равенствах переменным x_1, x_2, x_3, x_4 значения c_1, c_2, c_3, c_4 и учитывая, что

$$\sigma_1(c_1, c_2, c_3, c_4) = 0,$$

$$\sigma_2(c_1, c_2, c_3, c_4) = p,$$

$$\sigma_3(c_1, c_2, c_3, c_4) = -q,$$

$$\sigma_4(c_1, c_2, c_3, c_4) = r$$

(формулы Виета для многочлена $f(x)$), получаем:

$$a_1 + a_2 + a_3 = p,$$

$$a_1a_2 + a_1a_3 + a_2a_3 = -4r,$$

$$a_1a_2a_3 = q^2 - 4pr.$$

Таким образом, искомым многочлен имеет вид

$$g(x) = x^3 - px^2 - 4rx + (4pr - q^2).$$

Этот пример будет использован в § 4 гл. IV для решения в радикалах уравнения четвертой степени.

Теория симметрических многочленов может быть применена к решению систем алгебраических уравнений вида

$$f_i(x_1, x_2, \dots, x_n) = 0 \quad (i = 1, 2, \dots, n),$$

где $f_1, f_2, \dots, f_n$ — симметрические многочлены. Выразив левые части уравнений через $\sigma_1, \sigma_2, \dots, \sigma_n$, иногда удается решить получившуюся систему уравнений относительно $\sigma_1, \sigma_2, \dots, \sigma_n$ и тем самым найти значения многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$ в точках, являющихся решениями исходной системы. Далее, из формул Виета следует, что если значения $\sigma_1, \sigma_2, \dots, \sigma_n$ в точке $(c_1, c_2, \dots, c_n)$ равны $a_1, a_2, \dots, a_n$, то $c_1, c_2, \dots, c_n$ — корни уравнения

$$t^n - a_1t^{n-1} + a_2t^{n-2} + \dots + (-1)^n a_n = 0.$$

Таким образом, решение исходной системы сводится к решению одного или нескольких уравнений n -й степени с одним неизвестным.

Пример 6. Решим систему уравнений

$$\begin{cases} x + y + z = 0, \\ x^2 + y^2 + z^2 = 42, \\ x^3 + y^3 + z^3 = 60. \end{cases}$$

Выражая по формулам (3) и (5) левые части уравнений через элементарные симметрические многочлены, приходим к следующей системе уравнений относительно $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{cases} \sigma_1 = 0, \\ \sigma_1^2 - 2\sigma_2 = 42, \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 60. \end{cases}$$

Решая эту систему, находим:

$$\sigma_1 = 0, \sigma_2 = -21, \sigma_3 = 20.$$

Следовательно, любое решение исходной системы есть набор из трех корней уравнения

$$t^3 - 21t - 20 = 0.$$

Одним из корней этого уравнения является -1 . Два других корня находятся после деления на $t + 1$. Это будут -4 и 5 . Таким образом, исходная система уравнений имеет 6 решений, представляющих собой всевозможные перестановки из чисел $-1, -4, 5$.

Вопросы для самопроверки

1. Являются ли симметрическими многочлены $x_1x_2 + x_3x_4$ и $x_1^3 + x_2^3 + x_3^3 - x_1x_2x_3$ из кольца $R[x_1, x_2, x_3, x_4]$?
2. Что такое элементарные симметрические многочлены?
3. Докажите, что если сумма двух однородных многочленов разных степеней является симметрическим многочленом, то каждый из них также является симметрическим многочленом.
4. Докажите, что любой многочлен от симметрических многочленов также является симметрическим многочленом.
5. В чем состоит основная теорема о симметрических многочленах?
6. Что можно сказать о старшем члене симметрического многочлена?
7. Покажите, что не может быть бесконечной убывающей (в смысле лексикографической упорядоченности) последовательности старших членов симметрических многочленов.
8. Какой старший член у многочлена $\sigma_1\sigma_2^3\sigma_4$, где $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ — элементарные симметрические многочлены от x_1, x_2, x_3, x_4 ?
9. Докажите, что если $H(X_1, X_2, \dots, X_n)$ — такой многочлен от переменных $X_1, X_2, \dots, X_n$, что $H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$, то $H(X_1, X_2, \dots, X_n) = 0$.
10. При каком условии на многочлен $H(X_1, X_2, \dots, X_n)$ многочлен $H(\sigma_1, \sigma_2, \dots, \sigma_n)$ от переменных $x_1, x_2, \dots, x_n$ будет однороден?

Упражнения

1. Выразите через элементарные симметрические многочлены следующие многочлены из кольца $Z[x_1, x_2, x_3]$:

а) $x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$;

б) $S(x_1^3 x_2)$;

в) $(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$;

г) $x_1^4 + x_2^4 + x_3^4 - 2x_1^2 x_2^2 - 2x_1^2 x_3^2 - 2x_2^2 x_3^2$;

д) $(x_1^2 + x_2 + x_3)(x_2^2 + x_1 + x_3)(x_3^2 + x_1 + x_2)$.

2. Выразите через элементарные симметрические многочлены следующие многочлены из кольца $\mathbf{Z}[x_1, x_2, x_3, x_4]$:

а) $(x_1^2 + 1)(x_2^2 + 1)(x_3^2 + 1)(x_4^2 + 1)$;

б) $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$.

3. Определите значение многочлена $f(x_1, x_2, \dots, x_n)$ от корней данного алгебраического уравнения над полем $\mathbf{C}$:

а) $f(x_1, x_2, x_3) = S(x_1^3 x_2), x^3 - x^2 - 4x + 1 = 0$;

б) $f(x_1, x_2, x_3, x_4) = S(x_1^3 x_2 x_3), x^4 + x^3 - 2x^2 - 3x + 1 = 0$.

4. а) Найдите многочлен третьей степени, корнями которого являются кубы корней многочлена $x^3 - x - 1 \in \mathbf{C}[x]$.

б) Найдите многочлен четвертой степени, корнями которого являются квадраты корней многочлена $x^4 + 2x^3 - x + 3 \in \mathbf{C}[x]$.

5. Решите систему уравнений (над полем $\mathbf{R}$):

а)
$$\begin{cases} x_1^2 + x_2^2 + x_3^2 = 6, \\ x_1^3 + x_2^3 + x_3^3 - x_1 x_2 x_3 = -4, \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = -3; \end{cases}$$

б)
$$\begin{cases} x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 + x_2 + x_3 = -3, \\ x_1^2 + x_2^2 + x_3^2 - 4(x_1 + x_2 + x_3) = 5, \\ x_1^2(x_2 + x_3) + x_2^2(x_1 + x_3) + x_3^2(x_1 + x_2) = 8. \end{cases}$$

§ 3. СИСТЕМЫ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

С различного рода уравнениями и системами уравнений мы сталкиваемся почти во всех областях науки и техники, используя математический аппарат. В данном пособии рассматриваются только алгебраические уравнения и системы алгебраических уравнений, причем основное внимание уделяется алгебраическим методам их решения. Нужно отметить, что эти методы имеют скорее теоретическое, чем прикладное значение. Что касается практических методов решения уравнений (в том числе и алгебраических), то они рассматриваются в курсах приближенных вычислений.

1. **Метод последовательного исключения неизвестных.** Пусть P — произвольное поле.

Системой алгебраических уравнений над полем P называется система уравнений вида

$$f_i(x_1, x_2, \dots, x_n) = 0 \quad (i = 1, 2, \dots, m), \quad (1)$$

где $f_1, f_2, \dots, f_m$ — многочлены с коэффициентами из поля P . Простейшие типы систем алгебраических уравнений — это алгебраические уравнения произвольной степени с одним неизвестным и системы линейных уравнений.

Аналогично тому как это делается в случае систем линейных уравнений, решение системы алгебраических уравнений произвольной степени путем последовательного исключения неизвестных может быть сведено к решению уравнений с одним неизвестным.

Покажем, как производится исключение неизвестного в системе двух алгебраических уравнений с двумя неизвестными:

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0, \end{cases} \quad (f, g \in P[x, y]). \quad (2)$$

Представим левые части уравнений данной системы в виде многочленов от x с коэффициентами из кольца $K = P[y]$:

$$\begin{aligned} f(x, y) &= F(x) = a_0(y)x^n + a_1(y)x^{n-1} + \dots + a_n(y), \\ g(x, y) &= G(x) = b_0(y)x^m + b_1(y)x^{m-1} + \dots + b_m(y), \end{aligned}$$

причем будем считать, что a_0 и b_0 — ненулевые многочлены от y . Пусть для определенности $n \geq m$. Если многочлен $F(x)$ домножить на b_0^{n-m+1} , то его можно будет разделить с остатком на $G(x)$ в кольце $K[x]$ (см. п. 1 § 3 гл. II), т. е. найдутся такие многочлены $Q(x)$, $R(x) \in K[x]$, что

$$b_0^{n-m+1} F(x) = Q(x) G(x) + R(x), \quad (3)$$

причем ст. $R(x) < \text{ст. } G(x)$. Равенство (3) можно рассматривать как соотношение в кольце $P[x, y]$:

$$b_0(y)^{n-m+1} f(x, y) = q(x, y) g(x, y) + r(x, y), \quad (4)$$

где

$$q(x, y) = Q(x), \quad r(x, y) = R(x).$$

Умножим теперь первое уравнение системы (2) на $b_0(y)^{n-m+1}$ и вычтем из него второе уравнение, умноженное на $q(x, y)$. Мы получим уравнение

$$r(x, y) = 0, \quad (5)$$

являющееся следствием системы (2).

При условии, что значение неизвестного y не обращает в нуль многочлен $b_0(y)$, исходная система уравнений (2) эквивалентна системе, которая получается из нее заменой первого уравнения уравнением (5). Однако среди решений системы (2) могут быть и такие, которые обращают в нуль многочлен $b_0(y)$. Эти решения совпадают с решениями системы, которая получается из системы (2) добавлением уравнения

$$b_0(y) = 0$$

и заменой второго уравнения уравнением

$$\tilde{g}(x, y) = 0,$$

где

$$\tilde{g}(x, y) = b_1(y)x^{m-1} + \dots + b_m(y).$$

Таким образом, множество решений системы (2) есть объединение множеств решений следующих двух систем уравнений:

$$\text{I} \begin{cases} r(x, y) = 0, \\ g(x, y) = 0, \\ b_0(y) \neq 0; \end{cases} \quad \text{II} \begin{cases} f(x, y) = 0, \\ \tilde{g}(x, y) = 0, \\ b_0(y) = 0. \end{cases}$$

(Первая из этих систем наряду с уравнениями содержит неравенство $b_0(y) \neq 0$). Каждая из систем I и II проще исходной системы уравнений в том смысле, что сумма степеней всех ее уравнений по x меньше, чем у системы (2).

Применяя описанную выше процедуру к первым двум уравнениям каждой из систем I и II, а затем к уравнениям каждой из вновь получившихся систем и т. д. до тех пор, пока это возможно, мы в конце концов придем к ряду систем уравнений и неравенств, в каждой из которых лишь одно уравнение содержит неизвестное x . В самом деле, если бы в какой-то из получившихся систем было два уравнения, содержащих x , то к этой системе можно было бы еще раз применить указанную выше процедуру. Итак, каждая из получившихся систем уравнений и неравенств имеет вид

$$\begin{aligned} h(x, y) &= 0, \\ p_i(y) &= 0 \quad (i = 1, 2, \dots, k), \\ q_j(y) &\neq 0 \quad (j = 1, 2, \dots, l). \end{aligned} \quad (6)$$

Для решения системы (6) нужно, очевидно, найти общие корни многочленов $p_1, p_2, \dots, p_k$, выбрать из них те, которые не являются корнями ни одного из многочленов $q_1, q_2, \dots, q_l$, а затем каждый из оставшихся корней подставить в первое уравнение и решить полученное уравнение относительно x .

Таким образом, решение каждой из получившихся систем вида (6) сводится к последовательному решению алгебраических уравнений с одним неизвестным. Множество решений исходной системы (2) есть объединение множеств решений всех этих систем.

Пример 1. Решим систему уравнений (над полем $\mathbf{R}$):

$$\begin{cases} 2x^3 - 2xy^2 + y^3 - 2x^2 - 2x - y = 0, \\ x^2 + xy - y^2 + y = 0. \end{cases}$$

Левые части уравнений представим как многочлены от x с коэффициентами из кольца $\mathbf{R}[y]$:

$$\begin{aligned} F(x) &= 2x^3 - 2x^2 - 2(y^2 + 1)x + (y^3 - y), \\ G(x) &= x^2 + xy - (y^2 - y). \end{aligned}$$

Так как старший коэффициент многочлена $G(x)$ равен единице, то $F(x)$ можно разделить с остатком на $G(x)$ в кольце многочленов над $\mathbf{R}[y]$. Выполнив это деление, найдем, что остаток равен

$$(2y^2 - 2)x - (y^3 - y) = (y^2 - 1)(2x - y).$$

Следовательно, исходная система уравнений эквивалентна системе

$$\begin{cases} (y^2 - 1)(2x - y) = 0, \\ x^2 + xy - (y^2 - y) = 0. \end{cases}$$

Множество решений этой системы уравнений есть объединение множеств решений следующих двух систем:

$$\begin{cases} x^2 + xy - y^2 + y = 0, \\ y^2 - 1 = 0; \end{cases} \quad \begin{cases} 2x - y = 0, \\ x^2 + xy - y^2 + y = 0. \end{cases}$$

Первая из них имеет следующие 4 решения: $(0; 1)$, $(-1; 1)$, $(2; -1)$, $(-1; -1)$. Для решения второй системы можно было бы исключить неизвестное x , разделив с остатком левую часть второго уравнения на левую часть первого уравнения (как многочлены от x). Однако в данном случае проще выразить y через x из первого уравнения и подставить это выражение во второе уравнение. Таким образом найдем еще 2 решения исходной системы уравнений: $(0; 0)$, $(2; 4)$.

Пример 2. Решим систему уравнений:

$$\begin{cases} 2xy^3 - x^2y + y + 5 = 0, \\ x^2y^2 + 2x^2y - 5x + 1 = 0. \end{cases}$$

Представим левые части уравнений как многочлены от x :

$$F(x) = -yx^2 + 2y^3x + (y + 5),$$

$$G(x) = (y^2 + 2y)x^2 - 5x + 1.$$

При делении $G(x)$ на $F(x)$ получается остаток

$$R(x) = (2y^4 + 4y^3 - 5)x + (y^2 + 7y + 11).$$

Исходная система уравнений эквивалентна системе

$$\begin{cases} F(x) = 0, \\ R(x) = 0. \end{cases}$$

(Здесь $F(x)$ и $R(x)$ следует понимать как многочлены от x и y .) Домножим $F(x)$ на $(2y^4 + 4y^3 - 5)^2$ и разделим с остатком на $R(x)$. В результате получится остаток

$$R_1 = -(4y^7 + 8y^6 + 11y^5 + 84y^4 + 161y^3 + 154y^2 + 96y - 125).$$

Следовательно, множество решений исходной системы уравнений есть объединение множеств решений двух систем

$$\text{I} \begin{cases} R(x) = 0, \\ R_1 = 0, \\ 2y^4 + 4y^3 - 5 \neq 0; \end{cases} \quad \text{II} \begin{cases} F(x) = 0, \\ y^2 + 7y + 11 = 0, \\ 2y^4 + 4y^3 - 5 = 0 \end{cases}$$

С помощью алгоритма Евклида можно убедиться, что многочлены $y^2 + 7y + 11$ и $2y^4 + 4y^3 - 5$ взаимно просты и, значит, не имеют общих корней. Следовательно, система II не имеет решений. Что

касается системы I, то для ее решения необходимо решить уравнение $R_1 = 0$ относительно y . Мы не будем этим заниматься. Отметим только, что многочлены R_1 и $2y^4 + 4y^3 - 5$ взаимно просты и поэтому каждому решению уравнения $R_1 = 0$ отвечает ровно одно решение исходной системы. (При каждом найденном из уравнения $R_1 = 0$ значении y значение x будет однозначно определяться из первого уравнения системы 1, линейного по x .)

Аналогичный метод может быть применен к системе из произвольного числа алгебраических уравнений с любым числом неизвестных. Если система имеет конечное число решений, то все они могут быть найдены этим способом (при условии, что мы умеем решать алгебраические уравнения с одним неизвестным).

В том случае, когда система алгебраических уравнений имеет бесконечно много решений, можно ставить вопрос о нахождении «общего решения» в виде набора многочленов (или рациональных функций) от некоторого числа параметров, дающего все решения системы при подстановке в него всевозможных наборов значений параметров. Такое общее решение, как известно из линейной алгебры, допускает любая система линейных уравнений. Однако для произвольной системы алгебраических уравнений общего решения, вообще говоря, не существует. Вопросы, связанные с описанием многообразий решений произвольных систем алгебраических уравнений (так называемых алгебраических многообразий), весьма сложны. Ими занимается раздел математики, называемый алгебраической геометрией.

2. Исключение неизвестного при помощи результата. Если воспользоваться теоремой 5 § 1 гл. II, то исключение неизвестного из системы алгебраических уравнений можно провести другим способом.

Покажем, как это может быть сделано для системы двух алгебраических уравнений с двумя неизвестными x, y . Если представить левые части уравнений системы в виде многочленов от x с коэффициентами из кольца $P[y]$, то система запишется в виде

$$\begin{cases} F(x) = a_0(y)x^n + a_1(y)x^{n-1} + \dots + a_n(y) = 0, \\ G(x) = b_0(y)x^m + b_1(y)x^{m-1} + \dots + b_m(y) = 0. \end{cases} \quad (7)$$

Положим $y = y_0 \in P$. Тогда левые части уравнений станут многочленами от x с коэффициентами из P . Согласно теореме 5 § 1 гл. II и замечанию к ней эти многочлены могут иметь общий корень только в том случае, когда их результат (вычисленный как для многочленов степеней n и m) равен нулю. Следовательно, если существует решение (x_0, y_0) системы (7), то y_0 — корень многочлена

$$R(F, G) = \left| \begin{array}{cccc} a_0(y) & a_1(y) & \dots & a_n(y) \\ & a_0(y) & a_1(y) & \dots & a_n(y) \\ & & \ddots & \ddots & \ddots \\ & & & a_0(y) & a_1(y) & \dots & a_n(y) \\ b_0(y) & b_1(y) & \dots & b_m(y) \\ & b_0(y) & b_1(y) & \dots & b_m(y) \\ & & \ddots & \ddots & \ddots \\ & & & b_0(y) & b_1(y) & \dots & b_m(y) \end{array} \right| \left. \begin{array}{l} m \text{ строк} \\ \\ \\ n \text{ строк} \end{array} \right\} \quad (8)$$

Таким образом, решение системы (7) сводится к решению одного алгебраического уравнения $R(F, G) = 0$ относительно неизвестного u и затем, для каждого решения u_0 этого уравнения, к совместному решению двух алгебраических уравнений с одним неизвестным, которые получаются из уравнений (7) подстановкой $u = u_0$.

Пример 3. При помощи результата исключим неизвестное из системы уравнений примера 2.

По формуле (8) находим:

$$R(F, G) = \begin{vmatrix} -y & 2y^3 & y+5 & 0 \\ 0 & -y & 2y^3 & y+5 \\ y^2+2y & -5 & 1 & 0 \\ 0 & y^2+2y & -5 & 1 \end{vmatrix} =$$

$$= y(4y^7 + 8y^6 + 11y^5 + 84y^4 + 161y^3 + 154y^2 + 96y - 125).$$

Одним из корней уравнения $R(F, G) = 0$ является 0; однако при подстановке его в исходную систему получается противоречивое равенство $5 = 0$, так что этому корню не соответствует никакого решения системы. Следовательно, всевозможные значения u удовлетворяют уравнению

$$4y^7 + 8y^6 + 11y^5 + 84y^4 + 161y^3 + 154y^2 + 96y - 125 = 0.$$

Таким образом, мы приходим к тому же результату, что и при решении примера 2.

Ситуация, с которой мы встретились при решении последнего примера, является типичной в том смысле, что решение системы алгебраических уравнений обычно сводится к решению алгебраических уравнений с одним неизвестным, но значительно более высокой степени, чем степени уравнений исходной системы. Ввиду этого способ решения систем алгебраических уравнений, основанный на исключении неизвестных, оказывается практически менее удобным, чем некоторые методы, используемые с одинаковым успехом для решения систем как алгебраических, так и трансцендентных уравнений.

Вопросы для самопроверки

1. Что такое система алгебраических уравнений?
2. Как исключается неизвестное из системы двух алгебраических уравнений с двумя неизвестными? Почему в процессе исключения появляются не только новые уравнения, но и неравенства?
3. Как можно исключить неизвестное из системы двух алгебраических уравнений с двумя неизвестными с помощью результата? Что получится, если применить этот метод к системе двух линейных уравнений с двумя неизвестными?

Упражнения

1. Методом, описанным в п. 1, исключите x из системы уравнений (над R):

$$\text{а) } \begin{cases} x^2 - xy + y^2 = 3, \\ x^2y + xy^2 = 6; \end{cases} \quad \text{б) } \begin{cases} x^3 - xy - y^3 + y = 0, \\ x^2 + x - y^2 - 1 = 0; \end{cases}$$

$$\text{в) } \begin{cases} y = x^3 - 2x^2 - 6x + 8, \\ y = 2x^3 - 8x^2 + 5x + 2. \end{cases}$$

2. Выполните упражнение 1 а) и б) при помощи результата.

3. Решите систему уравнений над полем C :

$$\text{а) } \begin{cases} 5y^2 - 6xy + 5x^2 - 16 = 0, \\ y^2 - xy + 2x^2 - y - x - 4 = 0; \end{cases}$$

$$\text{б) } \begin{cases} y^2 + (x - 4)y + x^2 - 2x + 3 = 0, \\ y^3 - 5y^2 + (x + 7)y + x^3 - x^2 - 5x - 3 = 0. \end{cases}$$

МНОГОЧЛЕНЫ НАД ПОЛЯМИ $\mathbb{C}$ И $\mathbb{R}$. АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ С КОМПЛЕКСНЫМИ И ДЕЙСТВИТЕЛЬНЫМИ КОЭФФИЦИЕНТАМИ

В предыдущих главах мы, как правило, рассматривали многочлены с коэффициентами из произвольного поля P или даже из произвольной области целостности. Лишь в нескольких местах нам пришлось наложить некоторые ограничения на поле P : например, в пп. 6—8 § 2 гл. II мы требовали, чтобы это поле имело нулевую характеристику. Свойства кольца $P[x]$ для конкретного поля P могут оказаться значительно богаче. В настоящей главе мы остановимся более подробно на двух случаях: $P = \mathbb{C}$ (поле комплексных чисел) и $P = \mathbb{R}$ (поле действительных чисел). Большинство приложений относится именно к этим случаям.

Главный вопрос, который нас теперь будет интересовать, — это вопрос о корнях многочленов, или, что то же самое, о корнях соответствующих алгебраических уравнений. Напомним, что *алгебраическим уравнением* (с одним неизвестным) *степени n* называется уравнение вида

$$f(x) = 0, \quad (1)$$

где $f(x)$ — многочлен степени n с коэффициентами из некоторого поля P . Решение уравнения (1) — это элемент x_0 поля P , удовлетворяющий условию $f(x_0) = 0$, т. е. корень многочлена $f(x)$. Поскольку слово «решение» может означать также процесс отыскания решений, то во избежание двусмысленности мы будем называть решения уравнения (1) его *корнями*.

Иногда говорят о корнях (решениях) уравнения (1), лежащих в каком-либо заданном расширении L поля P , например о комплексных корнях уравнения с действительными коэффициентами. Это следует понимать в том смысле, что многочлен $f(x)$ рассматривается как элемент кольца $L[x]$ (см. п. 7 § 1 гл. I).

Свойства алгебраических уравнений с коэффициентами из поля P тесно связаны со свойствами кольца $P[x]$ и существенно зависят от поля P . Как уже было сказано выше, эта глава будет посвящена случаям $P = \mathbb{C}$ и $P = \mathbb{R}$. В следующей главе мы рассмотрим случай $P = \mathbb{Q}$.

§ 1. КОМПЛЕКСНЫЕ ЧИСЛА

В одной из предыдущих глав курса было построено поле комплексных чисел. Напомним, что всякое комплексное число c единственным образом представляется в виде $a + bi$, где a, b — действительные числа.

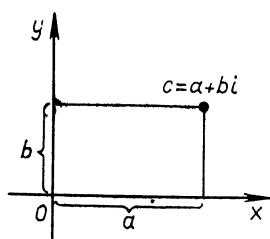


Рис. 3

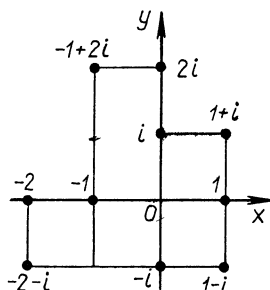


Рис. 4

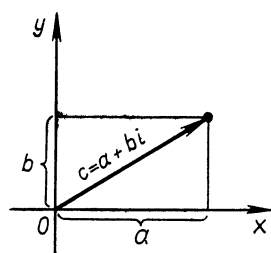


Рис. 5

тельные числа, а i — «мнимая единица», обладающая тем свойством, что $i^2 = -1$. Число a называется действительной, а bi — мнимой частью числа c . Они обозначаются через $\operatorname{Re} c$ и $\operatorname{Im} c$ соответственно.

Поле действительных чисел является подполем поля комплексных чисел (комплексное число $a + bi$ действительно, если $b = 0$), или, что то же самое, поле комплексных чисел является расширением поля действительных чисел. Комплексное число, не являющееся действительным, называется мнимым.

1. Геометрическое изображение комплексных чисел. Рассмотрим плоскость с декартовой системой координат (рис. 3). Сопоставим комплексному числу $c = a + bi$ ($a, b \in \mathbf{R}$) точку плоскости с координатами a, b . Мы будем говорить, что эта точка *изображает* число c . Очевидно, что каждая точка плоскости изображает единственное комплексное число. В частности, точки оси абсцисс изображают действительные числа, точки оси ординат — чисто мнимые числа, т. е. числа вида bi ($b \in \mathbf{R}$). На рисунке 4 показаны изображения нескольких комплексных чисел.

Комплексному числу $c = a + bi$ можно сопоставить также вектор плоскости с координатами a, b , который можно представлять в виде направленного отрезка, соединяющего начало координат с точкой, изображающей число c (рис. 5).

При изображении комплексных чисел с помощью векторов сложению комплексных чисел соответствует сложение векторов. В самом деле, пусть

$$c_1 = a_1 + b_1 i, c_2 = a_2 + b_2 i \quad (a_1, b_1, a_2, b_2 \in \mathbf{R});$$

тогда $c_1 + c_2 = (a_1 + a_2) + (b_1 + b_2)i$. Числу c_1 сопоставляется вектор с координатами a_1, b_1 , числу c_2 — вектор с координатами a_2, b_2 . При сложении векторов их соответствующие координаты складываются.

Следовательно, сумма векторов, сопоставленных числам c_1 и c_2 , имеет координаты $a_1 + a_2, b_1 + b_2$ и совпадает с вектором, сопоставленным числу $c_1 + c_2$ (рис. 6).

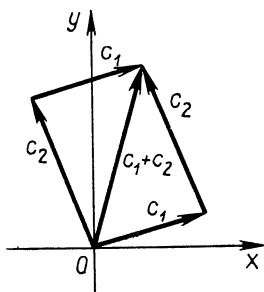


Рис. 6

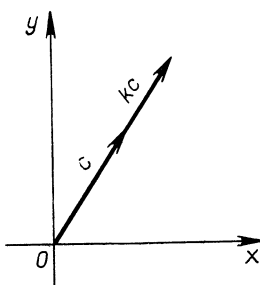


Рис. 7

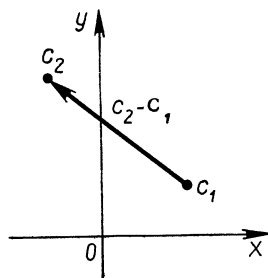


Рис. 8

Аналогично доказывается, что умножению комплексного числа c на действительное число k соответствует умножение вектора на число k (рис. 7).

Вектор, соединяющий точки, изображающие комплексные числа c_1 и c_2 , является изображением числа $c_2 - c_1$ (рис. 8). В самом деле, координаты этого вектора равны $a_2 - a_1$, $b_2 - b_1$; с другой стороны,

$$c_2 - c_1 = (a_2 - a_1) + (b_2 - b_1)i,$$

так что число $c_2 - c_1$ изображается как раз вектором с координатами $a_2 - a_1$, $b_2 - b_1$.

Исходя из этих основных свойств, можно интерпретировать некоторые геометрические построения в терминах операций над комплексными числами. Для краткости мы будем в дальнейшем говорить о «точке c » или «векторе c », понимая под этим точку или вектор, изображающие комплексное число c .

Пример 1. Докажем, что точка $\frac{1}{2}(c_1 + c_2)$ есть середина отрезка, соединяющего точки c_1 и c_2 .

Построим параллелограмм на радиус-векторах точек c_1 и c_2 (рис. 9). Середина отрезка, соединяющего точки c_1 и c_2 , есть в то же время середина другой диагонали этого параллелограмма и, значит, совпадает с точкой $\frac{1}{2}(c_1 + c_2)$, что и требовалось доказать.

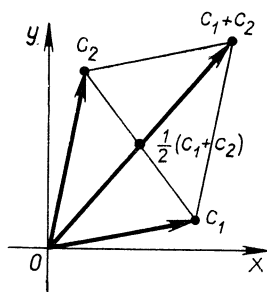


Рис. 9

2. Тригонометрическая форма комплексных чисел. Точка плоскости, отличная от начала координат, может быть задана своими полярными координатами r , φ , где r — расстояние от данной точки до начала координат, φ — угол между положительной полуосью абсцисс и радиус-вектором данной точки, отсчитываемый против часовой стрелки (угол φ определен с точностью до прибавления целого кратного 2π).

Полярные координаты r , φ точки, изоб-

ражающей комплексное число $c \neq 0$, называются *модулем* и *аргументом* числа c и обозначаются через $|c|$ и $\arg c$ соответственно:

$$r = |c|, \quad \varphi = \arg c.$$

Если изображать число c вектором, то $|c|$ будет длиной этого вектора, а $\arg c$ — углом, который он образует с положительной полуосью абсцисс. На рисунке 10 изображено несколько комплексных чисел с указанием их модулей и аргументов. Модуль числа 0 считается равным 0, аргумент этого числа не определен.

С помощью геометрической интерпретации сложения комплексных чисел как сложения векторов (см. рис. 6) доказывается неравенство

$$|c_1 + c_2| \leq |c_1| + |c_2| \quad (c_1, c_2 \in \mathbb{C}).$$

В самом деле, $|c_1|$, $|c_2|$ и $|c_1 + c_2|$ — длины сторон треугольника (быть может, вырожденного), так что рассматриваемое неравенство — это просто теорема о том, что длина стороны треугольника не превосходит суммы длин двух других его сторон. Заменяя в этом неравенстве c_1 на $c_1 - c_2$, мы можем получить неравенство

$$|c_1 - c_2| \geq |c_1| - |c_2| \quad (c_1, c_2 \in \mathbb{C}).$$

Наконец, заменяя в последнем неравенстве c_2 на $-c_2$, получаем неравенство

$$|c_1 + c_2| \geq |c_1| - |c_2| \quad (c_1, c_2 \in \mathbb{C}).$$

Рассмотрим какое-либо комплексное число $c = a + bi$ ($a, b \in \mathbb{R}$), отличное от нуля; обозначим через r и φ его модуль и аргумент соответственно. Тогда a и b — декартовы координаты точки, изображающей число c , а r и φ — ее полярные координаты. Согласно формулам перехода от декартовых координат к полярным и обратно, имеем:

$$r = \sqrt{a^2 + b^2}, \quad \operatorname{tg} \varphi = \frac{b}{a} \quad (1)$$

и, с другой стороны,

$$a = r \cos \varphi, \quad b = r \sin \varphi \quad (2)$$

(рис. 11),

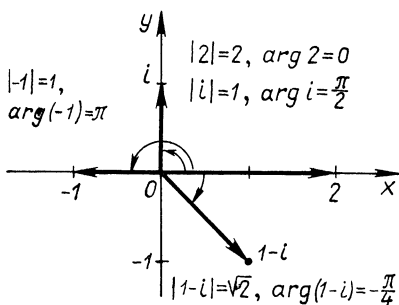


Рис. 10

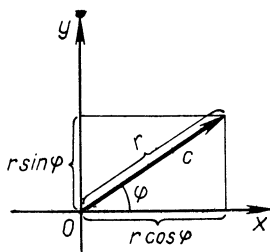


Рис. 11

Формулы (1) позволяют найти модуль и тангенс аргумента комплексного числа, заданного в виде $a + bi$. Для определения аргумента по его тангенсу достаточно знать, в какой координатной четверти находится точка, изображающая данное число, что устанавливается по знакам a и b .

Пример 2. Найдем модуль и аргумент числа $c = -1 + i\sqrt{3}$. В данном случае

$$a = -1, b = \sqrt{3}, r = \sqrt{1+3} = 2, \operatorname{tg} \varphi = -\sqrt{3},$$

откуда следует, что $\varphi = -\frac{\pi}{3}$ или $\frac{2\pi}{3}$ (с точностью до прибавления целого кратного 2π), но так как точка $-1 + i\sqrt{3}$ находится во второй четверти ($a < 0, b > 0$), то $\varphi = \frac{2\pi}{3}$.

Исходя из формул (2), получаем, что

$$c = r(\cos \varphi + i \sin \varphi). \quad (3)$$

Представление комплексного числа c в виде $r(\cos \varphi + i \sin \varphi)$, где r, φ — действительные числа, причем $r > 0$, называется *тригонометрической формой* числа c . Из предыдущего следует, что всякое комплексное число, отличное от нуля, представляется в тригонометрической форме, если в качестве r взять его модуль, а в качестве φ — аргумент. Так, число $-1 + i\sqrt{3}$ представляется в виде $2\left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right)$ (см. пример 2).

Покажем, что если равенство (3) выполняется для каких-то действительных чисел r, φ , причем $r > 0$, то r неизбежно является модулем, а φ — аргументом числа c . Для этого рассмотрим точку плоскости с полярными координатами r, φ . Она изображает комплексное число, модуль которого равен r , а аргумент равен φ и которое, по предыдущему, равно $r(\cos \varphi + i \sin \varphi)$, т. е. c . Следовательно, r есть модуль, а φ — аргумент числа c , что и требовалось доказать.

Так как модуль комплексного числа определен однозначно, а аргумент — с точностью до прибавления целого кратного 2π , то из доказанного выше следует единственность тригонометрической формы комплексного числа, понимаемая в следующем смысле: если

$$r_1(\cos \varphi_1 + i \sin \varphi_1) = r_2(\cos \varphi_2 + i \sin \varphi_2),$$

причем $r_1 > 0, r_2 > 0$, то $r_1 = r_2$ и $\varphi_1 \equiv \varphi_2 \pmod{2\pi}$. (Последнее сравнение означает, что $\varphi_1 - \varphi_2 = 2k\pi$, где $k \in \mathbb{Z}$.)

Пример 3. Запишем в тригонометрической форме число $c = -3 - 4i$.

Имеем:

$$a = -3, b = -4, r = \sqrt{3^2 + 4^2} = 5, \operatorname{tg} \varphi = \frac{4}{3}.$$

Так как точка c находится в третьей четверти, то

$$\varphi = \operatorname{arctg} \frac{4}{3} + \pi. \quad (4)$$

Таким образом,

$$-3 - 4i = 5 (\cos \varphi + i \sin \varphi),$$

где угол φ определяется по формуле (4).

3. Умножение комплексных чисел в тригонометрической форме. Тригонометрическая форма хорошо приспособлена для умножения комплексных чисел и как следствие этого — для деления, возведения в степень и извлечения корня.

Рассмотрим два комплексных числа, записанных в тригонометрической форме:

$$c_1 = r_1 (\cos \varphi_1 + i \sin \varphi_1), \quad (5)$$

$$c_2 = r_2 (\cos \varphi_2 + i \sin \varphi_2). \quad (6)$$

Вычислим их произведение:

$$c_1 c_2 = r_1 r_2 ((\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i (\cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2)).$$

Воспользовавшись формулами для косинуса и синуса суммы двух углов, полученное выражение можно переписать следующим образом:

$$c_1 c_2 = r_1 r_2 (\cos (\varphi_1 + \varphi_2) + i \sin (\varphi_1 + \varphi_2)). \quad (7)$$

Тем самым произведение $c_1 c_2$ представлено в тригонометрической форме, причем его модуль равен $r_1 r_2$, а аргумент равен $\varphi_1 + \varphi_2$.

Таким образом, *модуль произведения двух комплексных чисел равен произведению их модулей, а аргумент произведения равен сумме аргументов*, например:

$$\begin{aligned} & 2 \left(\cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5} \right) 3 \left(\cos \frac{4\pi}{15} + i \sin \frac{4\pi}{15} \right) = \\ & = 6 \left(\cos \left(\frac{2\pi}{5} + \frac{4\pi}{15} \right) + i \sin \left(\frac{2\pi}{5} + \frac{4\pi}{15} \right) \right) = 6 \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \right) = \\ & = 3 (-1 + i \sqrt{3}). \end{aligned}$$

Из этого правила у м н о ж е н и я комплексных чисел в тригонометрической форме вытекает следующее правило д е л е н и я: *модуль отношения двух комплексных чисел равен отношению их модулей, а аргумент отношения равен разности аргументов*. В самом деле, пусть числа c_1 и c_2 заданы формулами (5) и (6) соответственно и пусть c — комплексное число с модулем $\frac{r_1}{r_2}$ и аргументом $\varphi_1 - \varphi_2$. Тогда число $c_2 c$ имеет модуль $r_2 \cdot \frac{r_1}{r_2} = r_1$ и аргумент $\varphi_2 + (\varphi_1 - \varphi_2) = \varphi_1$. Стало быть, $c_2 c = c_1$, т. е. $\frac{c_1}{c_2} = c$, что и требовалось доказать.

Например,

$$\frac{-1 + i\sqrt{3}}{1 + i} = \frac{2\left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right)}{\sqrt{2}\left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}\right)} = \sqrt{2}\left(\cos \frac{5\pi}{12} + i \sin \frac{5\pi}{12}\right).$$

Комплексные числа, модуль которых равен 1, представляются в виде $\cos \varphi + i \sin \varphi$. Их произведение также имеет модуль 1 и вычисляется по формуле

$$(\cos \varphi_1 + i \sin \varphi_1)(\cos \varphi_2 + i \sin \varphi_2) = \cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2). \quad (8)$$

Совокупность T всех комплексных чисел, модуль которых равен 1, является подгруппой мультипликативной группы комплексных чисел, отличных от нуля. В самом деле, только что мы отметили, что эта совокупность замкнута относительно умножения. Кроме того, ясно, что $1 \in T$ и что если $c \in T$, то и $c^{-1} \in T$: точнее,

$$(\cos \varphi + i \sin \varphi)^{-1} = \cos(-\varphi) + i \sin(-\varphi). \quad (9)$$

Геометрически подгруппа T изображается окружностью радиуса 1 с центром в начале координат.

С точки зрения теории групп возможность и единственность представления в тригонометрической форме всякого комплексного числа, отличного от нуля, означает, что мультипликативная группа всех комплексных чисел, отличных от нуля, разлагается в прямое произведение подгруппы T , описанной выше, и подгруппы положительных чисел.

Что касается строения группы T , то формула (8) означает, что отображение $\varphi \rightarrow \cos \varphi + i \sin \varphi$ является гомоморфизмом аддитивной группы действительных чисел на группу T . Ядро этого гомоморфизма есть подгруппа $2\pi\mathbb{Z}$, состоящая из чисел вида $2k\pi$, где $k \in \mathbb{Z}$. Следовательно, группа T изоморфна фактор-группе $\mathbb{R}/2\pi\mathbb{Z}$ (которая, как легко видеть, изоморфна фактор-группе $\mathbb{R}/\mathbb{Z}$).

Правило умножения комплексных чисел в тригонометрической форме допускает следующую геометрическую интерпретацию: *при умножении какого-либо комплексного числа z на число $c = r(\cos \varphi + i \sin \varphi)$ вектор, изображающий число z , растягивается в r раз и поворачивается на угол φ* . В самом деле, при умножении на c модуль числа z умножается на r , а к его аргументу прибавляется φ .

В частности, умножение на $\cos \varphi + i \sin \varphi$ равносильно повороту на угол φ (рис. 12). Например, умножение на $i = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$ равносильно повороту на $\frac{\pi}{2}$.

Пример 4. Две вершины равно-
стороннего треугольника находятся в точ-

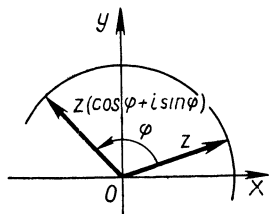


Рис. 12

ках 1 и $-1 + 2i$. Найдем его третью вершину.

Вектор, соединяющий точку 1 с точкой $-1 + 2i$, изображает комплексное число $(-1 + 2i) - 1 = -2 + 2i$. Вектор, соединяющий точку 1 с третьей вершиной треугольника, получается из него поворотом на $\frac{\pi}{3}$ в ту или другую сторону (рис. 13), т. е. умножением на

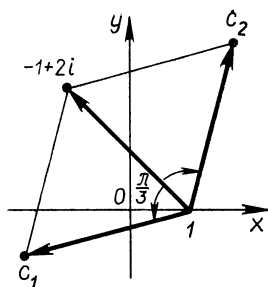


Рис. 13

$$\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} = \frac{1}{2} + \frac{i\sqrt{3}}{2}$$

или на

$$\cos \left(-\frac{\pi}{3}\right) + i \sin \left(-\frac{\pi}{3}\right) = \frac{1}{2} - \frac{i\sqrt{3}}{2}.$$

Обозначая искомую вершину через c , имеем:

$$c - 1 = \left(\frac{1}{2} \pm \frac{i\sqrt{3}}{2}\right)(-2 + 2i),$$

откуда находим два возможных значения c :

$$c_1 = 1 + \left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)(-2 + 2i) = -\sqrt{3} + (1 - \sqrt{3})i,$$

$$c_2 = 1 + \left(\frac{1}{2} - \frac{i\sqrt{3}}{2}\right)(-2 + 2i) = \sqrt{3} + (1 + \sqrt{3})i.$$

4. Возведение в степень. Правило умножения комплексных чисел в тригонометрической форме, найденное в п. 3, очевидным образом переносится на любое число множителей. А именно модуль произведения нескольких комплексных чисел равен произведению их модулей, а аргумент произведения равен сумме их аргументов. В частности, взяв n одинаковых множителей, получим следующую формулу, называемую *формулой Муавра*:

$$(r(\cos \varphi + i \sin \varphi))^n = r^n (\cos n\varphi + i \sin n\varphi).$$

Пример 5. Вычислим $(-1 + i\sqrt{3})^7$.

Имеем:

$$\begin{aligned} (-1 + i\sqrt{3})^7 &= \left(2 \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right)\right)^7 = 2^7 \left(\cos \frac{14\pi}{3} + i \sin \frac{14\pi}{3}\right) = \\ &= 128 \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right) = 64 (-1 + i\sqrt{3}). \end{aligned}$$

При $r = 1$ формула Муавра принимает особенно простой вид:

$$(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi.$$

Эта формула позволяет выразить $\cos n\varphi$ и $\sin n\varphi$ через $\cos \varphi$ и $\sin \varphi$. Для этого нужно вычислить $(\cos \varphi + i \sin \varphi)^n$ другим

способом, пользуясь формулой бинома Ньютона. Действительная часть полученного выражения будет равна $\cos n\varphi$, а мнимая — $\sin n\varphi$. В результате получим:

$$\begin{aligned}\cos n\varphi &= \cos^n \varphi - C_n^2 \cos^{n-2} \varphi \cdot \sin^2 \varphi + C_n^4 \cos^{n-4} \varphi \cdot \sin^4 \varphi - \dots \\ \sin n\varphi &= n \cos^{n-1} \varphi \cdot \sin \varphi - C_n^3 \cos^{n-3} \varphi \cdot \sin^3 \varphi + \\ &+ C_n^5 \cos^{n-5} \varphi \cdot \sin^5 \varphi - \dots\end{aligned}$$

Например,

$$\begin{aligned}\cos 4\varphi &= \cos^4 \varphi - 6 \cos^2 \varphi \cdot \sin^2 \varphi + \sin^4 \varphi, \\ \sin 4\varphi &= 4 \cos^3 \varphi \cdot \sin \varphi - 4 \cos \varphi \cdot \sin^3 \varphi.\end{aligned}$$

5. Извлечение корня. Рассмотрим задачу об извлечении корня n -й степени из комплексного числа $c = r(\cos \varphi + i \sin \varphi)$, т. е. о нахождении всех таких комплексных чисел z , что

$$z^n = c. \quad (10)$$

Пусть z — некоторое комплексное число, представленное следующим образом в тригонометрической форме:

$$z = s(\cos \psi + i \sin \psi) \quad (s > 0).$$

По формуле Муавра,

$$z^n = s^n (\cos n\psi + i \sin n\psi).$$

Равенство (10) будет выполняться тогда и только тогда, когда

$$s^n = r, \quad n\psi \equiv \varphi \pmod{2\pi}$$

(см. п. 2). Эти условия означают, что $s = \sqrt[n]{r}$ (арифметическое значение корня),

$$\psi = \frac{\varphi + 2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Таким образом, получается следующая общая формула для корней n -й степени из c :

$$z_k = \sqrt[n]{r} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right), \quad (11)$$

где k может быть любым целым числом. Однако не все числа z_k , получаемые по этой формуле, различны. А именно при $k_1 \equiv k_2 \pmod{n}$ аргументы чисел z_{k_1} и z_{k_2} отличаются на целое кратное 2π и, следовательно, $z_{k_1} = z_{k_2}$. С другой стороны, при $k_1 \not\equiv k_2 \pmod{n}$ разность аргументов чисел z_{k_1} и z_{k_2} , равная $\frac{2(k_1 - k_2)\pi}{n}$, не будет целым кратным 2π и, значит, $z_{k_1} \neq z_{k_2}$. Таким образом, различных корней будет ровно n . Они могут быть получены, например, при следующих значениях k :

$$k = 0, 1, 2, \dots, n-1. \quad (12)$$

Пример 6. Найдем все корни 5-й степени из $-1 + i\sqrt{3}$. Так как $-1 + i\sqrt{3} = 2 \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \right)$ (см. пример 2), то

$$\sqrt[5]{-1 + i\sqrt{3}} = \sqrt[5]{2} \left(\cos \frac{\frac{2\pi}{3} + 2k\pi}{5} + i \sin \frac{\frac{2\pi}{3} + 2k\pi}{5} \right) = \\ = \sqrt[5]{2} \left(\cos \frac{2(3k+1)\pi}{15} + i \sin \frac{2(3k+1)\pi}{15} \right).$$

Все 5 искомых корней получаются, например, при $k = 0, 1, 2, 3, 4$

$$z_0 = \sqrt[5]{2} \left(\cos \frac{2\pi}{15} + i \sin \frac{2\pi}{15} \right),$$

$$z_1 = \sqrt[5]{2} \left(\cos \frac{8\pi}{15} + i \sin \frac{8\pi}{15} \right),$$

$$z_2 = \sqrt[5]{2} \left(\cos \frac{14\pi}{15} + i \sin \frac{14\pi}{15} \right),$$

$$z_3 = \sqrt[5]{2} \left(\cos \frac{20\pi}{15} + i \sin \frac{20\pi}{15} \right) = -\sqrt[5]{2} \left(\frac{1}{2} + i \frac{\sqrt{3}}{2} \right),$$

$$z_4 = \sqrt[5]{2} \left(\cos \frac{26\pi}{15} + i \sin \frac{26\pi}{15} \right).$$

Подчеркнем, что операция извлечения корня из комплексного числа многозначна. А именно *при извлечении корня n -й степени из комплексного числа, отличного от нуля, получается n различных чисел*. Все эти числа имеют один и тот же модуль, а их аргументы образуют арифметическую прогрессию с разностью $\frac{2\pi}{n}$. Геомет-

рически это означает, что изображающие их точки являются вершинами правильного n -угольника с центром в начале координат. На рисунке 14 изображены корни 5-й степени из числа $-1 + i\sqrt{3}$.

6. Корни из единицы. Рассмотрим особо извлечение корня n -й степени из 1. В этом случае $r = 1$, $\varphi = 0$, и формула (11) принимает вид

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}. \quad (13)$$

Точки z_k ($k = 0, 1, 2, \dots, n-1$) являются вершинами правильного n -угольника, вписанного в окружность радиуса 1 с центром в начале координат, причем одной из вершин этого многоугольника является 1. На рисунке 15 показан случай $n = 7$.

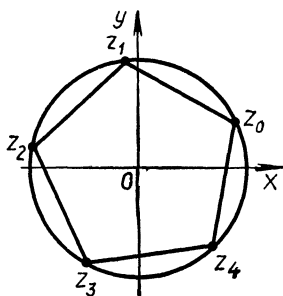


Рис. 14

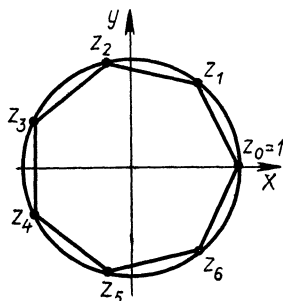


Рис. 15

Совокупность T_n всех корней n -й степени из 1 является подгруппой мультипликативной группы комплексных чисел (и даже ее подгруппы T , описанной в п. 3). В самом деле, из формул (8) и (9) следует, что

$$z_k z_l = z_{k+l}, \quad z_k^{-1} = z_{-k} \quad (14)$$

(где числа z_k определены формулой (13)); кроме того, $1 = z_0 \in T_n$.

Множество T_n является ядром гомоморфизма $z \rightarrow z^n$ мультипликативной группы комплексных чисел в себя. Отсюда также следует, что T_n — подгруппа этой группы.

Первое из соотношений (14) показывает, что отображение $k \rightarrow z_k$ является гомоморфизмом группы $\mathbf{Z}$ целых чисел (по сложению) на группу T_n . Ядром этого гомоморфизма является подгруппа $n\mathbf{Z}$ целых чисел, кратных n . По теореме о гомоморфизме группа T_n изоморфна фактор-группе $\mathbf{Z}/n\mathbf{Z}$, т. е. группе вычетов по модулю n .

В частности, группа T_n циклическая. В качестве ее образующего элемента можно взять, например,

$$z_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Из (14) следует, что $z_k = z_1^k$ для любого k .

Всякий образующий элемент группы T_n называется *первообразным корнем n -й степени из 1*. Иными словами, корень n -й степени из 1 называется первообразным, если любой корень n -й степени из 1 может быть получен из него возведением в некоторую степень. Из теории циклических групп (см., например, АТЧ III, п. 6 приложения к гл. II) следует, что z_k — первообразный корень тогда и только тогда, когда $(k, n) = 1$. Так, первообразными корнями 12-й степени из 1 будут z_1, z_5, z_7 и z_{11} . При простом n все корни, кроме 1, являются первообразными.

Корни n -й степени из 1 — это не что иное, как все корни многочлена $x^n - 1$ над полем комплексных чисел. Записывая для этого многочлена формулы Виета, можно получить ряд соотношений между корнями n -й степени из 1. Например, при $n > 1$ их сумма равна 0, так как коэффициент при x^{n-1} в многочлене $x^n - 1$ равен 0. Произведение всех корней n -й степени из 1 равно $(-1)^{n-1}$.

7. Комплексное сопряжение. Пусть $c = a + bi$ — какое-то комплексное число. Число $a - bi$ называется *сопряженным* (точнее, комплексно сопряженным) числу c и обозначается через $\bar{c}$. Геометрически комплексное сопряжение представляет собой отражение относительно действительной оси (рис. 16).

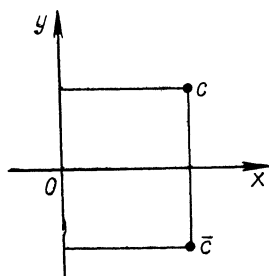


Рис. 16

Операция комплексного сопряжения обладает следующими свойствами:

$$1^0. \overline{\overline{c}} = c,$$

$$2^0. \overline{c_1 + c_2} = \overline{c_1} + \overline{c_2},$$

$$3^0. \overline{c_1 c_2} = \overline{c_1} \overline{c_2}.$$

Первое из этих свойств очевидно, второе и третье могут быть проверены непосредственным вычислением. Проверим, например, третье свойство. Пусть

$$c_1 = a_1 + b_1 i, \quad c_2 = a_2 + b_2 i;$$

тогда

$$c_1 c_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i.$$

С другой стороны,

$$\overline{c_1} = a_1 - b_1 i, \quad \overline{c_2} = a_2 - b_2 i,$$

$$\overline{c_1 c_2} = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + b_1 a_2) i = \overline{c_1} \overline{c_2},$$

что и требовалось доказать.

Отображение $c \rightarrow \overline{c}$ является взаимно однозначным отображением поля комплексных чисел на себя. Свойства 2^0 и 3^0 означают, что это отображение есть и з о м о р ф и з м поля комплексных чисел н а с е б я, или, как говорят, а в т о м о р ф и з м этого поля. Как и любой изоморфизм полей, комплексное сопряжение обладает следующими двумя свойствами:

$$4^0. \overline{c_1 - c_2} = \overline{c_1} - \overline{c_2},$$

$$5^0. \overline{\left(\frac{c_1}{c_2}\right)} = \frac{\overline{c_1}}{\overline{c_2}}.$$

Исходя из свойств $2^0 - 5^0$, нетрудно доказать по индукции, что если комплексное число c получается из чисел $c_1, c_2, \dots, c_k$ в результате каких-то арифметических операций, то эти же операции, произведенные над сопряженными числами $\overline{c_1}, \overline{c_2}, \dots, \overline{c_k}$, дадут сопряженный результат, т. е. число $\overline{c}$, например:

$$\frac{\overline{c_1^2 + c_2^2}}{\overline{c_1^3 - c_1 c_2}} = \overline{\left(\frac{c_1^2 + c_2^2}{c_1^3 - c_1 c_2}\right)}.$$

Полезно также отметить, что комплексное число совпадает со своим сопряженным тогда и только тогда, когда оно действительно. В частности, действительными будут числа $c + \overline{c}$ и $c\overline{c}$, каково бы ни было комплексное число c . Непосредственно проверяется, что если $c = a + bi$, то

$$c + \overline{c} = 2a, \quad c\overline{c} = a^2 + b^2;$$

иначе это можно записать следующим образом:

$$c + \overline{c} = 2 \operatorname{Re} c, \quad (15)$$

$$c\overline{c} = |c|^2. \quad (16)$$

Вопросы для самопроверки

1. Как строятся точка и вектор, изображающие комплексное число $c = a + bi$? Как они между собой связаны?
2. Каков геометрический смысл сложения комплексных чисел?
3. Каков геометрический смысл вычитания комплексных чисел?
4. Опишите множество точек, изображающих комплексные числа, модуль которых равен 2.
5. Опишите множество точек, изображающих комплексные числа, аргумент которых равен $\frac{3\pi}{4}$.
6. Что такое тригонометрическая форма комплексного числа? В каком смысле она единственна?
7. Как связаны между собой тригонометрические формы комплексных чисел c и $-c$? c и $\bar{c}$?
8. Каков геометрический смысл умножения на $-1 + i$ на $\frac{\sqrt{3}-i}{2}$?
9. Каков геометрический смысл деления на $r(\cos \varphi + i \sin \varphi)$, где $r > 0$?
10. Докажите, что комплексные числа, модуль которых равен 1, образуют группу по умножению.
11. В чем состоит формула Муавра?
12. Что такое корень n -й степени из комплексного числа c ?
13. Чему равна сумма всех корней n -й степени из числа c ? Чему равно их произведение?
14. Укажите какой-нибудь образующий элемент в группе корней 12-й степени из 1. Является ли $\frac{\sqrt{3}-i}{2}$ образующим этой группы?
15. Найдите все комплексные числа c , для которых $c^n = \bar{c}$.
16. Докажите, что всякое комплексное число, модуль которого равен 1, может быть представлено в виде $\frac{c}{\bar{c}}$, где c — некоторое комплексное число.
17. Докажите, что если c — корень n -й степени из 1, то и $\bar{c}$ будет корнем n -й степени из 1.
18. Что такое первообразный корень n -й степени из 1?
19. Укажите все первообразные корни 9-й степени из 1.
20. Напишите многочлен, корнями которого являются в точности первообразные корни 12-й степени из 1.

Упражнения

1. Найдите комплексное число c такое, что:
 - а) точка c делит в отношении 2 : 1 отрезок, соединяющий точки $-1 + i$ и $\frac{1}{2} - 2i$;
 - б) точка c есть точка пересечения медиан треугольника с вершинами в точках $2 - i$, $1 + 5i$ и $2i$;

в) точка c есть вершина параллелограмма, остальные три вершины которого находятся в точках $3i$, $4 - 3i$ и $-2 + i$, причем вершина c противоположна вершине $4 - 3i$.

2. Найдите модуль и аргумент комплексного числа: а) $-2i$; б) $-1 + i$; в) $-1 - i$; г) $\frac{\sqrt{3}}{2} - \frac{3}{2}i$.

3. Представьте в тригонометрической форме комплексное число: а) 3 ; б) $-1 - i$; в) $1 - i\sqrt{3}$; г) $\sqrt{3} + i$; д) $3 + i$; е) $-4 + i$.

4. Две вершины квадрата находятся в точках $-2 + i$ и $1 + 2i$. Найдите две другие его вершины, считая, что данные вершины: а) противоположные; б) соседние.

5. Вычислите

а) $(1 + i\sqrt{3})^{20}$; б) $(\sqrt{3} - i)^{12}$;

в) $\left(\frac{\sqrt{3} + i}{1 - i}\right)^{15}$; г) $\left(\frac{1 + i}{1 - i\sqrt{3}}\right)^{18}$.

6. Выразите через $\cos \varphi$ и $\sin \varphi$: а) $\cos 5\varphi$; б) $\sin 6\varphi$.

7. Извлеките корни: а) $\sqrt[3]{i}$; б) $\sqrt[3]{2 + 2i}$; в) $\sqrt[4]{-4}$; г) $\sqrt[6]{1}$;

д) $\sqrt[6]{\frac{1 - i}{\sqrt{3} + i}}$; е) $\sqrt[8]{\frac{1 + i}{\sqrt{3} - i}}$.

§ 2. ТЕОРЕМА О СУЩЕСТВОВАНИИ КОРНЯ В ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

1. Формулировка основной теоремы. Необходимость рассмотрения комплексных чисел связана с тем, что уравнение $x^2 + 1 = 0$ не имеет корней в поле действительных чисел. Можно было бы ожидать, что какие-то другие алгебраические уравнения с действительными (и тем более с комплексными) коэффициентами не имеют корней и в поле комплексных чисел. Однако это не так. Справедлива следующая теорема:

Теорема 1. *Всякое алгебраическое уравнение положительной степени с числовыми коэффициентами * имеет корень в поле комплексных чисел.*

Впервые доказанная в 1799 г. великим немецким математиком Гауссом, эта теорема известна как «основная теорема алгебры». Необходимо отметить, однако, что это название теоремы, несмотря на ее важность для всех разделов алгебры, связанных с числами, все же не может в настоящее время пониматься буквально, так как современная алгебра не ограничивается изучением операций над числами.

Существует много доказательств «основной теоремы алгебры», причем ни одно из них не является в полной мере алгебраическим. Это связано с тем, что в самой конструкции поля действительных

* Имеются в виду любые комплексные числа.

чисел и тем самым поля комплексных чисел заложены неалгебраические элементы. В следующем пункте будет приведено доказательство, основанное на теореме о минимуме непрерывной функции и на так называемой «лемме Даламбера».

2. Доказательство основной теоремы. Рассмотрим уравнение

$$f(x) = 0, \quad (1)$$

где $f(x)$ — нормированный многочлен степени $n \geq 1$ с комплексными коэффициентами

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n, \quad (2)$$

$$(a_1, a_2, \dots, a_n \in \mathbb{C}, n \geq 1).$$

Л е м м а 1. *Существует такое положительное число A , что при всех $x_0 \in \mathbb{C}$, удовлетворяющих условию $|x_0| > A$, выполняется неравенство $|f(x_0)| > |f(0)|$.*

Д о к а з а т е л ь с т в о. Воспользуемся соотношениями между модулями комплексных чисел (см. пп. 2, 3 § 1):

$$|c_1 c_2| = |c_1| |c_2|,$$

$$|c_1| - |c_2| \leq |c_1 + c_2| \leq |c_1| + |c_2|.$$

Для любого $x_0 \in \mathbb{C}$ имеем:

$$f(x_0) = x_0^n + a_1 x_0^{n-1} + a_2 x_0^{n-2} + \dots + a_n =$$

$$= x_0^n \left(1 + \frac{a_1}{x_0} + \frac{a_2}{x_0^2} + \dots + \frac{a_n}{x_0^n} \right),$$

так что

$$|f(x_0)| = |x_0|^n \left| 1 + \frac{a_1}{x_0} + \frac{a_2}{x_0^2} + \dots + \frac{a_n}{x_0^n} \right| \geq$$

$$\geq |x_0|^n \left(1 - \left| \frac{a_1}{x_0} + \frac{a_2}{x_0^2} + \dots + \frac{a_n}{x_0^n} \right| \right) \geq$$

$$\geq |x_0|^n \left(1 - \left| \frac{a_1}{x_0} \right| - \left| \frac{a_2}{x_0^2} \right| - \dots - \left| \frac{a_n}{x_0^n} \right| \right) =$$

$$= |x_0|^n \left(1 - \frac{|a_1|}{|x_0|} - \frac{|a_2|}{|x_0|^2} \dots - \frac{|a_n|}{|x_0|^n} \right).$$

Рассмотрим функцию

$$\varphi(t) = t^n \left(1 - \frac{|a_1|}{t} - \frac{|a_2|}{t^2} - \dots - \frac{|a_n|}{t^n} \right)$$

действительной переменной t . Очевидно, что $\lim_{t \rightarrow +\infty} \varphi(t) = +\infty$.

Следовательно, для любого C существует такое $A > 0$, что $\varphi(t) > C$ при всех $t > A$. В частности, можно взять $C = |f(0)| = |a_n|$. Соответствующее A будет удовлетворять требованию леммы. В самом деле, при $|x_0| > A$ имеем:

$$|f(x_0)| \geq \varphi(|x_0|) > C = |f(0)|.$$

Лемма доказана.

Пусть A — число, определенное по лемме 1. Рассмотрим на комплексной плоскости замкнутый круг K радиуса A с центром в начале координат. По лемме вне круга K многочлен $f(x)$ принимает значения по модулю большие, чем $f(0)$. (В частности, отсюда следует, что он может обращаться в нуль только в круге K .)

Рассмотрим функцию

$$\psi(u, v) = |f(u + iv)|$$

двух действительных переменных u, v . Покажем, что она непрерывна на всей плоскости. Пусть $a_k = b_k + ic_k$, где $b_k, c_k \in \mathbf{R}$; тогда

$$f(u + iv) = (u + iv)^n + (b_1 + ic_1)(u + iv)^{n-1} + \dots + (b_n + ic_n) = \psi_1(u, v) + i\psi_2(u, v),$$

где $\psi_1(u, v), \psi_2(u, v)$ — некоторые многочлены с действительными коэффициентами. Очевидно, что

$$\psi(u, v) = \sqrt{\psi_1(u, v)^2 + \psi_2(u, v)^2}.$$

Так как многочлены $\psi_1(u, v), \psi_2(u, v)$ — непрерывные функции, то и функция $\psi(u, v)$ непрерывна. Область определения функции $\psi(u, v)$, т. е. плоскость переменных u, v , можно отождествить с комплексной плоскостью.

Из курса анализа известно, что всякая функция двух (или любого другого числа) действительных переменных, определенная и непрерывная во всех точках замкнутого ограниченного множества, достигает минимума в некоторой точке этого множества. Применяя эту теорему к функции $\psi(u, v)$ в круге K , можно заключить, что существует точка $x_0 = u_0 + iv_0$ этого круга, в которой функция $\psi(u, v)$ достигает минимума. Это означает, что

$$|f(x_0)| \leq |f(x_1)| \quad (3)$$

для всех $x_1 \in K$. В частности,

$$|f(x_0)| \leq |f(0)|,$$

так как $0 \in K$. Согласно построению круга K , значения многочлена $f(x)$ вне этого круга по модулю больше, чем $f(0)$, и тем более, чем $f(x_0)$. Следовательно, неравенство (3) выполняется для всех $x_1 \in \mathbf{C}$.

Теперь нам понадобится такая лемма:

Л е м м а 2 (л е м м а Д а л а м б е р а). Если многочлен $f(x)$ не обращается в нуль в точке $x_0 \in \mathbf{C}$, то для любого $\varepsilon > 0$ существует такое $u \in \mathbf{C}$, что $|u| < \varepsilon$ и $|f(x_0 + u)| < |f(x_0)|$.

Иными словами, сколь угодно близко к точке x_0 на комплексной плоскости найдутся точки, в которых значение многочлена $f(x)$ по модулю меньше, чем $f(x_0)$. Поэтому если $|f(x)|$ достигает минимума в какой-то точке комплексной плоскости, то этот минимум равен нулю*. С другой стороны, выше было доказано, что $|f(x)|$ достигает минимума в некоторой точке x_0 . По лемме Далам-

* Из леммы Даламбера следует даже, что всякий локальный минимум равен нулю. Однако для доказательства основной теоремы это не требуется.

бера заключаем, что $|f(x_0)| = 0$ и, значит, $f(x_0) = 0$, т. е. x_0 — корень уравнения (1). Таким образом, для завершения доказательства основной теоремы остается лишь доказать лемму Даламбера.

Д о к а з а т е л ь с т в о л е м м ы 2. Сделав замену $x = x_0 + y$, где y — новая переменная, и произведя тождественные преобразования, представим многочлен $f(x)$ в виде многочлена от y :

$$\begin{aligned} f(x) &= (x_0 + y)^n + a_1(x_0 + y)^{n-1} + \dots + a_{n-1}(x_0 + y) + a_n = \\ &= c_0 + c_1 y + \dots + c_{n-1} y^{n-1} + c_n y^n. \end{aligned} \quad (4)$$

Так как $y = x - x_0$, то при подстановке в это равенство $x = x_0$ получаем $f(x_0) = c_0$. По условию $f(x_0) \neq 0$. Следовательно, $c_0 \neq 0$. Кроме того, $c_n = 1 \neq 0$, поскольку член, содержащий y^n , появляется только при раскрытии скобок в выражении $(x_0 + y)^n$. Пусть k — наименьшее положительное число такое, что $c_k \neq 0$. Иначе говоря, пусть $c_1 = c_2 = \dots = c_{k-1} = 0$, но $c_k \neq 0$. (Если $c_1 \neq 0$, то $k = 1$.) Имеем тогда:

$$f(x) = c_0 + c_k y^k + c_{k+1} y^{k+1} + \dots + c_n y^n \quad (c_0 \neq 0, c_k \neq 0). \quad (5)$$

Идея доказательства леммы Даламбера состоит в том, что поведение функции $f(x)$ (а значит, и $|f(x)|$) в малой окрестности точки x_0 в основном определяется первыми двумя членами разложения (5). Если бы остальных членов вообще не было, то можно было бы рассуждать следующим образом. Обозначим через y_0 какое-либо решение уравнения

$$c_0 + c_k y^k = 0, \quad (6)$$

т. е. одно из значений корня k -й степени из $-\frac{c_0}{c_k}$.

Пусть t — действительное число, лежащее в интервале $]0; 1[$. Тогда

$$f(x_0 + ty_0) = c_0 + c_k t^k y_0^k = c_0 (1 - t^k),$$

откуда видно, что

$$|f(x_0 + ty_0)| < |c_0|.$$

Выбирая t достаточно малым, можно добиться того, чтобы $|ty_0| < \varepsilon$, и тогда комплексное число $u = ty_0$ будет удовлетворять требованиям леммы.

В общем случае доказательство отличается лишь тем, что оценивается модуль суммы остальных членов разложения (5). А именно пусть y_0 , как и выше, — решение уравнения (6), $t \in]0; 1[$. Имеем:

$$\begin{aligned} f(x_0 + ty_0) &= c_0 + c_k t^k y_0^k + c_{k+1} t^{k+1} y_0^{k+1} + \dots + c_n t^n y_0^n = \\ &= c_0 (1 - t^k) + (c_{k+1} y_0^{k+1} + \dots + c_n t^{n-k-1} y_0^n) t^{k+1}. \end{aligned}$$

Модуль второго выражения, стоящего в скобках, не превосходит числа

$$M = |c_{k+1}| |y_0|^{k+1} + \dots + |c_n| |y_0|^n.$$

Следовательно,

$$|f(x_0 + ty_0)| \leq |c_0|(1 - t^k) + Mt^{k+1} = |c_0| \left(1 - t^k \left(1 - \frac{Mt}{|c_0|}\right)\right).$$

Выберем t в интервале $]0; 1[$ настолько малым, чтобы $Mt < |c_0|$. Тогда

$$0 < 1 - \frac{Mt}{|c_0|} < 1 \text{ и } |f(x_0 + ty_0)| < |c_0|.$$

Если дополнительно потребовать, чтобы $|ty_0| < \varepsilon$, то комплексное число $u = ty_0$ будет удовлетворять требованиям леммы.

3. Разложение на линейные множители в кольце $C[x]$. Согласно доказанной выше «основной теореме алгебры» всякий многочлен $f(x) \in C[x]$ степени $n \geq 1$ имеет корень x_0 в поле C . В случае когда степень $f(x)$ больше единицы, из наличия корня у многочлена $f(x)$ вытекает его приводимость (см. п. 3 § 2 гл. II). Следовательно, в кольце $C[x]$ неприводимы только многочлены первой степени.

Каждый многочлен $f(x) \in C[x]$ степени $n \geq 1$ может быть разложен на неприводимые множители в кольце $C[x]$. Из предыдущего замечания вытекает, что это разложение является разложением на линейные множители. Итак, доказана такая теорема:

Теорема 2. *Каждый многочлен $f(x) \in C[x]$ степени $n \geq 1$ может быть разложен на линейные множители в кольце $C[x]$.*

Пример 1. Разложим на линейные множители многочлен

$$f(x) = x^2 - x + 1 + i \in C[x].$$

По формуле решения квадратного уравнения (применимой и к уравнениям с комплексными коэффициентами) находим корни многочлена $f(x)$:

$$x_{1,2} = \frac{1 \pm \sqrt{-3-4i}}{2} = \frac{1 \pm (1-2i)}{2},$$

откуда $x_1 = 1 - i$, $x_2 = i$. Следовательно,

$$f(x) = (x - 1 + i)(x - i).$$

Пример 2. Разложим на линейные множители многочлен

$$f(x) = x^3 - 3x + 2 \in C[x].$$

Легко видеть, что один из корней многочлена $f(x)$ будет равен 1. Разделив $f(x)$ на $x - 1$, получим многочлен

$$x^2 + x - 2 = (x - 1)(x - 2).$$

Следовательно,

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

Комбинируя теорему 2 с теоремой 1 § 2 гл. I, получим следующее следствие.

Следствие. *Всякое алгебраическое уравнение степени $n \geq 1$ с числовыми коэффициентами имеет в поле C ровно n корней (с учетом кратностей).*

В дальнейшем, говоря о корнях алгебраических уравнений (или многочленов) с числовыми коэффициентами, мы всегда будем иметь в виду комплексные корни.

Пример 3. Найдем все корни уравнения

$$x^4 + x^3 + 2x + 2 = 0.$$

Левую часть уравнения можно представить в виде

$$(x + 1)(x^3 + 2).$$

Одним корнем, очевидно, будет -1 , а остальные три корня — это кубические корни из -2 , т. е. $-\sqrt[3]{2}$, $\sqrt[3]{2} \left(\frac{1}{2} + i\frac{\sqrt{3}}{2} \right)$ и $\sqrt[3]{2} \left(\frac{1}{2} - i\frac{\sqrt{3}}{2} \right)$.

Вопросы для самопроверки

1. В чем состоит «основная теорема алгебры»?
2. Докажите, что модуль многочлена от комплексной переменной $z = u + iv$ ($u, v \in \mathbf{R}$), является непрерывной функцией от u и v .
3. Докажите, что модуль многочлена от комплексной переменной достигает минимума.
4. В чем состоит смысл леммы Даламбера?
5. Пользуясь леммой Даламбера, докажите, что минимум модуля многочлена от комплексной переменной равен нулю.
6. Как определить число корней (с учетом кратностей) многочлена над полем комплексных чисел?
7. Докажите, что в кольце $\mathbf{C}[x]$ всякий многочлен разлагается на линейные множители.
8. Какие многочлены неприводимы в кольце $\mathbf{C}[x]$?

Упражнения

Разложите на линейные множители в кольце $\mathbf{C}[x]$ многочлены:

- а) $x^4 + 4$;
- б) $x^3 - 6x^2 + 11x - 6$;
- в) $x^4 + 4x^3 + 4x^2 + 1$;
- г) $x^4 - 10x^2 + 1$.

§ 3. МНОГОЧЛЕНЫ И АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ С ДЕЙСТВИТЕЛЬНЫМИ КОЭФФИЦИЕНТАМИ

1. Свойства мнимых корней. При изучении многочленов с действительными коэффициентами представляют интерес не только их действительные, но и мнимые корни, рассмотрение которых позволяет, в частности, выяснить, какие многочлены неприводимы в кольце $\mathbf{R}[x]$.

Установим одно простое свойство совокупности всех комплексных корней многочлена с действительными коэффициентами.

Теорема 1. Если комплексное число x_0 является корнем многочлена с действительными коэффициентами, то сопряженное число $\overline{x_0}$ также является корнем этого многочлена.

Отметим, что утверждение теоремы представляет интерес только в том случае, когда x_0 — мнимое число, поскольку если x_0 действительное, то $\overline{x_0} = x_0$.

Доказательство. Пусть данный многочлен имеет вид

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n. \\ (a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{R})$$

По условию, $f(x_0) = 0$, т. е.

$$a_0 x_0^n + a_1 x_0^{n-1} + \dots + a_{n-1} x_0 + a_n = 0.$$

Для вычисления $f(\overline{x_0})$ воспользуемся следующими свойствами операции комплексного сопряжения (см. п. 7 § 1):

$$\overline{c_1 + c_2} = \overline{c_1} + \overline{c_2}, \quad \overline{c_1 c_2} = \overline{c_1} \overline{c_2},$$

а также тем, что любое действительное число совпадает со своим сопряженным. Имеем:

$$\begin{aligned} f(\overline{x_0}) &= a_0 \overline{x_0}^n + a_1 \overline{x_0}^{n-1} + \dots + a_{n-1} \overline{x_0} + a_n = \\ &= \overline{a_0} \overline{x_0}^n + \overline{a_1} \overline{x_0}^{n-1} + \dots + \overline{a_{n-1}} \overline{x_0} + \overline{a_n} = \\ &= \overline{a_0 x_0^n + a_1 x_0^{n-1} + \dots + a_{n-1} x_0 + a_n} = \overline{f(x_0)} = \overline{0} = 0, \end{aligned}$$

т. е. $\overline{x_0}$ также является корнем многочлена $f(x)$.

2. Разложение на неприводимые множители в кольце $\mathbb{R}[x]$. Из теоремы 1 можно вывести, что в кольце $\mathbb{R}[x]$ неприводимы только многочлены первой степени и многочлены второй степени, не имеющие действительных корней.

В самом деле, пусть $f(x) \in \mathbb{R}[x]$ — многочлен степени $n \geq 3$ и x_0 — какой-либо его комплексный корень. Если $x_0 \in \mathbb{R}$, то многочлен $f(x)$ делится на $x - x_0$ в кольце $\mathbb{R}[x]$ и, следовательно, приводим. Если $x_0 \notin \mathbb{R}$, то, по теореме 1, $\overline{x_0}$ также является корнем многочлена $f(x)$ (причем $\overline{x_0} \neq x_0$). В этом случае в разложение многочлена $f(x)$ на линейные множители в кольце $\mathbb{C}[x]$ входят множители $x - x_0$ и $x - \overline{x_0}$. Следовательно, $f(x)$ делится на квадратный трехчлен

$$(x - x_0)(x - \overline{x_0}) = x^2 - (x_0 + \overline{x_0})x + x_0 \overline{x_0}.$$

Так как $x_0 + \overline{x_0} \in \mathbb{R}$ и $x_0 \overline{x_0} \in \mathbb{R}$, то

$$(x - x_0)(x - \overline{x_0}) \in \mathbb{R}[x]$$

и, значит, многочлен $f(x)$ приводим в кольце $\mathbb{R}[x]$.

Таким образом, в кольце $\mathbb{R}[x]$ всякий многочлен, степень которого больше двух, приводим. Что касается многочленов второй

степени, то из них неприводимы те и только те, которые не имеют действительных корней (см. п. 3 § 2 гл. II).

Из описания неприводимых многочленов в кольце $R[x]$ следует, что нормированное разложение на неприводимые множители любого многочлена $f(x) \in R[x]$ имеет вид

$$f(x) = a(x - x_1)^{k_1}(x - x_2)^{k_2} \dots (x - x_s)^{k_s} \times \\ \times (x^2 + p_1x + q_1)^{l_1}(x^2 + p_2x + q_2)^{l_2} \dots (x^2 + p_tx + q_t)^{l_t}, \quad (1)$$

где $x_1, x_2, \dots, x_s$ — различные числа, а $x^2 + p_1x + q_1, x^2 + p_2x + q_2, \dots, x^2 + p_tx + q_t$ — различные квадратные трехчлены, не имеющие действительных корней. Обозначим через y_i какой-либо комплексный корень трехчлена $x^2 + p_ix + q_i$; тогда другим его корнем будет $\bar{y}_i$ и, значит,

$$x^2 + p_ix + q_i = (x - y_i)(x - \bar{y}_i). \quad (2)$$

Подставляя эти выражения в (1), получаем разложение многочлена $f(x)$ на линейные множители в кольце $C[x]$:

$$f(x) = a(x - x_1)^{k_1}(x - x_2)^{k_2} \dots (x - x_s)^{k_s} \times \\ \times (x - y_1)^{l_1}(x - \bar{y}_1)^{l_1}(x - y_2)^{l_2}(x - \bar{y}_2)^{l_2} \dots (x - y_t)^{l_t}(x - \bar{y}_t)^{l_t}. \quad (3)$$

Заметим, что $y_i \neq y_j$ при $i \neq j$, так как в противном случае из формулы (2) следовало бы, что

$$x^2 + p_ix + q_i = x^2 + p_jx + q_j.$$

По той же причине $y_i \neq \bar{y}_j$. Отсюда следует, что y_i и $\bar{y}_i$ — корни кратности l_i . Таким образом, *каждому неприводимому делителю $h(x)$ второй степени многочлена $f(x) \in R[x]$ соответствует пара сопряженных мнимых корней многочлена $f(x)$, причем кратность каждого из них равна кратности делителя $h(x)$.*

Пример 1. Разложим на неприводимые множители в кольце $R[x]$ многочлен

$$f(x) = x^8 + 1.$$

Многочлен $f(x)$ не имеет действительных корней. Его комплексные корни — это корни восьмой степени из -1 . Они могут быть найдены по формуле

$$y_k = \cos \frac{\pi + 2k\pi}{8} + i \sin \frac{\pi + 2k\pi}{8} \quad (k = 0, 1, 2, \dots, 7).$$

При этом $\bar{y}_k = y_{7-k}$. Так как

$$(x - y_k)(x - \bar{y}_k) = x^2 - (y_k + \bar{y}_k)x + y_k\bar{y}_k = \\ = x^2 - 2x \cos \frac{\pi + 2k\pi}{8} + 1,$$

то разложение многочлена $f(x)$ на неприводимые множители в кольце $R[x]$ имеет вид

$$f(x) = \prod_{k=0}^3 \left(x^2 - 2x \cos \frac{\pi + 2k\pi}{8} + 1 \right) = \\ = \left(x^2 - 2x \cos \frac{\pi}{8} + 1 \right) \left(x^2 - 2x \cos \frac{3\pi}{8} + 1 \right) \times \\ \times \left(x^2 - 2x \cos \frac{5\pi}{8} + 1 \right) \left(x^2 - 2x \cos \frac{7\pi}{8} + 1 \right).$$

Пример 2. Найдем все корни многочлена

$$f(x) = x^5 - 8x^3 + 24x^2 - 24x + 16,$$

зная, что $1 - i$ является его двукратным корнем.

Число $\overline{1 - i} = 1 + i$ также должно быть двукратным корнем многочлена $f(x)$. Следовательно, $f(x)$ делится на квадрат трехчлена

$$(x - 1 + i)(x - 1 - i) = x^2 - 2x + 2.$$

Выполнив деление $f(x)$ на $(x^2 - 2x + 2)^2$, получаем разложение многочлена $f(x)$ на неприводимые множители в кольце $R[x]$:

$$f(x) = (x + 4)(x^2 - 2x + 2)^2.$$

Таким образом, кроме двукратных корней $1 - i$ и $1 + i$, многочлен $f(x)$ имеет еще один (простой) корень -4 .

3. Число действительных корней. В предыдущем пункте мы показали, что мнимые корни алгебраического уравнения с действительными коэффициентами разбиваются на пары сопряженных; поэтому число действительных корней (с учетом кратностей) либо равно степени уравнения, либо на четное число меньше. В частности, *любое уравнение нечетной степени с действительными коэффициентами имеет хотя бы один действительный корень.*

Понятно, что представляет интерес определение точного числа действительных корней.

Вычисляя значения многочлена $f(x)$ в отдельных точках, мы можем обнаружить, что в каких-то точках x_1, x_2 он принимает значения разных знаков. Поскольку многочлен — непрерывная функция, отсюда следует, что в некоторой точке интервала $[x_1, x_2]$ он должен обращаться в нуль. (Конечно, это еще не значит, что в интервале $[x_1, x_2]$ находится ровно один корень многочлена $f(x)$.) Таким способом мы можем оценить снизу число действительных корней. Однако точное определение этого числа требует привлечения других соображений.

Например, для многочлена $f(x) = x^4 + x^2 - 4x + 1$ находим:

$$f(0) = 1 > 0, f(1) = -1 < 0, f(2) = 13 > 0.$$

Следовательно, $f(x)$ имеет корни на каждом из интервалов $[0; 1]$ и $[1; 2]$. Нетрудно показать, что $f(x_0) > 0$ при $x_0 \leq 0$, а также при $x_0 \geq 2$. Следовательно, все действительные корни многочлена

$f(x)$ лежат в интервале $]0; 2[$. Однако мы не можем на основании проделанных вычислений утверждать, что в этом интервале находится только два корня, т. е. что многочлен $f(x)$ имеет только два действительных корня. Это можно было бы доказать, например, с помощью теоремы Декарта: *число положительных корней многочлена с действительными коэффициентами не превосходит числа перемен знака в последовательности его коэффициентов* (которое в рассмотренном примере равно двум).

Существуют теоремы (например, теорема Штурма), которые позволяют точно определить число действительных корней любого многочлена с действительными коэффициентами. Мы не будем приводить здесь эти теоремы. Интересующийся читатель может найти их, например, в книге А. Г. Куроша «Курс высшей алгебры».

4. Вычисление корней. Действительные корни любого алгебраического уравнения с действительными коэффициентами могут быть в принципе найдены с любой точностью путем вычисления значений многочлена в отдельных точках. Поясним это на примере. Многочлен

$$f(x) = x^4 + x^2 - 4x + 1$$

имеет корень в интервале $]1; 2[$ (см. п. 3). Обозначим этот корень через x_0 . Вычисляя значения $f(x)$ в точках 1,1, 1, 2, ..., 1, 9, мы обнаруживаем, что

$$f(1,2) < 0, f(1,3) > 0.$$

Следовательно, x_0 лежит в интервале $]1, 2; 1, 3[$. Вычисляя значения $f(x)$ в точках 1, 21, 1, 22, ..., 1, 29, находим, что

$$f(1,24) < 0, f(1,25) > 0.$$

Следовательно, x_0 лежит в интервале $]1,24; 1,25[$. Таким образом мы можем найти любое количество десятичных знаков искомого корня x_0 , т. е. вычислить его с любой наперед заданной точностью.

Описанный выше «табличный» метод решения уравнений требует больших вычислений. Существуют гораздо более совершенные методы: метод Ньютона, метод итерации, метод Лагранжа, метод Лобачевского и др. Они применимы к алгебраическим уравнениям любой степени, а некоторые из них — и к трансцендентным уравнениям. Существуют также методы (например, метод Лобачевского), пригодные для вычисления не только действительных, но и мнимых корней.

Изложение этих методов выходит за рамки нашей программы: они относятся скорее к вычислительной математике, чем к алгебре. Читателю, который заинтересуется этим вопросом, мы рекомендуем статью А. П. Доморяда в книге «Энциклопедия элементарной математики», т. II.

Вопросы для самопроверки

1. Каким свойством обладает совокупность всех комплексных корней многочлена с действительными коэффициентами?
2. Докажите, что если x_0 — двукратный комплексный корень многочлена с действительными коэффициентами, то $\overline{x_0}$ также будет двукратным корнем этого многочлена.
3. Пусть $f(x) \in C[x]$ — нормированный многочлен, корни которого (с учетом кратностей) разбиваются на пары сопряженных. Докажите, что коэффициенты многочлена $f(x)$ действительны.
4. Докажите, что многочлен нечетной степени с действительными коэффициентами имеет действительный корень.
5. Приводим ли в кольце $R[x]$ многочлен $x^4 + x + 1$?
6. Какие многочлены неприводимы в кольце $R[x]$?

Упражнения

1. Разложите на неприводимые множители в кольце $R[x]$:
а) $x^6 + 27$; б) $x^9 - 8$;
в) $x^6 + x^3 + 1$; г) $x^8 - x^6 + x^4 - x^2 + 1$.
2. Найдите корни уравнения с действительными коэффициентами, зная, что x_0 является k -кратным корнем:
а) $x^5 - 6x^4 + 15x^3 - 20x^2 + 14x - 4 = 0$,
 $x_0 = 1 + i$, $k = 1$;
б) $x^6 + 2x^5 + 4x^4 + 4x^3 + 5x^2 + 2x + 2 = 0$,
 $x_0 = i$, $k = 2$.
3. Вычислите табличным методом с точностью до 0,01 действительный корень уравнения, содержащийся в интервале $]1, 2[$:
а) $x^4 + 3x^3 - 9x - 9 = 0$;
б) $x^4 - 6x^2 + 12x - 8 = 0$.

§ 4. АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ ТРЕТЬЕЙ И ЧЕТВЕРТОЙ СТЕПЕНИ (РЕШЕНИЕ В РАДИКАЛАХ)

1. Решение алгебраических уравнений. Известная из школьной алгебры формула решения квадратного уравнения выражает его корни через коэффициенты и некоторые фиксированные числа (2 и 4) при помощи рациональных операций (сложения, вычитания, умножения и деления) и извлечения квадратного корня. Эта формула справедлива для квадратного уравнения с любыми действительными или комплексными коэффициентами. Естественно желание найти аналогичные формулы для уравнений более высоких степеней; при этом следует, конечно, допустить извлечение корня любой степени. Такие формулы называют решениями в радикалах. С практической точки зрения они не обладают никакими преимуществами по сравнению с так называемыми численными (или приближенными) методами решения уравнений, о которых шла речь в п. 4 § 3. Тео-

ретическое значение решений в радикалах состоит в том, что они в определенном смысле сводят решение произвольных уравнений данной степени к решению простейших, двучленных алгебраических уравнений вида $x^m - c = 0$.

Решения в радикалах уравнений третьей и четвертой степени были найдены в XVI в. итальянскими математиками Кардано* и Феррари, а в 1824 г. норвежский математик Абель доказал, что для уравнений пятой и более высокой степени таких решений не существует. (Эта теорема носит название теоремы Руффини — Абеля, поскольку первое ее доказательство было опубликовано в 1799 г. итальянским математиком Руффини; однако оно было неполным.)

В этом параграфе будут выведены формулы для решения в радикалах уравнений третьей и четвертой степени. Что же касается доказательства несуществования таких формул для уравнений более высоких степеней, то оно выходит за рамки нашей программы.

2. Решение кубических уравнений. Заметим, что решение любого алгебраического уравнения вида

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n = 0$$

с помощью замены $x = y - \frac{a_1}{n}$ сводится к решению «неполного» уравнения

$$y^n + b_2 y^{n-2} + \dots + b_{n-1} y + b_n = 0,$$

не содержащего $(n - 1)$ -й степени неизвестного. В самом деле, по формуле бинома Ньютона

$$\left(y - \frac{a_1}{n}\right)^n = y^n - n \frac{a_1}{n} y^{n-1} + \dots = y^n - a_1 y^{n-1} + \dots,$$

где многоточие обозначает члены степеней, меньших, чем $n - 1$.

Поэтому при подстановке $y - \frac{a_1}{n}$ вместо x в левую часть исходного уравнения члены с y^{n-1} уничтожаются. Именно этот прием приводит к решению квадратного уравнения; однако для уравнений более высоких степеней он оказывается недостаточным.

Рассмотрим неполное кубическое уравнение

$$x^3 + px + q = 0 \tag{1}$$

с произвольными комплексными коэффициентами p, q .

Положим $x = u + v$. Левая часть уравнения примет вид

$$(u + v)^3 + p(u + v) + q = u^3 + v^3 + (3uv + p)(u + v) + q. \tag{2}$$

Отсюда следует, что если $(u_0; v_0)$ — решение системы уравнений

$$\begin{cases} u^3 + v^3 + q = 0, \\ 3uv + p = 0, \end{cases} \tag{3}$$

то $x_0 = u_0 + v_0$ будет решением уравнения (1).

* Есть свидетельство, что формулу для решения кубического уравнения примерно на двадцать лет раньше Кардано открыл дель Ферро. Однако дель Ферро не опубликовал своего открытия.

Обратно, если x_0 — решение уравнения (1), то существует такое решение $(u_0; v_0)$ системы (3), что $x_0 = u_0 + v_0$. Действительно, пусть u_0 и v_0 — корни квадратного уравнения

$$t^2 - x_0 t - \frac{p}{3} = 0.$$

Тогда по формулам Виета имеем:

$$u_0 + v_0 = x_0, \quad u_0 v_0 = -\frac{p}{3}.$$

Последнее равенство показывает, что $3u_0 v_0 + p = 0$, т. е. пара $(u_0; v_0)$ удовлетворяет второму уравнению системы (3).

Подставляя u_0 и v_0 в равенство (2) и учитывая, что $x_0 = u_0 + v_0$ есть корень уравнения (1), находим, что $u_0^3 + v_0^3 + q = 0$, т. е. пара $(u_0; v_0)$ удовлетворяет и первому уравнению системы (3).

Итак, все корни уравнения (1) можно получить следующим образом: найти все решения системы (3) и для каждого из них взять сумму составляющих его чисел.

Для решения системы (3) представим ее в виде

$$\begin{cases} u^3 + v^3 = -q, \\ uv = -\frac{p}{3}. \end{cases} \quad (4)$$

Возведя второе уравнение в куб, получим:

$$u^3 v^3 = -\frac{p^3}{27}.$$

Следовательно, u^3 и v^3 — корни квадратного уравнения

$$z^2 + qz - \frac{p^3}{27} = 0,$$

решая которое находим:

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}. \quad (5)$$

(Знаки «+» и «-» перед квадратным корнем имеют только тот смысл, что при вычислении u^3 следует взять одно значение квадратного корня, а при вычислении v^3 — другое.)

Из формул (5) получаем следующую формулу решения уравнения (1), называемую ф о р м у л о й К а р д а н о:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \quad (6)$$

Значения кубических корней в формуле (6) не могут выбираться независимо, так как в системе (4) имеется уравнение

$$uv = -\frac{p}{3},$$

которое мы пока не учли в полной мере (мы возвели его в куб).

Значения кубических корней в формуле Кардано следует выбирать таким образом, чтобы их произведение равнялось $-\frac{p}{3}$. Так как куб этого произведения всегда равен $\left(-\frac{p}{3}\right)^3 = -\frac{p^3}{27}$, то само произведение может отличаться от $-\frac{p}{3}$ лишь множителем, являющимся кубическим корнем из единицы. Поэтому, выбрав произвольное значение одного из кубических корней в формуле (6), мы можем всегда подобрать значение другого корня таким образом, чтобы их произведение равнялось $-\frac{p}{3}$. Таким образом находятся все три корня уравнения (1).

Пусть u_1 и v_1 — какие-то значения кубических корней из $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ и $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, произведение которых равно $-\frac{p}{3}$. Двумя другими значениями первого кубического корня будут $u_1\omega$ и $u_1\omega^2$, где $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ — кубический корень из единицы. Аналогично двумя другими значениями второго кубического корня будут $v_1\omega$ и $v_1\omega^2$. При этом $u_1\omega$ будет комбинироваться с $v_1\omega^2$, а $u_1\omega^2$ — с $v_1\omega$. Таким образом, корнями уравнения (1) будут числа

$$\begin{aligned} x_1 &= u_1 + v_1, \\ x_2 &= u_1\omega + v_1\omega^2, \\ x_3 &= u_1\omega^2 + v_1\omega. \end{aligned} \quad (7)$$

Выясним, при каком условии числа x_1, x_2, x_3 различны. Согласно теореме 4 § 2 гл. II, это будет тогда и только тогда, когда дискриминант многочлена $x^3 + px + q$ отличен от нуля. В п. 8 § 2 гл. II был вычислен дискриминант любого многочлена третьей степени. В частности, для многочлена $x^3 + px + q$ он равен

$$D = -27q^2 - 4p^3. \quad (8)$$

С точностью до постоянного множителя -108 это выражение совпадает с тем, которое стоит под знаком квадратного радикала в формуле Кардано.

Таким образом, уравнение (1) имеет кратный корень тогда и только тогда, когда $D = 0$.

В случае, когда $D = 0$, для решения уравнения (1) нет необходимости прибегать к формуле Кардано. В самом деле, пусть x_1, x_2, x_3 — корни уравнения (1), причем $x_2 = x_3$. По формуле Виета $x_1 + x_2 + x_3 = 0$, откуда следует, что $x_1 = -2x_2$. Оставшиеся две формулы Виета запишутся так:

$$\begin{aligned} -2x_2^2 - 2x_2^2 + x_2^2 &= -3x_2^2 = p, \\ -2x_2^3 &= -q. \end{aligned}$$

Отсюда получаем:

$$x_2 = x_3 = -\frac{3q}{2p}, \quad x_1 = \frac{3q}{p}. \quad (9)$$

(Если $p = 0$, то и $q = 0$; в этом случае $x_1 = x_2 = x_3 = 0$).

Пример 1. Решим уравнение

$$x^3 - 4x^2 - 3x + 18 = 0.$$

Сделав замену $x = y + \frac{4}{3}$, получим неполное уравнение

$$y^3 - \frac{25}{3}y + \frac{250}{27} = 0,$$

в котором $p = -\frac{25}{3}$, $q = \frac{250}{27}$. Его дискриминант равен

$$D = -\frac{250^3}{27} + \frac{4 \cdot 25^3}{27} = 0.$$

По формулам (9) находим корни: $y_1 = -\frac{10}{3}$, $y_2 = y_3 = \frac{5}{3}$. Корни исходного уравнения равны: $x_1 = -2$, $x_2 = x_3 = 3$.

3. Кубические уравнения с действительными коэффициентами. Корни кубического уравнения с действительными коэффициентами могут быть как действительными, так и мнимыми. Число действительных корней зависит от знака дискриминанта.

Рассмотрим все три случая, которые могут представиться.

1°. $D > 0$. В этом случае под знаком квадратного корня в формуле Кардано находится отрицательное число и кубические корни извлекаются из двух сопряженных мнимых чисел. Пусть u_1 — какое-либо значение первого кубического корня. Тогда $\bar{u}_1$ будет одним из значений второго корня (поскольку $\bar{u}_1^3 = \bar{u}_1^3$). Так как значения кубических корней в формуле Кардано должны комбинироваться таким образом, чтобы их произведение равнялось действительному числу $-\frac{p}{3}$, то u_1

будет комбинироваться с $\bar{u}_1$. (В самом деле, $u_1 \bar{u}_1$ действительно, но ни $u_1 (\bar{u}_1 \omega) = (u_1 \bar{u}_1) \omega$, ни $u_1 (\bar{u}_1 \omega^2) = (u_1 \bar{u}_1) \omega^2$ не являются действительными числами.)

По формулам (7), учитывая, что $\omega^2 = \bar{\omega}$, находим:

$$\begin{aligned} x_1 &= u_1 + \bar{u}_1, \\ x_2 &= u_1 \omega + \bar{u}_1 \omega^2 = u_1 \omega + \bar{u}_1 \bar{\omega}, \\ x_3 &= u_1 \omega^2 + \bar{u}_1 \omega = u_1 \omega^2 + \bar{u}_1 \bar{\omega}^2, \end{aligned} \quad (10)$$

откуда видно, что все три корня действительны (и различны, поскольку $D \neq 0$).

Итак, если $D > 0$, то уравнение (1) имеет три различных действительных корня.

2°. $D < 0$. В этом случае под знаком квадратного корня в формуле Кардано находится положительное число и кубические корни извлекаются из двух различных действительных чисел. Пусть u_1 и v_1 — действительные значения этих корней. Тогда

$$\begin{aligned}x_1 &= u_1 + v_1, \\x_2 &= u_1\omega + v_1\omega^2, \\x_3 &= u_1\omega^2 + v_1\omega = \bar{x}_2.\end{aligned}\tag{11}$$

Так как $x_2 \neq x_3$, то x_2 и x_3 — сопряженные мнимые числа. Число x_1 , очевидно, действительное.

Итак, если $D < 0$, то уравнение (1) имеет один действительный и два сопряженных мнимых корня.

3°. $D = 0$. Из формул (9) следует, что если $D = 0$, то уравнение (1) имеет три действительных корня, два из которых (или все три) совпадают между собой.

Пример 2. Решим уравнение

$$x^3 - 9x^2 + 21x - 5 = 0.$$

Делая замену $x = y + 3$, получаем неполное уравнение

$$y^3 - 6y + 4 = 0,$$

в котором $p = -6$, $q = 4$ и

$$D = -27 \cdot 16 + 4 \cdot 216 = 432 > 0.$$

Следовательно, уравнение имеет три различных действительных корня.

Имеем:

$$\frac{q^2}{4} + \frac{p^3}{27} = -\frac{1}{108}D = -4,$$

так что по формуле Кардано

$$y = \sqrt[3]{-2 + 2i} + \sqrt[3]{-2 - 2i}.$$

Так как $-2 + 2i = 2\sqrt{2}\left(\cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4}\right)$, то одним из значений кубического корня из $-2 + 2i$ является

$$u_1 = \sqrt{2}\left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}\right) = 1 + i.$$

По формулам (10) находим:

$$y_1 = u_1 + \bar{u}_1 = 2,$$

$$y_2 = u_1\omega + \bar{u}_1\omega = -1 - \sqrt{3},$$

$$y_3 = u_1\omega^2 + \bar{u}_1\omega^2 = -1 + \sqrt{3}.$$

Корни исходного уравнения равны: $x_1 = 5$, $x_2 = 2 - \sqrt{3}$, $x_3 = 2 + \sqrt{3}$.

Пример 3. Решим уравнение

$$x^3 - 9x + 28 = 0.$$

Данное уравнение является неполным с $p = -9$, $q = 28$, $D = -108 \cdot 169 < 0$. Оно имеет один действительный и два сопряженных мнимых корня. Находим действительные значения кубических корней в формуле Кардано:

$$u_1 = \sqrt[3]{-14 + \sqrt{169}} = \sqrt[3]{-1} = -1,$$

$$v_1 = \sqrt[3]{-14 - \sqrt{169}} = \sqrt[3]{-27} = -3.$$

По формулам (11) находим корни данного уравнения:

$$x_1 = u_1 + v_1 = -4,$$

$$x_2 = u_1\omega + v_1\omega^2 = 2 + i\sqrt{3},$$

$$x_3 = \bar{x}_2 = 2 - i\sqrt{3}.$$

4. Решение уравнений четвертой степени. Изложим способ решения в радикалах уравнений четвертой степени, называемый способом Эйлера.

Рассмотрим неполное уравнение четвертой степени

$$x^4 + px^2 + qx + r = 0 \quad (12)$$

с произвольными комплексными коэффициентами p, q, r . Пусть x_1, x_2, x_3, x_4 — его корни. По формулам Виета,

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 &= p, \\ x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3 &= -q, \\ x_1x_2x_3x_4 &= r. \end{aligned} \quad (13)$$

В п. 6 § 2 гл. III (пример 5) мы показали, что числа $x_1x_2 + x_3x_4$, $x_1x_3 + x_2x_4$ и $x_1x_4 + x_2x_3$ являются корнями кубического уравнения

$$x^3 - px^2 - 4rx + (4pr - q^2) = 0. \quad (14)$$

Заметим, что

$$\begin{aligned} x_1x_2 + x_3x_4 &= \frac{1}{4}(x_1 + x_2 - x_3 - x_4)^2 - \frac{1}{4}(x_1 + x_2 + x_3 + \\ &+ x_4)^2 + (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = \\ &= \frac{1}{4}(x_1 + x_2 - x_3 - x_4)^2 + p. \end{aligned}$$

Аналогично

$$\begin{aligned} x_1x_3 + x_2x_4 &= \frac{1}{4}(x_1 - x_2 + x_3 - x_4)^2 + p, \\ x_1x_4 + x_2x_3 &= \frac{1}{4}(x_1 - x_2 - x_3 + x_4)^2 + p. \end{aligned}$$

Поэтому, если мы сделаем в уравнении (14) замену $x = y + p$, то полученное уравнение

$$y^3 + 2py^2 + (p^2 - 4r)y - q^2 = 0 \quad (15)$$

будет иметь своими корнями числа

$$\begin{aligned} y_1 &= \frac{1}{4}(x_1 + x_2 - x_3 - x_4)^2; \\ y_2 &= \frac{1}{4}(x_1 - x_2 + x_3 - x_4)^2, \\ y_3 &= \frac{1}{4}(x_1 - x_2 - x_3 + x_4)^2. \end{aligned} \quad (16)$$

Уравнение (15) называется *кубической резольвентой* уравнения (12). Его корни y_1, y_2, y_3 могут быть найдены способом, изложенным в п. 2. Нумерация корней y_1, y_2, y_3 при этом безразлична, так как выражения $x_1 + x_2 - x_3 - x_4, x_1 - x_2 + x_3 - x_4$ и $x_1 - x_2 - x_3 + x_4$ можно переставить произвольным образом, изменив нумерацию x_2, x_3 и x_4 .

Из формул (16) получаем, что

$$\begin{aligned} \frac{1}{2}(x_1 + x_2 - x_3 - x_4) &= u_1, \\ \frac{1}{2}(x_1 - x_2 + x_3 - x_4) &= u_2, \\ \frac{1}{2}(x_1 - x_2 - x_3 + x_4) &= u_3, \end{aligned} \quad (17)$$

где u_1, u_2, u_3 — квадратные корни из y_1, y_2, y_3 .

Поскольку квадратный корень из комплексного числа имеет два значения, необходимо уточнить, какие значения квадратных корней следует взять в формулах (17). В п. 2 § 2 гл. III (пример 1) мы доказали тождество

$$\begin{aligned} (x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4) = \\ = \sigma_1^3 - 4\sigma_1\sigma_2 + 8\sigma_3, \end{aligned}$$

где $\sigma_1, \sigma_2, \sigma_3$ — элементарные симметрические многочлены от x_1, x_2, x_3, x_4 . Для корней уравнения (12) имеем, в силу формул (13):

$$(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4) = -8q.$$

Отсюда следует, что

$$u_1 u_2 u_3 = -q. \quad (18)$$

Условие (18) оставляет четыре из восьми вариантов выбора значений квадратных корней из y_1, y_2, y_3 . Любой из этих четырех вариантов допустим, так как, перенумеровав подходящим образом x_1, x_2, x_3, x_4 , можно умножить на -1 любые два из выражений $x_1 + x_2 - x_3 - x_4, x_1 - x_2 + x_3 - x_4$ и $x_1 - x_2 - x_3 + x_4$, не изменив третьего. Например, если поменять номера у x_1 и x_2 и одно-

временно у x_3 и x_4 , то выражение $x_1 + x_2 - x_3 - x_4$ не изменится, в то время как остальные два умножатся на -1 .

Складывая равенства (17) и равенство $x_1 + x_2 + x_3 + x_4 = 0$, находим:

$$x_1 = \frac{1}{2}(u_1 + u_2 + u_3).$$

Аналогично находим:

$$x_2 = \frac{1}{2}(u_1 - u_2 - u_3),$$

$$x_3 = \frac{1}{2}(-u_1 + u_2 - u_3),$$

$$x_4 = \frac{1}{2}(-u_1 - u_2 + u_3).$$

Эти формулы можно объединить в одну:

$$x = \frac{1}{2}(V\overline{y_1} + V\overline{y_2} + V\overline{y_3}), \quad (19)$$

которую следует понимать таким образом, что значения квадратных корней выбираются всеми возможными способами, лишь бы их произведение равнялось $-q$.

Подставляя в (19) выражения для корней кубического уравнения (15), найденные при помощи формулы Кардано, можно получить явную формулу, выражающую корни уравнения (12) через его коэффициенты, которая, однако, столь громоздка, что выписывать ее не имеет смысла.

Выведенные выше формулы решения алгебраических уравнений третьей и четвертой степени естественным образом вытекают из теории Галуа. Они применимы к алгебраическим уравнениям с коэффициентами из любого (а не только числового) поля, лишь бы его характеристика не была равна 2 или 3. (Легко видеть, что формула для решения квадратного уравнения применима к уравнениям с коэффициентами из любого поля, характеристика которого не равна 2.) В рамках теории Галуа получается также доказательство того, что не существует общих формул для решения в радикалах уравнений выше четвертой степени.

Вопросы для самопроверки

1. Перечислите те значения n , для которых алгебраическое уравнение степени n может быть решено в радикалах в общем виде.
2. Что такое неполное алгебраическое уравнение?
3. Как решается в радикалах неполное кубическое уравнение?
4. Как комбинируются значения кубических корней в формуле Кардано?
5. Чему равен дискриминант кубического многочлена $x^3 + px + q$?
6. Непосредственно из формулы Кардано выведите, что многочлен $x^3 + px + q$ имеет кратные корни тогда и только тогда, когда его дискриминант равен нулю.

7. Как по дискриминанту определяется число действительных корней кубического уравнения с действительными коэффициентами?

8. В чем состоит способ Эйлера решения уравнения четвертой степени?

9. Что такое кубическая резольвента неполного уравнения четвертой степени?

Упражнения

1. Пользуясь формулой Кардано, решите уравнения:

а) $x^3 - 6x + 9 = 0$;

б) $x^3 + 9x^2 + 18x + 28 = 0$;

в) $x^3 + 6x + 2 = 0$.

2. Пользуясь формулой Кардано, найдите с точностью до 0,01 действительный корень уравнений:

а) $x^3 - 2x - 5 = 0$;

б) $x^3 + 2x - 30 = 0$.

МНОГОЧЛЕНЫ НАД $\mathbb{Q}$. АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ С РАЦИОНАЛЬНЫМИ КОЭФФИЦИЕНТАМИ

§ 1. РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ В КОЛЬЦЕ МНОГОЧЛЕНОВ С РАЦИОНАЛЬНЫМИ КОЭФФИЦИЕНТАМИ

Кольцо $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами, как и кольцо многочленов над произвольным полем, является евклидовым кольцом, и в нем справедлива теорема об однозначном разложении на неприводимые (простые) множители (теорема 1 § 2 гл. II). Однако, в отличие от многочленов над полем $\mathbb{C}$ или над полем $\mathbb{R}$, описание неприводимых многочленов над полем $\mathbb{Q}$ не так просто. В этом отношении кольцо $\mathbb{Q}[x]$ больше похоже на кольцо $\mathbb{Z}$ целых чисел. Подобно тому как существуют сколь угодно большие простые числа, в кольце $\mathbb{Q}[x]$, как будет показано ниже, существуют неприводимые многочлены сколь угодно высокой степени.

1. Рациональные корни. Отыскание рациональных корней многочлена с рациональными коэффициентами, очевидно, равносильно отысканию линейных множителей в его разложении на неприводимые множители в кольце $\mathbb{Q}[x]$. Так как всякий многочлен с рациональными коэффициентами может быть представлен в виде $\frac{a}{b}f(x)$, где $a, b \in \mathbb{Z}$, а $f(x)$ — многочлен с целыми коэффициентами, то достаточно научиться находить рациональные корни многочленов с целыми коэффициентами.

Существует простой способ нахождения рациональных корней. Он основан на следующей теореме:

Т е о р е м а 1. Пусть $f(x)$ — многочлен с целыми коэффициентами. Если рациональное число $x_0 = \frac{p}{q}$, где p и q — взаимно простые целые числа, является корнем многочлена $f(x)$, то q делит старший коэффициент этого многочлена, а p делит его свободный член.

Так как каждое целое число, отличное от нуля, имеет лишь конечное число делителей, то теорема позволяет путем конечного перебора найти все рациональные корни.

Д о к а з а т е л ь с т в о. Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

$$(a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{Z}).$$

Запишем условие того, что $x_0 = \frac{p}{q}$ является корнем многочлена $f(x)$:

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

или, после умножения на q^n

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

Так как все слагаемые в левой части этого равенства, кроме первого, делятся на q , то и первое слагаемое должно делиться на q . Поскольку p и q , согласно предположению, взаимно просты, отсюда следует, что a_0 делится на q . Аналогично доказывается, что a_n делится на p .

Пример 1. Найдем все рациональные корни уравнения

$$5x^4 - \frac{10}{3}x^3 + 5x^2 + \frac{5}{3}x - \frac{10}{3} = 0.$$

После умножения на $\frac{3}{5}$ получаем уравнение

$$3x^4 - 2x^3 + 3x^2 + x - 2 = 0,$$

в левой части которого стоит многочлен с целыми коэффициентами. Делителями его старшего коэффициента являются числа $\pm 1, \pm 3$, делителями свободного члена — числа $\pm 1, \pm 2$. Следовательно, рациональными корнями этого уравнения могут быть только числа $\pm 1, \pm 2, \pm \frac{1}{3}, \pm \frac{2}{3}$. Испытывая их, находим, что данное уравнение имеет один рациональный корень, а именно $\frac{2}{3}$.

Особенно простым является случай, когда старший коэффициент многочлена $f(x)$ равен единице. Рациональное число $x_0 = \frac{p}{q}$ может быть его корнем, только если $q = \pm 1$. Следовательно, x_0 — целое число, которое должно быть делителем свободного члена. Таким образом, получаем такое следствие:

С л е д с т в и е. Если $f(x)$ — нормированный многочлен с целыми коэффициентами, то все его рациональные корни суть целые числа, являющиеся делителями свободного члена.

Пример 2. Найдем все рациональные корни уравнения

$$x^4 - x^2 + x - 10 = 0.$$

Испытывая делители свободного члена, а именно числа $\pm 1, \pm 2, \pm 5, \pm 10$, находим, что единственный рациональный корень данного уравнения равен -2 .

В более сложных примерах, когда старший коэффициент и свободный член многочлена $f(x)$ имеют много делителей, отыскание всех рациональных корней указанным выше способом довольно затруднительно. Чтобы облегчить вычисления, можно воспользоваться следующим свойством любого рационального корня

$x_0 = \frac{p}{q}$ (p и q — взаимно простые целые числа): если c — любое целое число, то $p - cq$ делит $f(c)$. Для доказательства этого свойства разложим многочлен $f(x)$ по степеням $x - c = y$. При этом мы получим некоторый многочлен $g(y)$ с целыми коэффициентами. Число $y_0 = x_0 - c = \frac{p - cq}{q}$ является корнем многочлена $g(y)$. Так как свободный член этого многочлена равен $f(c)$, то, согласно теореме 1, $p - cq$ делит $f(c)$, что и требовалось доказать.

Пример 3. Найдем все рациональные корни уравнения

$$12x^5 + x^4 + x^3 - x - 165 = 0.$$

Пусть $x_0 = \frac{p}{q}$ (p и q — взаимно простые целые числа) — корень данного уравнения. Можно считать, что $q > 0$. Согласно теореме 1, p должно делить 165, а q должно делить 12, т. е. для p и q имеются следующие возможности:

$$p = \pm 1, \pm 3, \pm 5, \pm 11, \pm 15, \pm 33, \pm 55, \pm 165, \\ q = 1, 2, 3, 4, 6, 12.$$

Учитывая, что p и q взаимно просты, получаем все же 72 допустимые комбинации. Вычислим значения левой части уравнения в точках $\pm 1, \pm 2$:

	12	1	1	0	-1	-165
1	12	13	14	14	13	-152
-1	12	-11	12	-12	11	-176
2	12	25	51	102	203	241
-2	12	-23	47	-94	187	-539

Во-первых, мы видим, что проверяемые числа не являются корнями; во-вторых, получаем следующие необходимые условия для p и q :

$$p - q \mid 152, p + q \mid 176, p - 2q \mid 241, p + 2q \mid 539.$$

Особенно удобно условие $p - 2q \mid 241$, поскольку 241 — простое число. Так как во всех допустимых комбинациях $|p - 2q| < 241$, то отсюда следует, что $p - 2q = \pm 1$, т. е.

$$p = 2q \pm 1.$$

Этому условию удовлетворяют следующие 6 пар:

$\frac{p}{q}$	1	3	3	5	5	11
q	1	1	2	2	3	6

Из них условиям $p - q \mid 152, p + q \mid 176, p + 2q \mid 539$ удовлетворяет только пара (5; 3). Проверка показывает, что $x_0 = \frac{5}{3}$ является корнем уравнения.

Таким образом, данное уравнение имеет один рациональный корень $\frac{5}{3}$.

2. Неприводимые многочлены. Несмотря на то что, как уже отмечалось, простого описания всех неприводимых многочленов в кольце $\mathbb{Q}[x]$ не существует, можно указать некоторые легко проверяемые достаточные условия того, что данный многочлен неприводим. Для этой цели используется прежде всего следующая теорема, являющаяся частным случаем теоремы I из § 3 гл. II:

Теорема 2. Если многочлен с целыми коэффициентами не может быть разложен в произведение двух многочленов меньшей степени в кольце $\mathbb{Z}[x]$, то он не может быть разложен в произведение двух многочленов меньшей степени и в кольце $\mathbb{Q}[x]$.

В самом деле, кольцо целых чисел факториально, и поэтому к кольцу $\mathbb{Z}[x]$ применима вся теория, развитая в § 3 гл. II, и, в частности, теорема 1 из этого параграфа.

Если исключить тривиальный случай, когда данный многочлен имеет нулевую степень, то можно сказать, что многочлен, удовлетворяющий условию теоремы, будет неприводим в кольце $\mathbb{Q}[x]$.

С помощью этой теоремы можно получить различные достаточные условия неприводимости многочлена в кольце $\mathbb{Q}[x]$. Наиболее

простым из них является так называемый к р и т е р и й Э й з е н ш т е й н а:

Пусть $f(x)$ — многочлен с целыми коэффициентами. Если существует такое простое число p , что старший коэффициент многочлена $f(x)$ не делится на p , все остальные коэффициенты делятся на p , а свободный член, делясь на p , не делится на p^2 , то многочлен $f(x)$ неприводим в кольце $\mathbb{Q}[x]$.

Для доказательства запишем данный многочлен по возрастающим степеням x :

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

Предположим, что он разлагается в произведение двух многочленов с целыми коэффициентами:

$$g(x) = b_0 + b_1x + \dots + b_mx^m,$$

$$h(x) = c_0 + c_1x + \dots + c_lx^l,$$

причем $0 < m < n$ и $0 < l < n$. Тогда при любом k

$$a_k = b_0c_k + b_1c_{k-1} + \dots + b_kc_0$$

если считать, как обычно, что $b_s = 0$ при $s > m$ и $c_t = 0$ при $t > l$. Среди коэффициентов многочлена $g(x)$ (аналогично $h(x)$) обязательно найдутся такие, которые не делятся на p ; в противном случае и все коэффициенты многочлена $f(x)$ делились бы на p вопреки условию. Пусть b_s — первый из коэффициентов многочлена $g(x)$, не делящихся на p , и аналогично c_t — первый из коэффициентов многочлена $h(x)$, не делящихся на p . Тогда

$$a_{s+t} = b_0c_{s+t} + b_1c_{s+t-1} + \dots + b_sc_t + \dots + b_{s+t}c_0$$

также не делится на p , поскольку все слагаемые, кроме b_sc_t , делятся на p , а b_sc_t не делится. Из всех коэффициентов многочлена $f(x)$, согласно предположению, только a_n не делится на p . Следовательно, $s+t = n$. Так как $n = m+l$, а $s \leq m$ и $t \leq l$, то отсюда вытекает, что $s = m$ и $t = l$. Стало быть, $s, t > 0$, т. е. b_0 и c_0 делятся на p ; но тогда $a_0 = b_0c_0$ делится на p^2 , что противоречит предположению.

Таким образом, многочлен $f(x)$ не может быть разложен в произведение двух многочленов меньшей степени в кольце $\mathbb{Z}[x]$. Согласно теореме 2, многочлен $f(x)$ неприводим в кольце $\mathbb{Q}[x]$, что и требовалось доказать.

Доказательство критерия Эйзенштейна может быть изложено более изящно, если воспользоваться «редукцией по модулю p » (см. п. 7 § 1 гл. I). Рассмотрим многочлен $f(x) \in \mathbb{Z}[x]$, удовлетворяющий условиям критерия Эйзенштейна, и предположим, что он разлагается в произведение двух многочленов меньшей степени с целыми коэффициентами:

$$f(x) = g(x)h(x).$$

Применяя к этому равенству редукцию по модулю p , получаем:

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x).$$

Так как все коэффициенты многочлена $f(x)$, кроме старшего, делятся на p , то $\bar{f}(x) = ax^n$, где $a \in \mathbb{Z}_p$, $a \neq 0$. Очевидно, что все делители многочлена x^n ассоциированы со степенями x . Следовательно, $\bar{g}(x) = bx^m$, $\bar{h}(x) = cx^l$, где $0 < m < n$, $m + l = n$. Это означает, что у каждого из многочленов $g(x)$, $h(x)$ все коэффициенты, кроме старшего, делятся на p . В частности, их свободные члены делятся на p . Далее, как и выше, замечаем, что свободный член многочлена $f(x)$ равен произведению свободных членов многочленов $g(x)$ и $h(x)$ и, следовательно, делится на p^2 ; но это противоречит условию.

С л е д с т в и е. В кольце $\mathbb{Q}[x]$ существуют неприводимые многочлены любой степени.

В самом деле, применяя критерий Эйзенштейна для $p = 2$, мы видим, что многочлен $x^n - 2$ неприводим в кольце $\mathbb{Q}[x]$ при любом n .

П р и м е р 4. Докажем неприводимость многочлена $5x^4 + 30x - 12$ в кольце $\mathbb{Q}[x]$.

Для доказательства применяем критерий Эйзенштейна, взяв $p = 3$.

П р и м е р 5. Докажем, что для любого простого p «многочлен деления круга»

$$\psi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

неприводим в кольце $\mathbb{Q}[x]$.

(Название «многочлен деления круга» объясняется тем, что корни этого многочлена, будучи корнями p -й степени из единицы, вместе с самой единицей делят единичную окружность в комплексной плоскости на p равных частей.)

В данном случае критерий Эйзенштейна не может быть применен непосредственно к многочлену $\psi_p(x)$. Однако после замены $x = y + 1$ получаем многочлен

$$\begin{aligned} \varphi_p(y) &= \psi_p(y + 1) = \frac{(y + 1)^p - 1}{(y + 1) - 1} = \frac{(y + 1)^p - 1}{y} = \\ &= y^{p-1} + C_p^1 y^{p-2} + C_p^2 y^{p-3} + \dots + C_p^{p-2} y + C_p^{p-1}, \end{aligned}$$

к которому уже можно применить критерий Эйзенштейна. В самом деле, поскольку p — простое число, то при любом $k = 1, 2, \dots, p - 1$ коэффициент $C_p^k = \frac{p(p-1)\dots(p-k+1)}{1 \cdot 2 \cdot \dots \cdot k}$ делится на p ; кроме того, свободный член $C_p^{p-1} = C_p^1 = p$ не делится на p^2 . Стало быть, многочлен $\varphi_p(y)$ неприводим в кольце $\mathbb{Q}[y]$. Отсюда следует неприводимость и самого многочлена деления круга, так как если бы он допускал разложение в произведение двух многочленов меньшей степени, то после замены $x = y + 1$ мы получили бы такое же разложение для многочлена $\varphi_p(y)$.

Критерий Эйзенштейна, как и некоторые другие достаточные условия неприводимости, применим лишь к узкому классу неприводимых многочленов. Имеется, однако, способ, принадлежащий Кронекеру, который позволяет в принципе для любого многочлена

с рациональными коэффициентами установить, приводим он или неприводим в кольце $\mathbb{Q}[x]$, хотя и требует довольно больших вычислений.

Способ Кронекера основывается на следующих соображениях. Пусть $f(x)$ — многочлен степени n с целыми коэффициентами, не имеющий целых корней. Предположим, что он разлагается в произведение двух многочленов меньшей степени с целыми коэффициентами:

$$f(x) = g(x)h(x).$$

Степень одного из этих многочленов, скажем $g(x)$, не превосходит $m = \left\lfloor \frac{n}{2} \right\rfloor$.

Будем придавать x различные целые значения $x_0, x_1, \dots, x_m$. Из равенства $f(x_i) = g(x_i)h(x_i)$ следует, что $g(x_i)$ делит $f(x_i)$ ($i = 0, 1, \dots, m$). Многочлен $g(x)$ однозначно определяется своими значениями в точках $x_0, x_1, \dots, x_m$. Составляя всевозможные наборы делителей $d_0, d_1, \dots, d_m$ целых чисел $f(x_0), f(x_1), \dots, f(x_m)$ и вычисляя для каждого такого набора интерполяционный многочлен степени $\leq m$, принимающий в точках $x_0, x_1, \dots, x_m$ соответственно значения $d_0, d_1, \dots, d_m$, можно найти всех кандидатов на роль многочлена $g(x)$ (их будет конечное число). Интерполяционные многочлены с дробными коэффициентами следует сразу отбросить. Испытав оставшиеся многочлены, можно определить, имеются ли среди них делители многочлена $f(x)$, в зависимости от чего и будет решен вопрос о приводимости $f(x)$ в кольце $\mathbb{Q}[x]$.

Вопросы для самопроверки

1. Из чего следует единственность разложения на множители в кольце многочленов с рациональными коэффициентами?
2. Как находятся рациональные корни многочлена с рациональными коэффициентами?
3. Пусть $f(x)$ — нормированный многочлен с целыми коэффициентами. Докажите, что всякий рациональный корень уравнения $f(x) = 0$ является целым.
4. Сформулируйте и докажите критерий Эйзенштейна.
5. Докажите неприводимость многочлена деления круга $\psi_p(x)$, где p — простое число.

Упражнения

1. Найдите все рациональные корни уравнения:

- а) $x^3 - 6x^2 + 15x - 14 = 0$;
- б) $x^4 - 2x^3 - 8x^2 + 13x - 24 = 0$;
- в) $x^5 - 7x^3 - 12x^2 + 6x + 36 = 0$;
- г) $6x^4 + 19x^3 - 7x^2 - 26x + 12 = 0$;
- д) $24x^4 - 42x^3 - 77x^2 + 56x + 60 = 0$;
- е) $10x^4 - 13x^3 + 15x^2 - 18x - 24 = 0$.

2. Докажите неприводимость многочлена в кольце $\mathbb{Q}[x]$:

- а) $x^4 + 8x^3 + 12x^2 - 6x + 2$;
- б) $x^5 - 12x^3 + 36x - 12$.

§ 2. АЛГЕБРАИЧЕСКИЕ ЧИСЛА

1. Определения. Комплексное число называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами, и *трансцендентным* в противном случае. В частности, алгебраическими являются рациональные числа (корни многочленов первой степени), всякое число вида $\sqrt[n]{a}$ (корень многочлена $x^n - a$), где a — рациональное число, число i (корень многочлена $x^2 + 1$). Сумма и произведение алгебраических чисел, как мы увидим ниже, также будут алгебраическими числами. Так, например, $\sqrt{2} + i$ — это корень многочлена

$$((x - i)^2 - 2)((x + i)^2 - 2) = x^4 - 2x^2 + 9.$$

Каждое алгебраическое число α является корнем многих многочленов с рациональными коэффициентами. Обозначим через I_α совокупность всех многочленов из $\mathbb{Q}[x]$, имеющих α корнем. Нетрудно видеть, что I_α — идеал в $\mathbb{Q}[x]$: если $f \in I_\alpha$, а h — произвольный многочлен из $\mathbb{Q}[x]$, то $hf \in I_\alpha$, и если $f \in I_\alpha$, $g \in I_\alpha$, то $f \mp g \in I_\alpha$. Так как $\mathbb{Q}[x]$ — кольцо главных идеалов, то идеал I_α порождается некоторым (определенным с точностью до числового множителя) многочленом p_α , который называется *минимальным многочленом числа α* и может быть охарактеризован как многочлен наименьшей степени в идеале I_α .

Многочлен p_α неприводим в кольце $\mathbb{Q}[x]$. В самом деле, если бы он разлагался в этом кольце в произведение двух многочленов меньшей степени, то число α было бы корнем одного из этих многочленов и многочлен p_α не был бы многочленом наименьшей степени в идеале I_α .

Многочлен p_α — единственный (с точностью до числового множителя) неприводимый многочлен в идеале I_α , поскольку все многочлены из идеала I_α делятся на p_α .

Полезно отметить, что минимальный многочлен не имеет кратных корней; в частности, само число α является его простым корнем. В самом деле, будучи неприводим в кольце $\mathbb{Q}[x]$, многочлен p_α взаимно прост со своей производной. Последнее свойство сохраняется и в кольце $\mathbb{C}[x]$ (см. п. 3 § 1 гл. II). Следовательно, многочлен p_α не имеет кратных корней в поле $\mathbb{C}$ (см. § 2 гл. II).

Степень многочлена p_α называется *степенью алгебраического числа α* . Согласно этому определению, алгебраическими числами первой степени будут рациональные числа, алгебраическими числами второй степени — корни квадратных уравнений с рациональными коэффициентами (не являющиеся рациональными числами). Первообразный корень n -й степени из единицы при простом n является алгебраическим числом степени $n - 1$. В самом деле, он является корнем многочлена

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + x + 1,$$

неприводимость которого в кольце $\mathbb{Q}[x]$ была доказана в § 1.

2. Существование трансцендентных чисел. Множество алгебраических чисел намного шире, чем множество рациональных чисел. Естественно спросить, существуют ли вообще неалгебраические, т. е. трансцендентные числа. Оказывается, что существуют. Более того, в некотором смысле «почти все» числа трансцендентны. Известно, что множество всех действительных и тем более множество всех комплексных чисел несчетно. Если удастся доказать, что *множество всех алгебраических чисел счетно*, то тем самым мы докажем, что *множество трансцендентных чисел* не только непусто, но и *несчетно*. В самом деле, если бы оно было счетно, то и множество всех чисел было бы счетно как объединение двух счетных множеств.

Докажем счетность множества всех алгебраических чисел. Для каждого алгебраического числа α выберем минимальный многочлен p_α с целыми и взаимно простыми в совокупности коэффициентами (это можно сделать, так как минимальный многочлен определен с точностью до умножения на рациональное число, отличное от нуля). Назовем *высотой* числа α сумму абсолютных величин коэффициентов многочлена p_α плюс его степень. *Имеется лишь конечное число алгебраических чисел данной высоты m .* В самом деле, из определения высоты ясно, что каждое алгебраическое число высоты m является корнем многочлена степени не выше m с целыми коэффициентами, по абсолютной величине не превосходящими m . Поскольку число таких многочленов конечно и каждый многочлен имеет конечное число корней, то и алгебраических чисел высоты m имеется лишь конечное число. Расположим все алгебраические числа в порядке возрастания высоты, причем числа одинаковой высоты упорядочим между собой произвольным образом. Это и даст нам возможность занумеровать все алгебраические числа.

Первые примеры трансцендентных чисел были приведены в 1844 г. французским математиком Лиувиллем. Он исходил из того, что алгебраические иррациональные числа не допускают «слишком хороших» приближений рациональными числами. А именно имеет место следующая теорема:

Теорема Лиувилля. *Для всякого действительного алгебраического числа α степени $n > 1$ существует такое положительное число ε , что при любых целых p и q ($q > 0$)*

$$\left| \alpha - \frac{p}{q} \right| > \frac{\varepsilon}{q^n}. \quad (1)$$

Доказательство. Пусть

$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ — многочлен степени n с целыми коэффициентами, корнем которого является α . Представим $f(x)$ в виде

$$f(x) = (x - \alpha) f_1(x),$$

где $f_1(x)$ — многочлен, не обращающийся в нуль в точке α . Для любых целых p и q ($q > 0$) имеем тогда:

$$\frac{p}{q} - \alpha = \frac{f\left(\frac{p}{q}\right)}{f_1\left(\frac{p}{q}\right)} = \frac{a_0 p^n + a_1 p^{n-1} q + \dots + a_{n-1} p q^{n-1} + a_n q^n}{q^n f_1\left(\frac{p}{q}\right)}.$$

Числитель последней дроби — целое число, отличное от нуля (поскольку многочлен $f(x)$ не может иметь рациональных корней). Следовательно,

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q^n \left| f_1\left(\frac{p}{q}\right) \right|}.$$

В силу непрерывности функции $f_1(x)$ существует такое $\delta > 0$, что $|f_1(x)| < 2|f_1(\alpha)|$ при $|\alpha - x| \leq \delta$. Положим $\varepsilon = \min\left\{\frac{1}{2|f_1(\alpha)|}, \delta\right\}$. Тогда при $|\alpha - \frac{p}{q}| \leq \varepsilon$ имеем:

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{2q^n |f_1(\alpha)|} \geq \frac{\varepsilon}{q^n},$$

а при $|\alpha - \frac{p}{q}| > \delta$ —

$$\left| \alpha - \frac{p}{q} \right| > \delta \geq \frac{\varepsilon}{q^n},$$

т. е. неравенство (1) выполняется во всех случаях. Теорема доказана.

Заметим, что условие $n > 1$ в формулировке теоремы существенно. Действительно, если $n = 1$, то это означает, что число α рационально: $\alpha = \frac{p}{q}$, где p и q — целые числа. В этом случае, очевидно, $\left| \alpha - \frac{p}{q} \right| \leq \frac{\varepsilon}{q^n}$, каково бы ни было $\varepsilon > 0$.

Согласно теореме Лиувилля, иррациональное число α заведомо будет трансцендентным, если для любого $\varepsilon > 0$ и для любого натурального n найдутся такие числа p_n и q_n ($q_n > 0$), что

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{\varepsilon}{q_n^{n^*}}. \quad (2)$$

Рассмотрим, например, число

$$\alpha = \frac{1}{2!} + \frac{1}{2^2!} + \frac{1}{2^3!} + \dots \quad (3)$$

(сумма бесконечного ряда). Покажем прежде всего, что оно иррационально. Для любого n сумма первых n членов ряда (3) есть рациональное число $\frac{p_n}{q_n}$, где $q_n = 2^{n!}$, а p_n нечетно. Остаток ряда r_n меньше, чем

$$\frac{1}{2^{(n+1)!}} \left(1 + \frac{1}{2} + \frac{1}{4} + \dots \right) = \frac{2}{2^{(n+1)!}} = \frac{2}{q_n^{n+1}}.$$

Для любого натурального числа q можно найти такое n , что $q_n > 2q$. Имеем:

$$q\alpha = \frac{qp_n}{q_n} + qr_n.$$

Первое слагаемое в этой сумме не может быть целым, так как p_n и q_n взаимно просты, а $q < q_n$. Следовательно, его дробная часть не меньше, чем $\frac{1}{q_n}$. Посколь-

ку второе слагаемое меньше, чем $\frac{2q}{q_n^{n+1}} < \frac{1}{q_n^n} \leq \frac{1}{q_n}$, то, значит, и сумма не может быть целой. Итак, $q\alpha$ не является целым числом ни при каком натуральном q . Это означает, что α иррационально. Далее, для любого $\varepsilon > 0$ из неравенства

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{2}{q_n^{n+1}}$$

следует неравенство (2) при всех достаточно больших n (а именно таких, что $\frac{2}{q_n} < \varepsilon$). Следовательно, α трансцендентно.

Метод Лиувилля не позволяет, однако, доказать трансцендентность многих чисел, играющих важную роль в математике, таких, например, как числа e и π . Трансцендентность числа e была доказана в 1873 г. французским математиком Эрмитом. Развивая методы Эрмита, немецкий математик Линдеман (ученик Вейерштрасса) в 1882 г. доказал трансцендентность числа π и многих других чисел. Советский математик А. О. Гельфонд в 1936 г. доказал трансцендентность всех чисел вида α^β , где α и β — алгебраические числа, причем $\alpha \neq 0, 1$, а β иррационально*. (Таково, например, число $2^{\sqrt{2}}$.) Вопрос о трансцендентности таких чисел составлял содержание седьмой проблемы Гильберта, поставленной в 1900 г. на Международном конгрессе математиков.

3. Числа, алгебраические над заданным полем P . Кольцо $P[\alpha]$. В этом и следующих пунктах мы будем рассматривать числовые кольца и числовые поля, т. е. подкольца и подполя поля C комплексных чисел

Пусть P — числовое поле и α — произвольное число (вообще говоря, не принадлежащее полю P). Обозначим через $P[\alpha]$ совокупность всех чисел, которые могут быть получены из чисел, принадлежащих полю P , и числа α с помощью операций сложения и умножения. Ясно, что:

1) $P \subset P[\alpha]$;

2) $\alpha \in P[\alpha]$;

3) если числа γ и δ принадлежат $P[\alpha]$, то числа $\gamma + \delta$, $\gamma - \delta$ и $\gamma\delta$ также принадлежат $P[\alpha]$.

Поясним, что $\gamma - \delta \in P[\alpha]$ в силу того, что $\gamma - \delta = \gamma + (-1)\delta$ и $-1 \in P$.

Свойства 1—3 означают, что $P[\alpha]$ есть числовое кольцо, содержащее поле P и число α . Кроме того, из определения этого кольца следует, что $P[\alpha]$ — наименьшее числовое кольцо, содержащее P и α , в том смысле, что оно содержится в любом числовом кольце, содержащем P и α .

* Числа α и β не обязательно действительны. Возведение любого комплексного числа, отличного от нуля, в любую комплексную степень определяется в теории функций комплексной переменной. Эта операция многозначна (подобно операции извлечения корня из комплексного числа). Например, $(-1)^i$ имеет значения $e^{(2k+1)\pi}$, где $k = 0, \pm 1, \pm 2, \dots$. Результат А. О. Гельфонда следует понимать таким образом, что любое из значений α^β трансцендентно. В частности, трансцендентно число e^π , которое является одним из значений $(-1)^i$

Очевидно, что $P[\alpha]$ содержит все числа вида

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_m\alpha^m, \\ (m — \text{любое, } c_0, c_1, c_2, \dots, c_m \in P). \quad (4)$$

Непосредственно проверяется, что сумма, разность и произведение чисел вида (4) также могут быть представлены в таком виде. Это означает, что совокупность K чисел вида (4) является числовым кольцом. Далее ясно, что K содержит все элементы поля P (которые получаются при $m = 0$) и число α . Так как $P[\alpha]$ — наименьшее кольцо, содержащее P и α , то $P[\alpha] \subset K$. С другой стороны, очевидно, что $K \subset P[\alpha]$. Следовательно, K совпадает с $P[\alpha]$. Таким образом, *кольцо $P[\alpha]$ есть в точности множество всех чисел вида (4).*

Вообще говоря, число из кольца $P[\alpha]$ представляется в виде (4) неоднозначно. Для того чтобы выяснить, когда такое представление однозначно (а также чтобы придать точный смысл этому понятию), заметим, что выражение (4) есть не что иное, как значение в точке α многочлена

$$c_0 + c_1x + c_2x^2 + \dots + c_mx^m \in P[x].$$

Могут существовать различные многочлены $f_1, f_2 \in P[x]$, принимающие в точке α одно и то же значение. Это и будет означать, что число $\beta = f_1(\alpha) = f_2(\alpha)$ представляется в виде (4) неоднозначно. Так как равенство $f_1(\alpha) = f_2(\alpha)$ равносильно тому, что $(f_1 - f_2)(\alpha) = 0$, то однозначность представления любого числа из кольца $P[\alpha]$ в виде (4) имеет место тогда и только тогда, когда число α не является корнем никакого ненулевого многочлена с коэффициентами из поля P .

Введем по аналогии со случаем $P = \mathbb{Q}$ следующие определения.

Число α называется *алгебраическим* над P , если оно является корнем ненулевого многочлена из $P[x]$, и *трансцендентным* над P в противном случае. В частности, числа алгебраические (соответственно трансцендентные) над $\mathbb{Q}$ — это просто алгебраические (соответственно трансцендентные) числа в смысле определения, данного в п. 1.

Из сказанного ясно, что *если α — трансцендентное над P число, то любое число β из кольца $P[\alpha]$ однозначно представляется в виде (4), т. е. существует единственный многочлен $f \in P[x]$ такой, что $\beta = f(\alpha)$.*

Пусть α — число, алгебраическое над P . Тогда, как и в случае $P = \mathbb{Q}$, совокупность I_α всех многочленов из $P[x]$, имеющих α своим корнем, является ненулевым идеалом в кольце $P[x]$. Образующий многочлен p_α этого идеала (определенный с точностью до ассоциированности) называется *минимальным многочленом числа α над P* , а его степень — *степенью числа α над P* .

Так же, как и в случае $P = \mathbb{Q}$, доказывается, что p_α — единственный (с точностью до ассоциированности) многочлен в идеале I_α ,

неприводимый в кольце $P[x]$. Вместе с тем p_α является многочленом наименьшей степени в идеале I_α .

Для двух многочленов $f_1, f_2 \in P[x]$ равенство $f_1(\alpha) = f_2(\alpha)$ имеет место тогда и только тогда, когда $f_1 - f_2 \in I_\alpha$. Согласно определению многочлена p_α , это равносильно тому, что $f_1 - f_2$ делится на p_α .

Среди всех многочленов, разность которых с данным многочленом f делится на p_α , имеется ровно один многочлен, степень которого меньше степени p_α , а именно остаток от деления f на p_α . Отсюда следует, что если α — алгебраическое над P число, то любое число из кольца $P[\alpha]$ однозначно представляется в виде

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1} \quad (c_0, c_1, c_2, \dots, c_{n-1} \in P), \quad (5)$$

где n — степень многочлена p_α , т. е. степень числа α над полем P .

Примеры. 1°. Всякое число α , принадлежащее полю P , является алгебраическим числом первой степени над P , так как является корнем многочлена $x - \alpha \in P[x]$. Очевидно, что в этом (и только в этом) случае $P[\alpha] = P$.

2°. Квадратный корень из числа $\delta \in P$ будучи корнем многочлена $x^2 - \delta$ является алгебраическим числом второй степени над P , если только он не принадлежит P . В этом случае всякое число из кольца $P[\sqrt{\delta}]$ однозначно представляется в виде $a + b\sqrt{\delta}$, где $a, b \in P$. Легко получить следующие формулы для суммы и произведения двух таких чисел:

$$(a + b\sqrt{\delta}) + (c + d\sqrt{\delta}) = (a + c) + (b + d)\sqrt{\delta}, \quad (6)$$

$$(a + b\sqrt{\delta}) + (c + d\sqrt{\delta}) = (ac + bd\delta) + (ad + bc)\sqrt{\delta}. \quad (7)$$

В частном случае, когда $P = \mathbf{R}$, $\delta = -1$, кольцо $P[\sqrt{\delta}] = \mathbf{R}[i]$ совпадает с полем комплексных чисел и формулы (6) и (7) превращаются в известные формулы для суммы и произведения двух комплексных чисел.

3°. Всякое комплексное число α является алгебраическим числом не выше второй степени над полем $\mathbf{R}$ действительных чисел, так как является корнем многочлена $x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$, коэффициенты которого действительны. Если $\alpha \notin \mathbf{R}$, то кольцо $\mathbf{R}[\alpha]$ совпадает с полем $\mathbf{C}$ (проверьте!).

4°. Пусть n — простое число. Обозначим через ω какой-нибудь первообразный корень n -й степени из единицы. Как было отмечено в п. 1, он является алгебраическим числом степени $n - 1$ над полем $\mathbf{Q}$. Отсюда следует, что всякое число из кольца $\mathbf{Q}[x]$ однозначно представляется в виде

$$c_0 + c_1\omega + c_2\omega^2 + \dots + c_{n-2}\omega^{n-2},$$

где $c_0, c_1, c_2, \dots, c_{n-2} \in \mathbf{Q}$.

4. Простые расширения числовых полей. Пусть P , как и в п. 1, — произвольное числовое поле и α — любое комплексное число. Обозначим через $P(\alpha)$ поле отношений кольца $P[\alpha]$ в поле C , т. е. совокупность всех чисел вида $\frac{a}{b}$, где $a, b \in P[\alpha]$, $b \neq 0$ (см. АТЧ III, п. 5 § 3 гл. II).

Говорят, что $P(\alpha)$ есть *простое расширение поля P* , получаемое *присоединением числа α* (хотя, разумеется, присоединяется не только это число).

Поле $P(\alpha)$ называется *простым алгебраическим расширением поля P* , если α — число, алгебраическое над P , и *простым трансцендентным расширением поля P* , если α трансцендентно над P .

Имеет место следующая теорема:

Теорема 1. Если α — алгебраическое над P число, то $P(\alpha) = P[\alpha]$.

Доказательство. Пусть $p_\alpha \in P[x]$ — минимальный многочлен числа α над полем P . Любой элемент поля $P(\alpha)$ представляется в виде $\frac{f(\alpha)}{g(\alpha)}$, где $f, g \in P[x]$, причем $g(\alpha) \neq 0$. Из условия $g(\alpha) \neq 0$ следует, что многочлен g не делится на p_α и, значит, взаимно прост с p_α (напомним, что p_α — неприводимый многочлен). Следовательно, существуют такие многочлены $u, v \in P[x]$, что

$$ug + vp_\alpha = f$$

(см. теорему 3 § 1 гл. II). Подставляя в это равенство $x = \alpha$, находим:

$$u(\alpha)g(\alpha) = f(\alpha),$$

откуда

$$\frac{f(\alpha)}{g(\alpha)} = u(\alpha) \in P[\alpha].$$

Таким образом, любой элемент поля $P(\alpha)$ принадлежит $P[\alpha]$. Тем самым теорема доказана.

Процедура представления дроби $\frac{f(\alpha)}{g(\alpha)}$ в виде многочлена от α называется *уничтожением иррациональности в знаменателе*. Практически удобно искать линейное выражение многочлена f через многочлены g и p_α методом неопределенных коэффициентов, описанным в п. 4 § 1 гл. II. При этом всегда можно добиться выполнения условия ст. $f < \text{ст. } g + \text{ст. } p_\alpha$, необходимого для применения этого метода (см. теорему 4 § 1 гл. II), заменив, если нужно, многочлен f остатком от его деления на p_α .

В приводимых ниже примерах считается, что $P = Q$.

Пример 1. Уничтожим иррациональность в знаменателе дроби

$$\frac{\alpha^4 + \alpha^2 - 2}{\alpha^2 + 2}, \text{ где } \alpha^3 + \alpha - 1 = 0.$$

Легко проверить, что многочлен $x^3 + x - 1$ не имеет рациональных корней и, значит, неприводим в кольце $\mathbb{Q}[x]$. Следовательно, он является минимальным многочленом числа α . Остаток от деления $\alpha^4 + \alpha^2 - 2$ на $\alpha^3 + \alpha - 1$ равен $\alpha - 2$. В примере 4 § 1 гл. II было найдено линейное выражение многочлена $x - 2$ через $x^2 + 2$ и $x^3 + x - 1$:

$$x - 2 = (x^2 - 1)(x^2 + 2) - x(x^3 + x - 1).$$

Подставляя в это равенство $x = \alpha$, находим, что $\alpha - 2 = (\alpha^2 - 1)(\alpha^2 + 2)$ и, значит,

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

Пример 2. Уничтожим иррациональность в знаменателе дроби $\frac{1}{\sqrt[3]{4} + 3\sqrt[3]{2} - 1}$ (имеются в виду положительные значения кубических корней).

Запишем данную дробь в виде $\frac{1}{\alpha^2 + 3\alpha - 1}$, где $\alpha = \sqrt[3]{2}$. Минимальный многочлен числа α равен $x^3 - 2$. Найдём линейное выражение единицы через многочлены $x^2 + 3x - 1$ и $x^3 - 2$:

$$1 = (a_0x^2 + a_1x + a_2)(x^2 + 3x - 1) + (b_0x + b_1)(x^3 - 2).$$

Решая систему уравнений

$$\begin{cases} a_0 + b_0 = 0, \\ 3a_0 + a_1 + b_1 = 0, \\ -a_0 + 3a_1 + a_2 = 0, \\ -a_1 + 3a_2 - 2b_0 = 0, \\ -a_2 - 2b_1 = 0, \end{cases}$$

находим: $a_0 = \frac{2}{15}$, $a_1 = \frac{1}{15}$, $a_2 = -\frac{1}{15}$, $b_0 = -\frac{2}{15}$, $b_1 = -\frac{7}{15}$, т. е.

$$1 = \frac{1}{15} (2x^2 + x - 1)(x^2 + 3x - 1) - \frac{1}{15} (2x + 7)(x^3 - 2).$$

Отсюда получаем:

$$1 = \frac{1}{15} (2\alpha^2 + \alpha - 1)(\alpha^2 + 3\alpha - 1),$$

так что

$$\frac{1}{\sqrt[3]{4} + 3\sqrt[3]{2} - 1} = \frac{1}{15} (2\sqrt[3]{4} + 3\sqrt[3]{2} - 1).$$

Докажем, что если α — трансцендентное над P число, то поле $P(\alpha)$ изоморфно полю $P(x)$ рациональных дробей (см. § 4 гл. II). Каждой рациональной дроби $\frac{f}{g}$ ($f, g \in P[x]$, $g \neq 0$) сопоставим ее значение в точке α , т. е. число $\frac{f(\alpha)}{g(\alpha)} \in P(\alpha)$. Легко видеть, что эквивалентным дробям таким образом сопоставля-

ется одно и то же число. Обратно, если

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)},$$

то $f_1(\alpha) g_2(\alpha) = f_2(\alpha) g_1(\alpha)$. Ввиду трансцендентности числа α над P следует, что $f_1 g_2 = f_2 g_1$ и, значит,

$$\frac{f_1}{g_1} \sim \frac{f_2}{g_2}.$$

Далее, из определения поля $P(\alpha)$ вытекает, что каждое число из этого поля представляется в виде $\frac{f(\alpha)}{g(\alpha)}$, где $f, g \in P[x]$, $g \neq 0$.

Сказанное выше позволяет построить взаимно однозначное отображение поля $P(x)$ на поле $P(\alpha)$, сопоставив каждому классу эквивалентных рациональных дробей значение в точке α любой дроби из этого класса. Так как при сложении (соответственно умножении) рациональных дробей их значения в точке α складываются (соответственно перемножаются), то это отображение является изоморфизмом полей.

В связи с введенными в этом параграфе понятиями алгебраического числа и простого алгебраического расширения возникает целый ряд вопросов, например:

1) Будет ли алгебраическим над P всякое число, принадлежащее простому алгебраическому расширению поля P ?

2) Будут ли алгебраическими сумма и произведение алгебраических чисел?

Ответы на эти и другие подобные вопросы будут получены в следующем параграфе.

Вопросы для самопроверки

1. Что такое алгебраическое число?
2. Что такое минимальный многочлен алгебраического числа?
3. Каким свойством обладает минимальный многочлен любого алгебраического числа?
4. Какой минимальный многочлен у числа $\frac{\sqrt{5}-1}{2}$?
5. Докажите существование трансцендентных чисел.
6. Дайте определение кольца $P[\alpha]$, где P — числовое поле и α — любое число.
7. Каков общий вид элементов кольца $P[\alpha]$?
8. В каком случае число α называется алгебраическим числом степени n над полем P ? В каком виде однозначно представляется в этом случае любой элемент кольца $P[\alpha]$?
9. Какова степень числа $\sqrt[3]{2} \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2} \right)$ над полем $Q(\sqrt[3]{2})$?
10. Пусть n — простое число и ω — первообразный корень n -й степени из единицы. Докажите, что всякий элемент кольца $Q[\omega]$ однозначно представляется в виде $a_1\omega + a_2\omega^2 + \dots + a_{n-1}\omega^{n-1}$, где $a_1, a_2, \dots, a_{n-1} \in Q$.

11. Что такое простое расширение числового поля?
12. Как устроено поле $P(\alpha)$ в случае, когда α — алгебраическое над P число?
13. Что такое «уничтожение иррациональности в знаменателе»?

Упражнения

Освободитесь от иррациональности в знаменателе дроби:

- а) $\frac{\alpha}{\alpha+1}$, $\alpha^3 - 3\alpha + 1 = 0$;
- б) $\frac{\alpha^2 - 3\alpha - 1}{\alpha^2 + 2\alpha + 1}$, $\alpha^3 + \alpha^2 + 3\alpha + 4 = 0$;
- в) $\frac{1}{3\alpha^3 + \alpha^2 - 2\alpha - 1}$, $\alpha^4 - \alpha^3 + 2\alpha + 1 = 0$;
- г) $\frac{1}{\alpha^3 + 3\alpha^2 + 3\alpha + 2}$, $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$.

§ 3. КОНЕЧНЫЕ РАСШИРЕНИЯ ЧИСЛОВЫХ ПОЛЕЙ

1. Критерий алгебраичности числа над заданным полем. Пусть P — числовое поле. Рассмотрим какое-либо числовое кольцо K , содержащее поле P (таким кольцом может быть, например, кольцо $\mathbb{C}$ всех комплексных чисел). Очевидно, что:

- а) если $x, y \in K$, то $x + y \in K$;
- б) если $x \in K, c \in P$, то $cx \in K$.

Это позволяет рассматривать K как векторное пространство над полем P (аксиомы векторного пространства выполняются очевидным образом в силу свойств операций над комплексными числами). Полученное таким образом векторное пространство мы будем обозначать через $K|P$.

Рассмотрим, например, кольцо $P[\alpha]$, где α — число, алгебраическое над P . В п. 3 § 2 было показано, что если степень α над P равна n , то всякий элемент кольца $P[\alpha]$ однозначно представляется в виде линейной комбинации чисел $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ с коэффициентами из P . Это означает, что числа $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ составляют базис пространства $P[\alpha]|P$ и, стало быть,

$$\dim P[\alpha]|P = n.$$

Таким образом, если α — алгебраическое над P число, то пространство $P[\alpha]|P$ конечномерно.

С другой стороны, если α — трансцендентное над P число, то пространство $P[\alpha]|P$ бесконечномерно. Действительно, поскольку в этом случае α не является корнем никакого ненулевого многочлена с коэффициентами из P , числа $1, \alpha, \alpha^2, \dots, \alpha^m$ линейно независимы как элементы векторного пространства $P[\alpha]|P$ при любом m и, следовательно, пространство $P[\alpha]|P$ бесконечномерно.

Таким образом, доказана такая теорема:

Теорема 1. Число α является алгебраическим над полем P тогда и только тогда, когда векторное пространство $P[\alpha]|P$ конечномерно. При этом степень α над P равна размерности этого пространства.

Отсюда получается важное следствие:

С л е д с т в и е. Пусть K — числовое кольцо, содержащее поле P . Если пространство $K|P$ конечномерно, то всякое число из кольца K алгебраично над P .

Д о к а з а т е л ь с т в о. Пусть α — любой элемент кольца K . Очевидно, что $P[\alpha] \subset K$ и, значит, пространство $P[\alpha]|P$ является подпространством пространства $K|P$. Так как $K|P$ конечномерно, то и $P[\alpha]|P$ конечномерно. По теореме 1 число α является алгебраическим над P .

2. Определение конечных расширений. Свойство их транзитивности. Пусть K — числовое кольцо, содержащее поле P . Докажем, что если кольцо K конечномерно над P , то оно является полем. Возьмем произвольное число $\alpha \in K$. Согласно следствию теоремы 1, оно алгебраично над P . Пусть

$$p_\alpha = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n =$$

его минимальный многочлен над P . Если $\alpha \neq 0$, то $a_n \neq 0$ (иначе многочлен p_α можно было бы сократить на x). Из равенства

$$a_0\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n = 0$$

следует тогда, что

$$\alpha^{-1} = -\frac{1}{a_n}(a_0\alpha^{n-1} + a_1\alpha^{n-2} + \dots + a_{n-1})$$

и, значит, $\alpha^{-1} \in K$. Таким образом, кольцо K содержит вместе с любым числом, отличным от нуля, число, ему обратное. Следовательно, K является числовым полем.

Из доказанного утверждения и теоремы 1 вытекает, что если α — число, алгебраическое над P , то кольцо $P[\alpha]$ является полем. Отсюда получается другое доказательство теоремы 1 предыдущего параграфа.

Числовое поле K называется *конечным расширением поля P* , если оно содержит поле P и если пространство $K|P$ конечномерно. Из теоремы 1 следует, что простое алгебраическое расширение является конечным расширением. В п. 4 покажем, что всякое конечное расширение в действительности является простым алгебраическим расширением.

Установим следующее «свойство транзитивности» конечных расширений.

Теорема 2. Пусть K — конечное расширение поля P , а L — конечное расширение поля K . Тогда L будет конечным расширением поля P , причем

$$\dim L|P = \dim L|K \cdot \dim K|P. \quad (1)$$

Формулу (1) легко запомнить с помощью символического равенства

$$\frac{L}{P} = \frac{L}{K} \cdot \frac{K}{P}.$$

Доказательство. Пусть числа $\alpha_1, \alpha_2, \dots, \alpha_n$ составляют базис пространства $K|P$, а числа $\beta_1, \beta_2, \dots, \beta_m$ — базис пространства $L|K$. Докажем, что nm чисел

$$\alpha_i \beta_j (i = 1, 2, \dots, n; j = 1, 2, \dots, m) \quad (2)$$

составляют базис пространства $L|P$.

Всякое число γ из поля L представляется в виде

$$\gamma = c_1 \beta_1 + c_2 \beta_2 + \dots + c_m \beta_m, \quad (3)$$

где $c_1, c_2, \dots, c_m \in K$. Каждое из чисел $c_1, c_2, \dots, c_m$, в свою очередь, представляется в виде линейной комбинации чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ с коэффициентами из поля P . Подставив эти выражения для $c_1, c_2, \dots, c_m$ в (3), получим представление числа γ в виде линейной комбинации чисел (2) с коэффициентами из P . Таким образом, векторное пространство $L|P$ порождается числами (2).

Покажем, что числа (2) линейно независимы над P . Предположим, что

$$\sum_{i=1}^n \sum_{j=1}^m c_{ij} \alpha_i \beta_j = 0 \quad (4)$$

для каких-то $c_{ij} \in P$. Перепишав это равенство в виде

$$\sum_{j=1}^m \left(\sum_{i=1}^n c_{ij} \alpha_i \right) \beta_j = 0,$$

получим линейную зависимость между числами $\beta_1, \beta_2, \dots, \beta_m$ с коэффициентами $\sum_{i=1}^n c_{ij} \alpha_i \in K$. Ввиду того что числа $\beta_1, \beta_2, \dots, \beta_m$ линейно независимы над K , отсюда следует, что

$$\sum_{i=1}^n c_{ij} \alpha_i = 0 \quad (j = 1, 2, \dots, m).$$

Из этих равенств, в силу линейной независимости чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ над P , в свою очередь, следует, что $c_{ij} = 0$ при всех i, j . Таким образом, соотношение (4) возможно, если только все коэффициенты c_{ij} равны нулю, а это и означает, что числа (2) линейно независимы.

Итак, числа (2) составляют базис пространства $L|P$. Следовательно,

$$\dim L|P = nm = \dim L|K \cdot \dim K|P.$$

В частности, пространство $L|P$ конечномерно, так что L есть конечное расширение поля P . Теорема доказана.

3. Поле алгебраических чисел. В этом пункте будет доказано, что сумма и произведение алгебраических чисел, а также число, обратное алгебраическому, являются алгебраическими числами. Это означает, что совокупность всех алгебраических чисел — поле. В действительности будет доказана даже следующая более общая теорема:

Теорема 3. Совокупность всех чисел, алгебраических над данным полем P , является полем.

Доказательство. Прежде всего заметим, что если число α , отличное от нуля, удовлетворяет алгебраическому уравнению

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0,$$

где $a_0, a_1, \dots, a_{n-1}, a_n \in P$, то число α^{-1} будет удовлетворять уравнению

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0.$$

Стало быть, если α — число, алгебраическое над P , то и α^{-1} алгебраично над P .

Пусть теперь α и β — числа, алгебраические над P . Рассмотрим поле $K = P(\alpha)$ и поле $L = K(\beta)$. Заметим, что число β , будучи алгебраическим над P , тем более алгебраично над K . По теореме 1, поле K есть конечное расширение поля P , а поле L — конечное расширение поля K . По теореме 2, поле L является также конечным расширением поля P . Но тогда из теоремы 1 следует, что все числа из поля L алгебраичны над P . В частности, это относится к числам $\alpha + \beta$ и $\alpha\beta$, которые, очевидно, принадлежат L . Тем самым теорема доказана.

Можно дать и другое, более «явное» доказательство теоремы 3. Пусть $\alpha_1, \alpha_2, \dots, \alpha_n$ — все корни минимального многочлена p_α числа α над полем P и $\beta_1, \beta_2, \dots, \beta_m$ — все корни минимального многочлена p_β числа β над этим полем. Образует многочлен

$$f(x) = \prod_{i=1}^n \prod_{j=1}^m (x - \alpha_i - \beta_j). \quad (5)$$

Будем временно рассматривать $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m$ как переменные. Очевидно, что многочлен $f(x)$ не меняется при любых перестановках $\alpha_1, \alpha_2, \dots, \alpha_n$, а также при любых перестановках $\beta_1, \beta_2, \dots, \beta_m$. Следовательно, его коэффициенты представляют собой многочлены от $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m$ симметрические как по $\alpha_1, \alpha_2, \dots, \alpha_n$, так и по $\beta_1, \beta_2, \dots, \beta_m$. Пусть $c(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m)$ — один из этих коэффициентов. Рассматривая его как симметрический многочлен от $\alpha_1, \alpha_2, \dots, \alpha_n$ с коэффициентами из кольца S симметрических многочленов от $\beta_1, \beta_2, \dots, \beta_m$, мы можем представить его в виде многочлена от элементарных симметрических многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$ от $\alpha_1, \alpha_2, \dots, \alpha_n$ с коэффициентами из кольца S . Каждый из этих коэффициентов можно представить как

многочлен от элементарных симметрических многочленов $\tau_1, \tau_2, \dots, \tau_m$ от $\beta_1, \beta_2, \dots, \beta_m$ с коэффициентами из поля P . В итоге получится выражение $c(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m)$ в виде многочлена от $\sigma_1, \sigma_2, \dots, \sigma_n$ и $\tau_1, \tau_2, \dots, \tau_m$ с коэффициентами из поля P . Подставляя в это выражение значения $\sigma_1, \sigma_2, \dots, \sigma_n$ и $\tau_1, \tau_2, \dots, \tau_m$, найденные по формулам Виета, мы получим, что

$$c(\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m) \in P.$$

Таким образом, все коэффициенты многочлена $f(x)$ принадлежат полю P . Так как $f(\alpha + \beta) = 0$, то $\alpha + \beta$ — алгебраическое над полем P число.

Аналогично, рассматривая многочлен

$$g(x) = \prod_{i=1}^n \prod_{j=1}^m (x - \alpha_i \beta_j), \quad (6)$$

можно доказать, что $\alpha\beta$ — алгебраическое над P число.

В качестве иллюстрации этого доказательства разберем следующий пример:

Пример 1. Найдем ненулевой многочлен с рациональными коэффициентами, имеющий своим корнем число $\sqrt{2} + \sqrt[3]{3}$ (имеются в виду положительные значения корней).

В этом примере $P = \mathbb{Q}$, $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{3}$. Минимальный многочлен числа α равен $x^2 - 2$; его корнями являются $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$. Минимальный многочлен числа β равен $x^3 - 3$; его корнями являются $\beta_1 = \sqrt[3]{3}$, $\beta_2 = \omega \sqrt[3]{3}$, $\beta_3 = \bar{\omega} \sqrt[3]{3}$, где $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ — кубический корень из единицы. Составляем многочлен $f(x)$ по формуле (5):

$$f(x) = \prod_{i=1}^2 \prod_{j=1}^3 (x - \alpha_i - \beta_j).$$

Так как $\prod_{j=1}^3 (x - \beta_j) = x^3 - 3$, то $\prod_{j=1}^3 (x - \alpha_i - \beta_j) = (x - \alpha_i)^3 - 3$ и, следовательно,

$$f(x) = \prod_{i=1}^2 ((x - \alpha_i)^3 - 3) =$$

$$= (x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} - 3)(x^3 + 3\sqrt{2}x^2 + 6x + 2\sqrt{2} - 3) = \\ = (x^3 + 6x - 3)^2 - 2(3x^2 + 2)^2 = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1.$$

Таким образом, число $\sqrt{2} + \sqrt[3]{3}$ является корнем многочлена

$$x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1.$$

Итак, совокупность всех алгебраических чисел замкнута относительно рациональных операций. Можно заметить, что она замкнута и относительно извлечения корней, т. е. корень любой степени из алгебраического числа также является алгебраическим числом. В самом деле, если число α является корнем многочлена $f(x) \in \mathbb{Q}[x]$, то $\sqrt[n]{\alpha}$ будет корнем многочлена $g(x) = f(x^n) \in \mathbb{Q}[x]$. Аналогичное утверждение справедливо, конечно, и для чисел, алгебраических над каким-либо заданным числовым полем P . Обобщением этого утверждения является следующая теорема:

Т е о р е м а 4. *Корень любого ненулевого многочлена, коэффициенты которого — алгебраические над P числа, также является алгебраическим над P числом.*

Д о к а з а т е л ь с т в о. Пусть β — корень многочлена

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

где $\alpha_0, \alpha_1, \dots, \alpha_{n-1}, \alpha_n$ — числа, алгебраические над P , причем $\alpha_0 \neq 0$. Рассмотрим возрастающую последовательность числовых полей

$$P_0 = P(\alpha_0), P_1 = P_0(\alpha_1), \dots, P_n = P_{n-1}(\alpha_n).$$

Число α_k , будучи алгебраическим над полем P , тем более алгебраично над полем P_{k-1} . Следовательно, P_k — конечное расширение поля P_{k-1} . Многократное применение теоремы 2 позволяет заключить, что P_n — конечное расширение поля P .

Поле P_n по построению содержит числа $\alpha_0, \alpha_1, \dots, \alpha_{n-1}, \alpha_n$. Следовательно, число β алгебраично над P_n . Рассмотрим поле $P_n(\beta)$. Применяя еще раз теорему 2, находим, что оно также является конечным расширением поля P . Следовательно, все его элементы, и в частности β , являются алгебраическими над P числами (следствие теоремы 1). Теорема доказана.

Поле L называется *алгебраически замкнутым*, если любой многочлен положительной степени с коэффициентами из поля L имеет корни в этом поле.

Согласно «основной теореме алгебры» поле $\mathbb{C}$ всех комплексных чисел алгебраически замкнуто. Из теоремы 4 следует, что поле $\overline{P}$ всех чисел, алгебраических над заданным числовым полем P , также алгебраически замкнуто. В самом деле, любой многочлен положительной степени с коэффициентами из поля P имеет корень в поле $\mathbb{C}$, но, по теореме 4, этот корень принадлежит полю $\overline{P}$.

В частности, поле $\overline{\mathbb{Q}}$ всех алгебраических чисел алгебраически замкнуто.

4. Простота конечных расширений.

Т е о р е м а 5. *Всякое конечное расширение числового поля является простым алгебраическим расширением этого поля.*

Д о к а з а т е л ь с т в о. Вначале мы докажем теорему не для любого конечного расширения числового поля P , а для расширения вида $P(\alpha)(\beta)$, где α и β — числа, алгебраические над P .

Иными словами, мы покажем, что «двукратное» алгебраическое расширение может быть заменено простым расширением.

Пусть α и β — числа, алгебраические над P . Наша задача состоит в том, чтобы найти число γ , для которого

$$P(\alpha)(\beta) = P(\gamma).$$

Будем искать его в виде

$$\gamma = \alpha + c\beta,$$

где c — подходящее число из поля P . Каким именно образом нужно выбрать число c , будет указано ниже.

Обозначим через p_α и p_β минимальные многочлены над полем P чисел α и β соответственно. Рассмотрим многочлен

$$q(x) = p_\alpha(\gamma - cx),$$

коэффициенты которого принадлежат полю $P(\gamma)$. Число β является его корнем. В самом деле,

$$q(\beta) = p_\alpha(\gamma - c\beta) = p_\alpha(\alpha) = 0.$$

В то же время число β является корнем многочлена p_β , коэффициенты которого принадлежат полю P и потому полю $P(\gamma)$. Допустим, что многочлены q и p_β не имеют общих корней, отличных от β . Тогда их наибольший общий делитель равен $x - \beta$, и, поскольку его коэффициенты должны принадлежать полю $P(\gamma)$, $\beta \in P(\gamma)$: Отсюда, в свою очередь, следует, что $\alpha = \gamma - c\beta \in P(\gamma)$ и, значит,

$$P(\alpha)(\beta) \subset P(\gamma).$$

С другой стороны, ясно, что

$$P(\alpha) \subset P(\alpha)(\beta).$$

Таким образом, при сделанном допущении

$$P(\alpha)(\beta) = P(\gamma).$$

Остается показать, что число $c \in P$ может быть выбрано так, чтобы многочлены q и p_β не имели других общих корней, кроме β .

Пусть $\alpha_1, \alpha_2, \dots, \alpha_n$ — все комплексные корни многочлена p_α и аналогично $\beta_1, \beta_2, \dots, \beta_m$ — все корни многочлена p_β . Будем считать, что $\beta = \beta_1$. Число β_j ($j \neq 1$) будет корнем многочлена q , если $\gamma - c\beta_j$ — корень многочлена p_α , т. е. если

$$\gamma - c\beta_j = \alpha_i \quad (7)$$

для некоторого i . Равенство (7) выполняется только при одном значении c , а именно при $c = \frac{\alpha_i - \alpha}{\beta - \beta_j}$. Стало быть, если выбрать c отличным от всех чисел

$$\frac{\alpha_i - \alpha}{\beta - \beta_j} \quad (i = 1, 2, \dots, n; j = 2, \dots, m),$$

то $\beta = \beta_1$ будет единственным общим корнем многочленов q и p_β ;

Для произвольного конечного расширения K числового поля P будем доказывать теорему индукцией по $\dim K|P$.

В случае $\dim K|P = 1$ имеем $K = P$, и утверждение теоремы очевидно.

Предположим теперь, что утверждение теоремы справедливо для всякого расширения F числового поля L , удовлетворяющего условию $\dim F|L < n$. Пусть K — расширение числового поля P , для которого $\dim K|P = n$. Выберем в поле K произвольное число α , не принадлежащее полю P , и рассмотрим «промежуточное» поле $L = P(\alpha)$. Так как

$$\dim K|L = \frac{\dim K|P}{\dim L|P} < n$$

(см. теорему 2), то по индуктивному предположению существует такое число β , что

$$K = L(\beta) = P(\alpha)(\beta).$$

Согласно доказанному ранее, отсюда следует, что поле K является простым алгебраическим расширением поля P . Тем самым теорема полностью доказана.

Вопросы для самопроверки

1. В каком случае поле $P(\alpha)$ является конечномерным векторным пространством над полем P ?
2. Что называется конечным расширением числового поля?
3. Докажите, что если α — алгебраическое число, то всякое число из поля $Q(\alpha)$ также является алгебраическим.
4. Докажите двумя способами, что сумма двух алгебраических чисел также является алгебраическим числом.
5. Докажите, что поле всех алгебраических чисел алгебраически замкнуто.
6. Докажите, что если L — алгебраически замкнутое поле, то всякий многочлен положительной степени с коэффициентами из L разлагается на линейные множители в кольце $L[x]$.
7. Найдите такое число γ , что $Q(\sqrt{2})(\sqrt{3}) = Q(\gamma)$.

Упражнения

Найдите ненулевой многочлен с рациональными коэффициентами, имеющий своим корнем число $\alpha + \beta$, где α и β — алгебраические числа, минимальные многочлены которых суть p_α и p_β соответственно:

- а) $p_\alpha(x) = x^2 + x + 1$, $p_\beta(x) = x^2 + 2x + 3$;
- б) $p_\alpha(x) = x^3 + x + 1$, $p_\beta(x) = x^2 - 5$;
- в) $p_\alpha(x) = x^3 - 2$, $p_\beta(x) = x^2 - 3x + 1$.

§ 4. РАЗРЕШИМОСТЬ УРАВНЕНИЙ В РАДИКАЛАХ

1. Понятие разрешимости в радикалах. Пусть P — числовое поле. Будем говорить, что число α представляется в радикалах над P , если оно выражается через элементы поля P при помощи извлечения корней (любой степени) и рациональных операций — сложения, вычитания, умножения и деления. Это означает, что существует такая последовательность чисел

$$\alpha_1, \alpha_2, \dots, \alpha_m, \quad (1)$$

что ее последний член α_m совпадает с α , а каждый член α_k ($k = 1, 2, \dots, m$) удовлетворяет одному из следующих условий:

$$1) \alpha_k \in P;$$

$$2) \alpha_k = \alpha_i + \alpha_j, \alpha_i - \alpha_j, \alpha_i \cdot \alpha_j \text{ или } \frac{\alpha_i}{\alpha_j} \text{ для каких-то } i, j < k;$$

$$3) \alpha_k = \sqrt[r]{\alpha_i} \text{ (одно из значений корня) для какого-то } i < k \text{ и какого-то натурального } r.$$

Алгебраическое уравнение

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0 \quad (2)$$

с коэффициентами из поля P называется *разрешимым в радикалах над P* , если все его корни представляются в радикалах над P .

Понятие разрешимости в радикалах конкретного алгебраического уравнения не следует путать с разрешимостью в радикалах общего уравнения степени n , о которой шла речь в § 4 гл. IV. Разрешимость в радикалах общего уравнения степени n над полем P означает возможность выразить ϵ и η о б р а з н о, т. е. одной и той же формулой, корни любого алгебраического уравнения степени n над полем P через его коэффициенты и фиксированные элементы поля P при помощи извлечения корней и рациональных операций. Ясно, что из разрешимости в радикалах общего уравнения степени n следует разрешимость в радикалах любого конкретного уравнения. Обратное же неверно. Например, общее уравнение степени n над полем C при $n \geq 5$ неразрешимо в радикалах, но любое конкретное алгебраическое уравнение над C разрешимо в радикалах, так как его корни лежат в C .

Наиболее интересен вопрос о разрешимости в радикалах алгебраических уравнений над полем рациональных чисел. Ясно, что существуют уравнения сколь угодно высокой степени, разрешимые в радикалах над $\mathbb{Q}$, например уравнения вида $x^n - a = 0$ ($a \in \mathbb{Q}$). Однако совершенно не ясно, существуют ли алгебраические уравнения, неразрешимые в радикалах над $\mathbb{Q}$. Ответ на этот вопрос получил около 1830 г. французский математик Эварист Галуа, который нашел необходимое и достаточное условие разрешимости в радикалах алгебраического уравнения над произвольным полем P . В частности, он доказал, что для любого $n \geq 5$ существуют алгебраические уравнения степени n с рациональными коэффициентами, неразрешимые в радикалах над $\mathbb{Q}$.

Изложение теории Галуа выходит за рамки нашего пособия. Отметим только, что в этой теории с каждым алгебраическим уравнением связывается некоторая конечная группа (называемая в современной литературе *группой Галуа данного уравнения*), по которой можно, в частности, определить, разрешимо данное уравнение в радикалах или нет. Теория Галуа позволяет также исследовать вопрос о разрешимости в радикалах в общем виде всех алгебраических уравнений из какой-либо заданной совокупности (например, всех уравнений данной степени).

В определении разрешимости уравнения в радикалах требуется, чтобы каждый корень представлялся в радикалах над P . Можно, однако, показать, что если многочлен $f(x)$ неприводим над полем P и если хотя бы один его корень представляется в радикалах над P , то это имеет место и для всех других корней.

2. Разрешимость в квадратных радикалах. Будем говорить, что число α представляется в квадратных радикалах над полем P , если оно выражается через элементы этого поля при помощи извлечения квадратных корней и рациональных операций.

Алгебраическое уравнение с коэффициентами из поля P называется *разрешимым в квадратных радикалах над P* , если все его корни представляются в квадратных радикалах над P . Вопрос о разрешимости уравнений в квадратных радикалах возникает в теории геометрических построений (см. пп. 3—6 этого параграфа).

Можно доказать, что если какой-либо один корень неприводимого многочлена $f(x) \in P[x]$ представляется в квадратных радикалах над P , то это имеет место и для всех других корней, т. е. уравнение $f(x) = 0$ разрешимо в квадратных радикалах над P . Однако этот факт нам не понадобится.

Теорема 1. Пусть $f(x) \in P[x]$ — многочлен степени n , неприводимый над полем P . Если n не является степенью двойки, то ни один корень уравнения $f(x) = 0$ не представляется в квадратных радикалах над P .

Доказательство. Пусть α — корень уравнения $f(x) = 0$, представимый в квадратных радикалах над P . Существует последовательность чисел

$$\alpha_1, \alpha_2, \dots, \alpha_m, \quad (3)$$

последний член α_m которой совпадает с α , а каждый член α_k ($k = 1, 2, \dots, m$) удовлетворяет одному из следующих условий:

- 1) $\alpha_k \in P$;
- 2) $\alpha_k = \alpha_i + \alpha_j$, $\alpha_k = \alpha_i - \alpha_j$, $\alpha_k = \alpha_i \cdot \alpha_j$ или $\frac{\alpha_i}{\alpha_j}$ для каких-то $i, j < k$;
- 3) $\alpha_k = \sqrt{\alpha_i}$ для какого-то $i < k$.

Построим цепочку полей:

$$P_0 = P, P_1 = P_0(\alpha_1), P_2 = P_1(\alpha_2), \dots, P_m = P_{m-1}(\alpha_m).$$

Если α_k принадлежит полю P или получается в результате рациональной операции над какими-то двумя предыдущими членами последовательности (3), то $\alpha_k \in P_{k-1}$ и, значит, $P_k = P_{k-1}$. Если же $\alpha_k = \sqrt{\alpha_i}$ ($i < k$), то либо опять-таки $\alpha_k \in P_{k-1}$ и $P_k = P_{k-1}$, либо α_k есть алгебраическое число второй степени над полем P_{k-1} и, значит, $\dim P_k | P_{k-1} = 2$. Таким образом, в любом случае

$$\dim P_k | P_{k-1} = 1 \text{ или } 2.$$

В силу теоремы 2 предыдущего параграфа,

$$\dim P_k | P = \dim P_{k-1} | P \cdot \dim P_k | P_{k-1}.$$

Из равенства (4) следует, что

$$\dim P_k | P = \dim P_{k-1} | P \text{ или } 2 \dim P_{k-1} | P,$$

и, значит,

$$\dim P_m | P = 2^p$$

(где p есть число индексов k , для которых $\alpha_k \notin P_{k-1}$).

Рассмотрим теперь поле $P(\alpha)$. Поскольку многочлен $f(x)$ неприводим, он является минимальным многочленом числа α над полем P . По теореме 1 § 3 размерность пространства $P(\alpha) | P$ равна степени n многочлена $f(x)$. Так как $\alpha \in P_m$, то $P(\alpha) \subset P_m$. По теореме 2 § 3,

$$\dim P_m | P = \dim P(\alpha) | P \cdot \dim P_m | P(\alpha),$$

т. е.

$$2^p = n \cdot \dim P_m | P(\alpha).$$

Отсюда видно, что $n = 2^q$, где $q \leq p$. Теорема доказана.

С л е д с т в и е. Пусть $f(x) \in P[x]$ — многочлен третьей степени. Кубическое уравнение $f(x) = 0$ разрешимо в квадратных радикалах над P тогда и только тогда, когда оно имеет хотя бы один корень в поле P .

Д о к а з а т е л ь с т в о. Если многочлен $f(x)$ не имеет корней в P , то он неприводим над полем P и по доказанной теореме уравнение $f(x) = 0$ неразрешимо в квадратных радикалах над P .

Обратно, если $f(x)$ имеет корень $x_0 \in P$, то после деления на $x - x_0$ решение уравнения $f(x) = 0$ сводится к решению квадратного уравнения с коэффициентами из P , которое, очевидно, разрешимо в квадратных радикалах.

Можно доказать, что уравнение четвертой степени разрешимо в квадратных радикалах тогда и только тогда, когда этим свойством обладает его кубическая резольвента (см. определение в п. 4 § 4 гл. IV). Отсюда следует, что утверждение, обратное теореме 1, неверно. Например, легко показать, что многочлен $x^4 + x + 1$ неприводим над $\mathbb{Q}$. Однако уравнение $x^4 + x + 1 = 0$ неразрешимо в квадратных радикалах над $\mathbb{Q}$, так как его кубическая резольвента $y^3 - 4y - 1 = 0$ не имеет рациональных корней.

3. Геометрические построения циркулем и линейкой. В задачах на построение требуется по данной фигуре построить другую, находящуюся в определенном отношении к данной (например, по точке и

окружности построить прямую, проходящую через данную точку и касающуюся данной окружности). При этом указывается, какими средствами построения разрешается пользоваться.

В задачах на построение циркулем и линейкой рассматриваются фигуры на плоскости, состоящие из конечного числа элементов следующего вида:

- 1) точек;
- 2) прямых, лучей или отрезков прямых;
- 3) окружностей или дуг окружностей.

Заметим, что задать отрезок — это все равно что задать прямую, на которой он лежит, и две точки на этой прямой, являющиеся его концами. Аналогично задание луча равносильно заданию прямой и точки на ней, с дополнительным указанием, по какую сторону от этой точки лежит луч; задание дуги окружности равносильно заданию самой окружности и двух точек на ней, с дополнительным указанием, какую из двух дуг, имеющих своими концами эти точки, следует выбрать*. Поэтому в дальнейшем мы можем считать, что все рассматриваемые фигуры состоят из конечного числа точек, прямых и окружностей (хотя практически, ввиду ограниченности чертежа, мы имеем дело именно с отрезками прямых, а не с прямыми).

В процессе построения к уже имеющимся точкам, прямым и окружностям добавляются новые. Целью является построение некоторых точек, прямых и окружностей, обладающих указанными в задаче свойствами.

Правила, по которым происходит построение циркулем и линейкой, могут быть описаны следующим образом. Построение разбивается на ряд последовательных шагов. Для того чтобы описать один шаг построения, обозначим через M совокупность всех точек, прямых и окружностей, заданных согласно условию задачи и построенных на предыдущих шагах. Очередной шаг построения заключается в добавлении к множеству M одного элемента t , т. е. в построении точки, прямой или окружности, согласно одному из следующих правил:

- (П1) t есть точка пересечения двух прямых из множества M ;
- (П2) t есть одна из точек пересечения прямой и окружности из множества M ;
- (П3) t есть одна из точек пересечения двух окружностей из множества M ;
- (П4) t есть прямая, проходящая через две точки из множества M ;
- (П5) t есть окружность с центром в точке из множества M и проходящая через точку из множества M .

* Имеется в виду равносильность с точки зрения построения циркулем и линейкой. Так, например, по дуге окружности с помощью циркуля и линейки можно, как известно, построить всю окружность. «Дополнительное условие» может быть дано в виде еще одной точки, лежащей на задаваемом луче или дуге окружности.

В число разрешенных операций при построениях циркулем и линейкой можно включить также такие операции, как выбор произвольной точки в области (быть может, бесконечной), ограниченной прямыми и окружностями из множества M , выбор произвольной точки в интервале прямой из множества M , ограниченном точками из множества M , и выбор произвольной точки на дуге окружности из множества M , ограниченной точками из множества M . Однако нетрудно видеть, что если исходные данные задачи включают в себя хотя бы две точки, то каждая из этих операций может быть заменена последовательностью операций типов (П1) — (П5), перечисленных выше. Например, выбор произвольной точки в конечном интервале можно заменить построением середины этого интервала, которое выполняется хорошо известным способом только при помощи операций типов (П1) — (П5); выбор произвольной точки в треугольнике можно заменить построением, скажем, точки пересечения медиан этого треугольника. Поэтому при исследовании вопроса о разрешимости задач на построение подобные операции можно не рассматривать.

4. Необходимое условие разрешимости задачи на построение. Вопрос о возможности того или иного геометрического построения с помощью циркуля и линейки относится скорее к алгебре многочленов, чем к геометрии. Впервые это понял, по-видимому, Гаусс. В своих «Арифметических исследованиях» (1801 г.) он устанавливает связь между построением правильного n -угольника и решением уравнения $x^n - 1 = 0$ в поле комплексных чисел. Пользуясь этой связью, он дает способ построения циркулем и линейкой правильного 17-угольника и находит необходимое и достаточное условие, которому должно удовлетворять простое число n для того, чтобы построение циркулем и линейкой правильного n -угольника было возможно. Это условие состоит в том, что n должно иметь вид $2^q + 1$, где q — целое число.*

Легко видеть, что число $2^q + 1$ может быть простым, если только q есть степень двойки. Числа $F_k = 2^{2^k} + 1$ ($k = 0, 1, 2, \dots$) называются числами Ферма. При $k = 0, 1, 2, 3, 4$ это простые числа 3, 5, 17, 257, 65537. Соответствующие правильные многоугольники, стало быть, могут быть построены циркулем и линейкой. Ферма предполагал, что все числа F_k простые. Это предположение оказалось неверным. Так, например, известно, что при $5 \leq k \leq 16$ числа F_k являются составными. В настоящее время не известно ни одного простого числа Ферма, кроме перечисленных выше пяти чисел.

Для произвольного n необходимое и достаточное условие возможности построения циркулем и линейкой правильного n -угольника состоит в том, что все нечетные простые делители числа n должны быть числами Ферма и входить в его каноническое разложение в первой степени.

В этом пункте мы найдем необходимое условие разрешимости задачи на построение циркулем и линейкой.

Зафиксируем на плоскости некоторую систему координат. Пусть P — какое-то числовое поле. Будем говорить, что *точка определена над P* , если обе ее координаты принадлежат полю P . Далее, будем говорить, что *прямая определена над P* , если она содержит две точки, определенные над P , и что *окружность определена над P* , если она содержит точку, определенную над P , и ее центр определен над P .

* Следует заметить, что хотя Гаусс и утверждает, что это условие необходимо и достаточно, доказательство необходимости не было им опубликовано.

Л е м м а 1. Если прямая l определена над полем P , то она может быть задана линейным уравнением

$$ax + by + c = 0 \quad (5)$$

с коэффициентами из P .

Д о к а з а т е л ь с т в о. Пусть $(x_1; y_1)$ и $(x_2; y_2)$ — точки прямой l , определенные над P . Тогда ее уравнение может быть записано в виде

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1}$$

или после преобразований

$$(y_2 - y_1)x + (x_1 - x_2)y + x_2y_1 - x_1y_2 = 0.$$

Коэффициенты этого уравнения принадлежат полю P .

Л е м м а 2. Если окружность s определена над полем P , то она может быть задана уравнением

$$x^2 + y^2 + px + qy + r = 0 \quad (6)$$

с коэффициентами из P .

Д о к а з а т е л ь с т в о. Пусть $(x_0; y_0)$ — центр окружности s и $(x_1; y_1)$ — ее точка, определенная над P . Уравнение окружности может быть записано в виде

$$(x - x_0)^2 + (y - y_0)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2,$$

откуда после очевидных преобразований получается уравнение вида (6) с коэффициентами из P .

Введем теперь одно определение. Расширение K поля P будем называть *допустимым*, если каждое число из K представляется в квадратных радикалах над P . Очевидно, что простое расширение $K = P(\alpha)$ допустимо тогда и только тогда, когда число α представляется в квадратных радикалах над P . Очевидно также, что если K — допустимое расширение поля P , а L — допустимое расширение поля K , то L будет допустимым расширением поля P .

Т е о р е м а 2. Пусть M — некоторое множество точек, прямых и окружностей, определенных над полем P . Для того чтобы некоторая точка, прямая или окружность могла быть построена циркулем и линейкой, исходя из множества M , необходимо, чтобы она была определена над некоторым допустимым расширением поля P .

Д о к а з а т е л ь с т в о. Предположим, что данная точка, прямая или окружность — обозначим ее через t — может быть построена циркулем и линейкой, исходя из множества M , и докажем, что в этом случае она определена над допустимым расширением поля P . Будем доказывать это индукцией по числу шагов построения — операций (П1) — (П5), перечисленных в п. 3 требующихся для построения элемента t .

Предположим вначале, что элемент t строится, исходя из совокупности M , за один шаг. Если это шаг типа (П4) или (П5), то t есть прямая или окружность, которая определена над P по самому

определению этого свойства. В этом случае утверждение теоремы очевидно, поскольку поле P является допустимым расширением самого себя. В оставшихся трех случаях m есть точка пересечения двух линий, каждая из которых есть прямая или окружность, определенная над P . Докажем, что в любом из этих случаев координаты точки m представляются в квадратных радикалах над P и, значит, принадлежат допустимому расширению поля P .

Согласно леммам 1 и 2, каждая из рассматриваемых двух линий может быть задана уравнением вида (5) или (6) с коэффициентами из P . Координаты точки m составляют, стало быть, решение системы уравнений одного из следующих трех типов:

$$\begin{cases} a_1x + b_1y + c_1 = 0, \\ a_2x + b_2y + c_2 = 0; \end{cases} \quad (7)$$

$$\begin{cases} ax + by + c = 0, \\ x^2 + y^2 + px + qy + r = 0; \end{cases} \quad (8)$$

$$\begin{cases} x^2 + y^2 + p_1x + q_1y + r_1 = 0, \\ x^2 + y^2 + p_2x + q_2y + r_2 = 0, \end{cases} \quad (9)$$

причем все коэффициенты уравнений принадлежат полю P .

В случае (П1) координаты точки m определяются из системы типа (7), причем $\begin{vmatrix} a_1b_1 \\ a_2b_2 \end{vmatrix} \neq 0$, поскольку соответствующие прямые не параллельны (и не совпадают). Координаты точки m могут быть найдены по формулам Крамера, откуда видно, что они принадлежат самому полю P .

В случае (П2) координаты точки m определяются из системы типа (8). Выражая из первого уравнения одно неизвестное через другое и подставляя это выражение во второе уравнение, получаем относительно первого неизвестного квадратное уравнение с коэффициентами из P . По известной формуле его корни, а значит, и координаты точки m представляются в квадратных радикалах над P .

В случае (П3) координаты точки m определяются из системы типа (9). Вычитая из первого уравнения второе, мы приходим к системе типа (8). Следовательно, и в этом случае координаты точки m представляются в квадратных радикалах над P .

Предположим теперь, что доказываемое утверждение справедливо для любого построения, осуществляемого за $n - 1$ шагов, и пусть элемент m строится, исходя из совокупности M , за n шагов. Обозначим через m' элемент, добавляемый к M , на первом шаге построения. По доказанному, он определен над некоторым допустимым расширением K поля P . Так как $K \supset P$, то все элементы совокупности $M' = M \cup \{m'\}$ определены над K . Элемент m строится, исходя из совокупности M' , уже за $n - 1$ шагов, и по индуктивному предположению он определен над некоторым допустимым расширением L поля K . Однако поле L можно рассматривать также как допустимое расширение поля P . Следовательно, элемент m

определен над допустимым расширением поля P , что и требовалось доказать.

5. Неразрешимость некоторых задач на построение. Покажем теперь, как с помощью теорем 1 и 2 доказывается неразрешимость некоторых классических задач на построение циркулем и линейкой.

1°. Квадратура круга. *Требуется построить квадрат, равновеликий данному кругу.*

Примем радиус данного круга за единицу измерения. Тогда его площадь будет равна π , и, значит, сторона искомого квадрата должна быть равна $\sqrt{\pi}$.

Выберем систему координат с началом в центре данного круга. Тогда его граничная окружность будет определена над полем $\mathbb{Q}$, так как будет содержать, например, точку $(1; 0)$. Если бы искомым квадрат мог быть построен с помощью циркуля и линейки, то, отложив его сторону на оси абсцисс от начала координат*, можно было бы построить точку $(\sqrt{\pi}; 0)$. По теореме 2 координаты этой точки представлялись бы тогда в квадратных радикалах над полем $\mathbb{Q}$ и, в частности, были бы алгебраическими числами. Однако известно, что число π , а значит и число $\sqrt{\pi}$, не является алгебраическим (это было доказано Линдеманом в 1872 г.). Следовательно, *квадратура круга не может быть выполнена циркулем и линейкой.*

2°. Удвоение куба. *Требуется построить куб, объем которого вдвое больше объема данного куба.*

Для того чтобы трактовать эту задачу как задачу на построение на плоскости, нужно понимать ее следующим образом. В плоскости построения задан отрезок, равный ребру данного куба; требуется построить в этой плоскости отрезок, равный ребру искомого куба.

Примем ребро данного куба за единицу измерения. Тогда ребро искомого куба должно быть равно $\sqrt[3]{2}$.

Выберем систему координат в плоскости таким образом, чтобы один из концов данного отрезка совпадал с началом координат, а другой имел координаты $(1; 0)$. Тогда прямая, на которой лежит этот отрезок (т. е. ось абсцисс), и оба его конца будут определены над $\mathbb{Q}$. Если бы искомым отрезок мог быть построен с помощью циркуля и линейки, то, отложив его на оси абсцисс от начала координат, можно было бы построить точку $(\sqrt[3]{2}; 0)$. По теореме 2 число $\sqrt[3]{2}$ представлялось бы тогда в квадратных радикалах над $\mathbb{Q}$. С другой стороны, это число является корнем многочлена $x^3 - 2 \in \mathbb{Q}[x]$, неприводимого над $\mathbb{Q}$ (см. § 1), и по теореме 1 не может представляться в квадратных радикалах над $\mathbb{Q}$. Следовательно, *удвоение куба не может быть выполнено циркулем и линейкой.*

3°. Трисекция угла. *Требуется разделить данный угол на три равные по величине части.*

* Это можно сделать с помощью операций типов (П1) — (П5), перечисленных в п. 3.

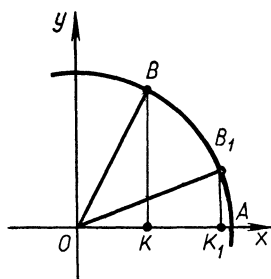


Рис. 17

Очевидно, что существуют углы, которые можно разделить на три равные по величине части с помощью циркуля и линейки, например прямой угол. Задачу, однако, следует понимать таким образом, что требуется указать алгоритм трисекции угла с помощью циркуля и линейки, применимый к любому углу. Неразрешимость этой задачи, очевидно, будет доказана, если мы докажем существование конкретных углов, трисекция которых не может быть выполнена циркулем и линейкой.

Пусть O — вершина данного угла, A и B — точки пересечения его сторон с некоторой окружностью c с центром в точке O . Обозначим через K проекцию точки B на прямую OA (рис. 17). Если заданы точки O , A и K , то точка B может быть построена с помощью циркуля и линейки как точка пересечения окружности c с перпендикуляром к прямой OA , восставленным в точке K . Таким образом, задание угла AOB равносильно заданию точек O , A и K .

Пусть теперь B_1 — такая точка окружности c , что $\widehat{AOB_1} = \frac{1}{3}\widehat{AOB}$, и K_1 — проекция точки B_1 на прямую OA . Построение угла AOB_1 равносильно построению точки B_1 . Поэтому задача о трисекции угла AOB с помощью циркуля и линейки может пониматься как задача о построении точки K_1 по точкам O , A и K .

Примем радиус окружности c за единицу измерения и выберем систему координат таким образом, чтобы точка O совпадала с началом координат, а точка A лежала на положительной части оси абсцисс. Тогда точка A будет иметь координаты $(1; 0)$, а точка K — координаты $(\cos \varphi; 0)$, где φ — мера угла AOB в радианах. Все три точки: O , A , K — будут определены над полем $P = \mathbb{Q}(\cos \varphi)$. Точка K_1 имеет координаты $(\cos \frac{\varphi}{3}; 0)$. Если она может быть построена по точкам O , A и K с помощью циркуля и линейки, то по теореме 2 число $\alpha = \cos \frac{\varphi}{3}$ должно представляться в квадратных радикалах над полем P . По известной формуле

$$\cos \varphi = 4 \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3},$$

так что α является корнем многочлена

$$f(x) = 4x^3 - 3x - \cos \varphi.$$

Если многочлен $f(x)$ неприводим над полем P , то по теореме 1 число α не представляется в квадратных радикалах над P и, значит, трисекция данного угла не может быть осуществлена циркулем и линейкой.

Возьмем, например, $\varphi = \frac{\pi}{3}$. Тогда $\cos \varphi = \frac{1}{2} \in \mathbb{Q}$, так что $P = \mathbb{Q}$. Многочлен $f(x)$ имеет вид

$$4x^3 - 3x - \frac{1}{2} = \frac{1}{2}(8x^3 - 6x - 1).$$

Согласно п. 1 § 1, его рациональными корнями могут быть только числа $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$. Проверка показывает, что ни

одно из них не является корнем. Следовательно, многочлен $f(x)$ не имеет рациональных корней и, значит, неприводим над $\mathbb{Q}$. Согласно предыдущему, отсюда вытекает, что *трисекция угла $\frac{\pi}{3}$ не может быть осуществлена циркулем и линейкой.*

4°. Деление круга на n равных частей, или, что то же, построение правильного n -угольника.

Пусть c — окружность, которую требуется разделить на n равных по величине частей. Примем ее радиус за единицу измерения и выберем произвольную систему координат с началом в центре этой окружности. Обозначим через A точку пересечения с окружностью c положительной части оси абсцисс и через B такую точку окружности c , что $\widehat{AOB} = \frac{2\pi}{n}$ (рис. 18). Задача может быть сформулирована следующим образом: по точкам O и A построить точку B .

Точка O по построению совпадает с началом координат, а точка A имеет координаты $(1; 0)$, так что обе эти точки определены над $\mathbb{Q}$. Точка B имеет координаты $(\cos \frac{2\pi}{n}; \sin \frac{2\pi}{n})$. Согласно теореме 2, для того чтобы она могла быть построена по точкам O и A с помощью циркуля и линейки, необходимо, чтобы числа $\cos \frac{2\pi}{n}$ и $\sin \frac{2\pi}{n}$ представлялись в квадратных радикалах над $\mathbb{Q}$. Если это имеет место, то и комплексное число $\alpha = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ представляется в квадратных радикалах над $\mathbb{Q}$ (поскольку $i = \sqrt{-1}$). Число α является корнем n -й степени из единицы. Если n — простое, то минимальный многочлен числа α равен

$$f(x) = x^{n-1} + x^{n-2} + \dots + x + 1$$

(см. п. 1 § 2). Из теоремы 1 следует, что α может представляться в квадратных радикалах над $\mathbb{Q}$, если $n - 1$ есть степень двойки.

Таким образом, *если n — простое число, не имеющее вида $2^q + 1$, то правильный n -угольник не может быть построен циркулем и линейкой.* Например, правильный семиугольник не может быть построен циркулем и линейкой.

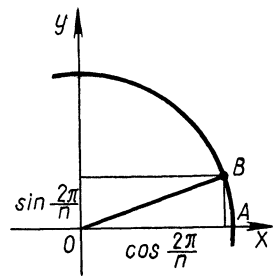


Рис. 18

6. О доказательстве разрешимости задач на построение. В п. 4 было найдено необходимое условие разрешимости задачи на построение циркулем и линейкой (теорема 2). При надлежащем выборе поля P это условие является и достаточным.

Будем предполагать, что задано некоторое множество M точек, прямых и окружностей, содержащее по меньшей мере две точки, скажем O и A . Примем расстояние между этими точками за единицу измерения и выберем систему координат так, чтобы точка O совпадала с началом координат, а точка A лежала на положительной части оси абсцисс.

Будем говорить, что действительное число α может быть построено циркулем и линейкой, исходя из множества M , если может быть построена точка $(\alpha; 0)$. Заметим, что для этого достаточно построить любой отрезок длины $|\alpha|$: отложив его на оси абсцисс от точки O в ту или другую сторону, мы сможем тогда построить точку $(\alpha; 0)$.

Легко видеть, что точка может быть построена циркулем и линейкой, исходя из множества M , тогда и только тогда, когда могут быть построены обе ее координаты.

Введем теперь понятие координат прямой. Пусть прямая l задается уравнением (5). Если $a \neq 0$, то ее координатами первого рода назовем числа $b_1 = \frac{b}{a}$

и $c_1 = \frac{c}{a}$. Эти числа не зависят от выбора уравнения, которое определено с точностью до пропорциональности, и однозначно определяют прямую l . Аналогично, если $b \neq 0$, то координатами второго рода прямой l назовем числа $a_2 = \frac{a}{b}$

и $c_2 = \frac{c}{b}$. Если $a \neq 0$ и $b \neq 0$, то для прямой l определены координаты обоих родов. Они связаны соотношениями

$$a_2 = \frac{1}{b_1}, \quad c_2 = \frac{c_1}{b_1}.$$

Нетрудно показать, что прямая может быть построена циркулем и линейкой, исходя из множества M тогда и только тогда, когда могут быть построены обе ее координаты (любого рода).

Координатами окружности назовем ее радиус и координаты центра (всего три числа). Окружность может быть построена циркулем и линейкой, исходя из множества M и только тогда, когда могут быть построены все ее координаты.

Рассмотрим теперь совокупность всех чисел, которые могут быть получены с помощью рациональных операций из координат всех точек, прямых и окружностей, принадлежащих множеству M . Эта совокупность является полем; назовем его *полем определения множества M* .

При сделанных предположениях справедлива следующая теорема, которую мы приводим без доказательства.

Теорема 3. *Для того чтобы число α могло быть построено циркулем и линейкой, исходя из данного множества M точек, прямых и окружностей, необходимо и достаточно, чтобы оно представлялось в квадратных радикалах над полем определения множества M .*

Чтобы доказывать разрешимость задач на построение с помощью этой теоремы, желательно иметь какой-то простой критерий представимости числа в квадратных радикалах над данным полем. Теорема 1 дает необходимое, но не достаточное условие для этого. Необходимое и достаточное условие представимости в квадратных радикалах доказывается в теории Галуа. Мы приведем здесь без доказательства лишь частный случай соответствующего утверждения.

Пусть α — число, алгебраическое над полем P . Предположим, что все корни его минимального многочлена $f(x)$ над полем P лежат в поле $P(\alpha)$. Тогда для представимости числа α в квадратных радикалах над полем P необходимо и достаточно, чтобы степень многочлена $f(x)$ была степенью двойки.

Рассмотрим, например, число $\alpha = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, где n — простое.

Корнями его минимального многочлена (над $\mathbb{Q}$)

$$f(x) = x^{n-1} + x^{n-2} + \dots + x + 1$$

являются все корни n -й степени из единицы, кроме самой единицы. Все они являются степенями числа α и потому лежат в поле $\mathbb{Q}(\alpha)$. Следовательно, α представляется в квадратных радикалах над $\mathbb{Q}$ тогда и только тогда, когда $n-1$ есть степень двойки, т. е. n — простое число Ферма. Это приводит, в частности, к следующему результату: если n — простое число Ферма, то правильный n -угольник может быть построен циркулем и линейкой (см. пример 4^о предыдущего пункта). В частности, правильный 17-угольник может быть построен циркулем и линейкой. Способ такого построения был предложен Гауссом.

Вопросы для самопроверки

1. В чем разница между разрешимостью в радикалах конкретного алгебраического уравнения и разрешимостью в радикалах общего уравнения степени n ?

2. Докажите, что всякое алгебраическое уравнение с действительными коэффициентами разрешимо в радикалах над $\mathbb{R}$.

3. Докажите, что всякое алгебраическое уравнение четвертой степени с рациональными коэффициентами разрешимо в радикалах над $\mathbb{Q}$.

4. Укажите необходимое условие разрешимости алгебраического уравнения в квадратных радикалах.

5. В каком случае кубическое уравнение разрешимо в квадратных радикалах?

6. Как ставится задача на построение циркулем и линейкой?

7. Укажите, как при помощи операций (П1) — (П5), перечисленных в п. 3, описать окружность с центром в данной точке радиусом, равным данному отрезку.

8. Пусть n — простое число. Каково необходимое и достаточное условие того, чтобы правильный n -угольник мог быть построен циркулем и линейкой?

9. Что такое допустимое расширение числового поля?

10. Укажите необходимое условие разрешимости задачи на построение циркулем и линейкой.

11. Докажите, что с помощью циркуля и линейки нельзя построить отрезок, равный длине данной окружности.

12. Докажите, что с помощью циркуля и линейки нельзя разделить угол $\frac{2\pi}{3}$ на три равные по величине части.

13. Докажите, что с помощью циркуля и линейки нельзя построить угол, равный $\frac{2\pi}{11}$.

ОТВЕТЫ

ГЛАВА I

- § 1. 1. а) $f(x) = (x^3 + x^2 + 10x + 30)(x - 4) + 136$, $f(x_0) = 136$; б) $f(x) = (x^3 + x^2 - 4x)(x + 1) + 1$, $f(x_0) = 1$. 2. а) $7 + 5i$; б) $-1 - 44i$. 3. а) $x \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & \\ \hline \end{array}$; б) $x \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & 5 & 6 & \\ \hline \end{array}$. 4. а) $x^6 + 3x^5 + 2x^4 - 3x^3 - x^2 - x - 3$; б) 0.
- § 2. 1. а) 3; б) 4. 2. а) 4; б) 1. 3. а) $x^4 + 4x^3 - 7x^2 - 22x + 24$; б) $x^4 + (3-i)x^3 + (3-3i)x^2 + (1-3i)x - i$; в) $x^4 - (6+2i)x^3 + (12+10i)x^2 - (8+16i)x + 8i$. 4. а) $\frac{2}{3}$ и $-\frac{2}{3}$; б) $-4(1+i)$ и $3+i$; в) a^2 и $(-1)^n b$. 5. а) 0; б) -1 . 6. $\sqrt{5}$. 7. а) $x \equiv 2 \pmod{5}$; б) $x \not\equiv 0 \pmod{3}$; в) $x \equiv \pm 3 \pmod{11}$; г) решений нет.

ГЛАВА II

- § 1. 1. а) Неполное частное $2x^2 + 3x + 11$, остаток $25x - 5$; б) неполное частное $\frac{1}{9}(3x - 7)$, остаток $-\frac{1}{9}(26x + 2)$. 2. а) $x + 1$; б) $x^3 - x + 1$. 3. а) $x^2 + 1$; б) $x^3 + 1$. 4. а) $x^2 - 2 = -(x + 1)(x^4 + 2x^3 - x^2 - 4x - 2) + (x + 2) \times (x^4 + x^3 - x^2 - 2x - 2)$; б) $1 = x(3x^3 - 2x^2 + x + 2) - (3x^2 + x - 1)(x^2 - x + 1)$. 5. а) $1 = \frac{1}{3}(-16x^2 + 37x + 26)(x^4 - 4x^3 + 1) + \frac{1}{3}(16x^3 - 53x^2 - 37x - 23)(x^3 - 3x^2 + 1)$; б) $x^4 = (9x^2 - 26x - 21)(x^4 - 2x^3 - 4x^2 + 6x + 1) - (9x^3 - 44x^2 + 39x + 7)(x^3 - 5x - 3)$; в) $2x - 1 = -(6x^2 - 11x + 4)x^3 + (6x^3 + x^2 - 1)(x - 1)^2$; г) $1 = \frac{1}{24}(3x^2 + 11x + 12)(x - 1)(x - 2) - \frac{1}{24}(3x - 7)x(x + 1)(x + 2)$. 6. а) $3x^7 - 6x^6 + 2x^5 + 23x^4 - 37x^3 + 23x^2 + 12x - 10$; б) $x^6 - 2\sqrt{2}x^5 - 11x^4 + 20\sqrt{2}x^3 + 11x^2 - 2\sqrt{2}x - 1$. 7. а) -7 ; б) 0.

- § 2. 1. Нормированные неприводимые многочлены не выше третьей степени: x , $x + 1$, $x - 1$, $x^2 + 1$, $x^2 + x - 1$, $x^2 - x - 1$, $x^3 - x + 1$, $x^3 + x^2 - x + 1$, $x^3 - x^2 + 1$, $x^3 - x^2 + x + 1$, $x^3 - x - 1$, $x^3 + x^2 - 1$, $x^3 + x^2 + x - 1$, $x^3 - x^2 - x - 1$. Имеется 18 нормированных неприводимых многочленов четвертой степени. 2. 40. 3. а) $x(x^3 - 2)$; б) $x^2 + 2$. 4. а) $(x - 1)^2(x + i)$; б) $x^2 - x + 1$. 5. а) $x^2 - 2x + 2$ (кратности 2); б) $x - 1$ (кратности 3) и $x + 3$ (кратности 2). 6. а) -1 (кратности 4); б) 1 (кратности 3) и $\pm i$ (кратности 2). 7. а) При $a = \pm 2$; б) при $a = 0, -3, 125$.

ГЛАВА III

§ 1. 1. а) $x_1^2 x_2^2 x_3^2$, $x_1^3 x_2^2 + x_2^3 x_3^2 + x_3^3 x_1^2$, $x_1^3 x_3 + x_2^3 x_1 + x_3^3 x_2$, $x_1 x_2 x_3$; б) x_1^8 ,
 $-2x_1^4 x_2 x_3$, $2x_1^4 + x_2^2 x_3^2 - 2x_2 x_3$, 1. 2. а) $-x_1^3 + x_1^2 x_2^2 x_3^2 + 2x_1^2 x_3^4 + x_2^4$; б) $x_1^4 x_2 x_3 -$
 $-x_1^3 x_2^3 - x_1^3 x_3^3 + x_1 x_2^4 x_3 + x_1 x_2 x_3^4 - x_2^3 x_3^3$.

§ 2. 1. а) $\sigma_1^3 - 3\sigma_1\sigma_2$; б) $\sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\sigma_2^2$; в) $\sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 +$
 $+18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2$; г) $\sigma_1^4 - 4\sigma_1^2\sigma_2 + 8\sigma_1\sigma_3$; д) $\sigma_3^2 + \sigma_1\sigma_2^2 - 2\sigma_1^2\sigma_3 - \sigma_2\sigma_3 +$
 $+ \sigma_1^4 - 3\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + \sigma_1\sigma_2 - \sigma_3$. 2. а) $\sigma_4^2 + \sigma_3^2 - 2\sigma_2\sigma_4 + \sigma_2^2 + 2\sigma_4 - 2\sigma_1\sigma_3 +$
 $+ \sigma_1^2 - 2\sigma_2 + 1$; б) $\sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2$. 3. а) -35 ; б) 16. 4. а) $x^3 - 3x^2 + 2x - 1$;
б) $x^4 - 4x^3 + 10x^2 - x + 9$. 5. а) $(-2; 1; 1)$, $(1; -2; 1)$, $(1; 1; -2)$; б) $(1; 2; -2)$,
 $(1; -2; 2)$, $(2; 1; -2)$, $(2; -2; 1)$, $(-2; 1; 2)$, $(-2; 2; 1)$.

§ 3. 1. а) $y^6 - 4y^4 + 3y^2 - 12y + 12 = 0$; б) $5y^5 - 7y^4 + 6y^3 - 2y^2 - y -$
 $-1 = 0$; в) $y^3 + 4y^2 - y - 4 = 0$. 3. а) $(1; -1)$, $(-1; 1)$, $(2; 2)$; б) $(0; 1)$, $(0; 3)$,
 $(-1, 2)$, $(-1; 3)$, $(2; 1 \pm i\sqrt{2})$.

ГЛАВА IV

§ 1. 1. а) $-i$; б) $1 + 2i$; в) $-6 + 7i$. 2. а) $r = 2$, $\varphi = -\frac{\pi}{2}$; б) $r = \sqrt{2}$, $\varphi = \frac{3\pi}{4}$;
в) $r = \sqrt{2}$, $\varphi = -\frac{3\pi}{4}$; г) $r = \sqrt{3}$, $\varphi = -\frac{\pi}{3}$. 3. а) $3(\cos 0 + i \sin 0)$;
б) $\sqrt{2} \left(\cos \left(-\frac{3\pi}{4} \right) + i \sin \left(-\frac{3\pi}{4} \right) \right)$; в) $2 \left(\cos \left(-\frac{\pi}{3} \right) + i \sin \left(-\frac{\pi}{3} \right) \right)$; г) $2 \left(\cos \frac{\pi}{6} + \right.$
 $\left. + i \sin \frac{\pi}{6} \right)$; д) $\sqrt{10} (\cos \varphi + i \sin \varphi)$, где $\varphi = \arctg \frac{1}{3}$; е) $\sqrt{17} (\cos \varphi + i \sin \varphi)$,
где $\varphi = \pi - \arctg \frac{1}{4}$. 4. а) 0 и $-1 + 3i$; б) либо $-3 + 4i$ и $5i$, либо $-1 - 2i$
и $2 - i$. 5. а) $2^{19} (-1 + i\sqrt{3})$; б) 2^{12} ; в) $2^7 (1 + i)$; г) $2^{-9}i$. 6. а) $\cos^5 \varphi -$
 $-10 \cos^3 \varphi \sin^2 \varphi + 5 \cos \varphi \sin^4 \varphi$; б) $6 \cos^5 \varphi \sin \varphi - 20 \cos^3 \varphi \sin^3 \varphi + 6 \cos \varphi \times$
 $\times \sin^5 \varphi$. 7. а) $-i$, $\frac{\sqrt{3}+i}{2}$, $\frac{-\sqrt{3}+i}{2}$; б) $-1+i$, $\frac{1+\sqrt{3}}{2}$, $\frac{\sqrt{3}-1}{2}i$, $\frac{1-\sqrt{3}}{2}$,
 $-\frac{1+\sqrt{3}}{2}i$; в) $1+i$, $1-i$, $-1+i$, $-1-i$; г) 1 , -1 , $-\frac{1}{2} + \frac{i\sqrt{3}}{2}$,
 $-\frac{1}{2} - \frac{i\sqrt{3}}{2}$, $\frac{1}{2} + \frac{i\sqrt{3}}{2}$, $\frac{1}{2} - \frac{i\sqrt{3}}{2}$; д) $\frac{1}{\sqrt[12]{2}} \left(\cos \frac{24k+19}{72} \pi + \right.$
 $\left. + i \sin \frac{24k+19}{72} \pi \right)$, где $k = 0, 1, 2, 3, 4, 5$; е) $\frac{1}{\sqrt[16]{2}} \left(\cos \frac{24k+5}{96} \pi + \right.$
 $\left. + i \sin \frac{24k+5}{96} \pi \right)$, где $k = 0, 1, 2, 3, 4, 5, 6, 7$.

§ 2. а) $(x-1-i)(x-1+i)(x+1-i)(x+1+i)$; б) $(x-1)(x-2) \times$
 $\times (x-3)$; в) $\left(x+1 - \sqrt{\frac{\sqrt{2}+1}{2}} - i \sqrt{\frac{\sqrt{2}-1}{2}} \right) \left(x+1 - \sqrt{\frac{\sqrt{2}+1}{2}} + \right.$

$$+ i \sqrt{\frac{\sqrt{2}-1}{2}} \left(x+1 + \sqrt{\frac{\sqrt{2}+1}{2}} - i \sqrt{\frac{\sqrt{2}-1}{2}} \right) \left(x+1 + \sqrt{\frac{\sqrt{2}+1}{2}} + i \sqrt{\frac{\sqrt{2}-1}{2}} \right); \quad \text{г)} (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3}) \times \\ \times (x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}).$$

§ 3. 1. а) $(x^2 + 3)(x^2 - 3x + 3)(x^2 + 3x + 3)$; б) $(x - \sqrt[3]{2})(x^2 - 2x\sqrt[3]{2}\cos\frac{2\pi}{9} + \sqrt[3]{4})(x^2 - 2x\sqrt[3]{2}\cos\frac{4\pi}{9} + \sqrt[3]{4})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})(x^2 + 2x\sqrt[3]{2}\cos\frac{\pi}{9} + \sqrt[3]{4})$; в) $(x^2 - 2x\cos\frac{2\pi}{9} + 1)(x^2 - 2x\cos\frac{4\pi}{9} + 1)(x^2 + 2x\cos\frac{\pi}{9} + 1)$; г) $(x^2 - 2x\cos\frac{\pi}{10} + 1)(x^2 - 2x\cos\frac{3\pi}{10} + 1)(x^2 + 2x\cos\frac{\pi}{10} + 1)(x^2 + 2x\cos\frac{3\pi}{10} + 1)$. 2. а) 1 (кратности 2), 2, $1 \pm i$; б) $\pm i$ (кратности 2), $-1 \pm i$. 3. а) 1,73; б) 1,23.

§ 4. 1. а) $-3, \frac{3}{2} \pm i\sqrt{\frac{3}{2}}$; б) $-7, -1 \pm i\sqrt{3}$; в) $-\sqrt[3]{4} + \sqrt[3]{2}, \frac{1}{2}(\sqrt[3]{4} - \sqrt[3]{2}) \pm \frac{i\sqrt{3}}{2}(\sqrt[3]{4} + \sqrt[3]{2})$. 2. а) 2,09; б) 2,89.

ГЛАВА V

§ 1. 1. а) 2; б) -3 ; в) $-2, 3$; г) $-3, \frac{1}{2}$; д) $\frac{5}{2}, -\frac{3}{4}$; е) рациональных корней нет.

§ 2. а) $\frac{1}{3}(\alpha^2 - \alpha + 1)$; б) $17\alpha^2 - 3\alpha + 55$; в) $-3\alpha^3 + 8\alpha^2 - 10\alpha + 3$; г) $\frac{1}{7}(\alpha^2 - 4\alpha + 4)$.

§ 3. а) $x^4 + 6x^3 + 19x^2 + 30x + 19$; б) $x^6 - 13x^4 + 2x^3 + 76x^2 + 32x - 179$; в) $x^6 - 9x^5 + 30x^4 - 49x^3 + 48x^2 - 51x + 41$.

О Г Л А В Л Е Н И Е

Предисловие	3
Глава I. Многочлены от одной переменной	5
§ 1. Понятие многочлена	—
§ 2. Корни многочлена	21
Глава II. Теория делимости в кольце многочленов	33
§ 1. Наибольший общий делитель	—
§ 2. Разложение на неприводимые множители	48
§ 3. Многочлены над кольцом с однозначным разложением на простые множители	63
§ 4. Поле рациональных дробей	69
Глава III. Многочлены от нескольких переменных	72
§ 1. Кольцо многочленов от n переменных	—
§ 2. Симметрические многочлены	85
§ 3. Системы алгебраических уравнений	97
Глава IV. Многочлены над полями C и R . Алгебраические уравнения с комплексными и действительными коэффициентами	104
§ 1. Комплексные числа	—
§ 2. Теорема о существовании корня в поле комплексных чисел	117
§ 3. Многочлены и алгебраические уравнения с действительными коэффициентами	122
§ 4. Алгебраические уравнения третьей и четвертой степени (решение в радикалах)	127
Глава V. Многочлены над Q . Алгебраические уравнения с рациональными коэффициентами	137
§ 1. Разложение на множители в кольце многочленов с рациональными коэффициентами	—
§ 2. Алгебраические числа	143
§ 3. Конечные расширения числовых полей	152
§ 4. Разрешимость уравнений в радикалах	160
Ответы	172

Эрнест Борисович Винберг
АЛГЕБРА МНОГОЧЛЕНОВ

Редактор *Л. В. Туркестанская*
Художественный редактор *Е. Н. Карасик*
Технические редакторы *В. Ф. Коскина* и *М. М. Широкова*
Корректоры *К. А. Иванова*, *О. В. Ивашкина*

Сдано в набор 20.04.79. Подписано к печати 29.01.80. 60×90¹/₁₆. Бумага типограф. № 2.
Литер. гарн. Высокая печать. Условн. печ. л. 11. Уч.-изд. л. 10/12. Тираж 35 000 экз.
Заказ № 98. Цена 45 коп.

Ордена Трудового Красного Знамени издательство «Просвещение» Государственного комитета РСФСР по делам издательств, полиграфии и книжной торговли. Москва, 3-й проезд Марьиной рощи, 41

Саратовский ордена Трудового Красного Знамени полиграфический комбинат Росглаво-лиграфпрома Государственного комитета РСФСР по делам издательств, полиграфии и книжной торговли. Саратов, ул. Чернышевского, 59.

