С. В. Ларин

АЛГЕБРА: МНОГОЧЛЕНЫ

УЧЕБНОЕ ПОСОБИЕ ДЛЯ СПО

2-е издание, исправленное и дополненное

Рекомендовано Учебно-методическим отделом среднего профессионального образования в качестве учебного пособия для студентов образовательных учреждений среднего профессионального образования

Книга доступна в электронной библиотечной системе biblio-online.ru

Москва ▪ Юрайт ▪ 2019

УДК 511.2(075.32)
ББК 22.132я723
Л25

***Автор*:**

Ларин Сергей Васильевич — кандидат физико-математических наук, профессор кафедры алгебры, геометрии и методики их преподавания Института математики, физики и информатики Красноярского государственного педагогического университета имени В. П. Астафьева.

Ларин, С. В.

Л25 Алгебра: многочлены : учеб. пособие для СПО / С. В. Ларин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 136 с. — (Серия : Профессиональное образование).

ISBN 978-5-534-07828-2

В пособии изложен материал по многочленам в рамках дисциплины предметной подготовки «Алгебра и теория чисел» Данный материал обеспечивает способность студента осуществлять профессиональную деятельность в области преподавания соответствующих разделов алгебры. В пособии рассмотрены теория делимости многочленов, вопросы, связанные с нахождением корней, многочлены от нескольких переменных, симметрические многочлены, результант и дискриминант. Большое внимание уделяется примерам. Они предваряют введение новых понятий, на них отрабатывается и закрепляется изученный материал.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта среднего профессионального образования и профессиональным требованиям.

Для студентов математических специальностей педагогических коллеждей и ссузов, практикующих учителей школ и колледжей, а также всех интересующихся.

УДК 511.2(075.32)
ББК 22.132я723

ISBN 978-5-534-07828-2

Оглавление

Предисловие

Учебное пособие адресовано в первую очередь студентам математических специальностей педагогических колледжей и ссузов и содержит материал семестрового курса по многочленам в рамках дисциплины «Алгебра» («Алгебра и теория чисел»). Вместе с тем изложение имеет целостный, замкнутый характер и может быть использовано всеми желающими для первичного знакомства с многочленами как в плане теории, так и в плане вычислительных приложений.

Многочлены от одной переменной рассматриваются с точки зрения теории делимости и с точки зрения нахождения корней. В теории многочленов от нескольких переменных центральное место занимает теория симметрических многочленов. С использованием основной теоремы о симметрических многочленах приводится «самое алгебраическое» доказательство основной теоремы алгебры, в котором четко указывается момент использования свойства непрерывности системы действительных чисел.

При доказательстве теоремы о делении с остатком рассматривается школьный алгоритм деления «уголком» многочлена на многочлен. Школьный аспект присутствует при освещении разложения многочленов на множители, формул Виета, вопросов нахождения рациональных корней многочленов с целыми коэффициентами, приложений симметрических многочленов. Так что пособие может оказаться полезным школьным учителям математики. Стремясь избежать излишней формализации, мы формальные обоснования отодвигаем на конец изложения соответствующего материала.

Отметим основополагающую роль примеров. Они не только иллюстрируют теоретические положения, но и подготавливают введение новых понятий. Зачастую доказательства теорем повторяют в общем виде те же рассуждения, которые накануне проводились при решении конкретных числовых примеров.

В результате усвоения изложенного материала студент должен освоить следующие компетенции:

трудовые действия

- владения вычислительными алгоритмами;
- приложением теории многочленов к решению вычислительных задач;

необходимые умения

- доказывать основные теоремы о многочленах;
- решать задачи, связанные с многочленами;
- находить корни многочлена;
- производить разложение многочлена на множители;

необходимые знания

- формулировок определений основных понятий и теорем;
- основных операций с многочленами.

В конце каждого из основных пунктов приведены «Контрольные вопросы» и «Задачи», которые призваны проверить и закрепить полученные знания. Контрольные вопросы чаще всего приведены не в тривиальной форме типа «что называется» или «как формулируется», а с некоторой изобретательностью, позволяющей выявить владение знаниями.

В тексте используются значки: $\vdots$ (делится), $\Leftrightarrow$ (тогда и только тогда, когда), $\Rightarrow$ (отсюда следует), ($\Rightarrow$) — доказательство необходимости, ($\Leftarrow$) — доказательство достаточности. Знаком * отмечены пункты дополнительного материала.

Автор выражает благодарность доктору физико-математических наук, профессору М. М. Глухову, доктору физико-математических наук, профессору Б. В. Яковлеву, а также рецензентам доктору физико-математических наук, профессору В. М. Левчуку и доктору физико-математических наук, профессору Н. Н. Осипову за ряд ценных советов и замечаний.

Глава 1
МНОГОЧЛЕНЫ НАД ОБЛАСТЬЮ ЦЕЛОСТНОСТИ

1.1. Основные понятия теории многочленов

1.1.1. Многочлены, их сложение и умножение

Нашей ближайшей целью является уточнение понятия многочлена. На базе школьных знаний приведем примеры многочленов: $3x^2 - 2x + 5$ — многочлен степени 2 с целыми коэффициентами, $x^3 + \frac{2}{3}x + 5$ — многочлен степени 3 с рациональными коэффициентами, $0x^3 + \sqrt{2}x - 7$ — многочлен первой степени с действительными коэффициентами, -147 — многочлен степени 0, наконец, 0 — нулевой многочлен. Уточним область значений для коэффициентов многочленов, которые мы будем рассматривать в дальнейшем. Начнем с определения базовых понятий.

Определение 1.1. *Кольцом* называется непустое множество K с определенными на нем бинарными операциями сложения и умножения, которые удовлетворяют следующим условиям:

1) сложение ассоциативно и коммутативно: $(a + b) + c = a + (b + c)$ и $a + b = b + a$ для любых $a, b, c \in K$;

2) существует элемент $0 \in K$, называемый нулем, такой что $a + 0 = a$ для любого $a \in K$;

3) для всякого элемента $a \in K$ существует элемент $-a \in K$, называемый противоположным для a, такой что $a + (-a) = 0$;

4) умножение ассоциативно: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых $a, b, c \in K$.

5) умножение дистрибутивно относительно сложения: $(a + b) \cdot c = a \cdot c + b \cdot c$ и $c \cdot (a + b) = c \cdot a + c \cdot b$ для любых $a, b, c \in K$.

Кольцо K называется *коммутативным*, если умножение в нем коммутативно: $a \cdot b = b \cdot a$ для любых $a, b \in K$.

Кольцо K называется *кольцом с единицей*, если существует элемент $1 \in K$, называемый единицей, такой что $a \cdot 1 = 1 \cdot a = a$.

Элементы $a, b \in K$ называются *делителями нуля*, если $a \neq 0$, $b \neq 0$, но $a \cdot b = 0$. Если же в кольце нет таких элементов, то оно называется *кольцом без делителей нуля*.

Определение 1.2. *Полем* называется коммутативное кольцо P с единицей, отличной от нуля, в котором всякий ненулевой элемент имеет обратный, т.е. для любого $0 \neq a \in P$ существует элемент $a^{-1} \in P$, такой что $a \cdot a^{-1} = 1$.

Глядя на кольцо целых чисел, введем обобщающее понятие.

Определение 1.3. *Областью целостности* называется коммутативное кольцо с единицей, отличной от нуля, и без делителей нуля.

Примерами областей целостности являются кольцо целых чисел $\mathbb{Z}$, числовые поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Вообще, всякое поле является областью целостности. Не является областью целостности, например, кольцо четных целых чисел, поскольку не содержит единицы. Но многочлены с четными коэффициентами входят в область многочленов с любыми целыми коэффициентами, так что не выпадают из нашего рассмотрения. Не является областью целостности кольцо квадратных матриц, поскольку оно не коммутативно (хотя в линейной алгебре рассматриваются «значения многочленов от матриц»). Заметим, что нулевое кольцо — это единственное кольцо, в котором нуль равен единице. Оно не является областью целостности.

Определение 1.4. *Многочленом над областью целостности K* называется формальное выражение вида $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ (*стандартная запись многочлена*), где a_n, a_{n-1}, ..., a_1, a_0 являются элементами из K и называются *коэффициентами многочлена*, буква x обозначает *переменную* с областью определения K. Каждое слагаемое называется *членом многочлена*. Отсюда происходят названия «одночлен», «двучлен», «трехчлен». Слагаемое a_0 называется *свободным членом* (он «свободен» от переменной x). Кратко многочлен обозначается $f(x)$, а множество всех многочленов над областью целостности K обозначается $K[x]$. Если все коэффициенты многочлена равны нулю, то он называется *нулевым*. Если же в приведенной выше стандартной записи многочлена коэффициент $a_n \neq 0$, то он называется *старшим коэффициентом*, соответствующий одночлен $a_n x^n$ называется *старшим членом многочлена*, а n называется *степенью многочлена*. Таким образом, нулевой многочлен — единственный многочлен без степени. Многочлен называется *приве-*

денным (или *нормированным*), если его старший коэффициент равен 1. Считаем, что $x^0 = 1$. По обыкновению, коэффициент ± 1 при переменной не записывают, считая $\pm 1x^k = \pm x^k$, $k = 1, 2, \ldots$.

Договоримся считать, что многочлен не изменится, если к нему приписать любое количество недостающих одночленов с нулевыми коэффициентами, а также исключить из записи такие одночлены. Таким образом, в записи многочлена $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ по умолчанию считаем, что $0 = a_{n+1} = a_{n+2} = \ldots$. При этой договоренности можно сказать, что *два многочлена равны* (*алгебраически*), если равны их соответствующие коэффициенты.

Определим сложение многочленов:

$$(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0) = \\ = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0).$$

Таким образом, чтобы *сложить* два многочлена, нужно сложить их соответствующие коэффициенты. В записи суммы двух многочленов слагаемые $a_i x^i$ и $b_i x^i$, $i = 0, 1, \ldots, n$, называются *подобными*, а нахождение их суммы $a_i x^i + b_i x^i = (a_i + b_i)x^i$ называется *приведением подобных*. Следовательно, сложение многочленов сводится к приведению подобных.

Заметим, что *степень суммы многочленов не превосходит степени каждого из многочленов-слагаемых*.

Определим умножение многочленов, положив

$$(a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0) \cdot (b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0) = \\ = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \ldots + c_1 x + c_0,$$

где $c_k = a_k b_0 + a_{k-1}b_1 + \ldots + a_1 b_{k-1} + a_0 b_k = \sum\limits_{i+j=k} a_i b_j$ для $k = 0, 1, \ldots$ (напомним, что $0 = a_{m+1} = a_{m+2} = \ldots$, $0 = b_{n+1} = b_{n+2} = \ldots$). Если $a_m \neq 0$ и $b_n \neq 0$, то $c_{m+n} = a_m b_n \neq 0$, поскольку в области целостности нет делителей нуля. При этом $c_{m+n+1} = 0$, $c_{m+n+2} = 0, \ldots$. Отсюда делаем вывод, что *степень произведения двух многочленов равна сумме степеней перемножаемых многочленов*. Таким образом,

$$(a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0) \cdot (b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0) = \\ = a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1}b_n)x^{m+n-1} + \ldots + (a_1 b_0 + a_0 b_1)x + a_0 b_0.$$

В частности, для одночленов получаем

$$a_i x^i \cdot b_j x^j = a_i b_j x^{i+j},\ i, j = 0, 1, \ldots .$$

Из определения подмечаем правило умножения многочленов: *чтобы первый многочлен умножить на второй, нужно каждый член первого многочлена умножить на каждый член второго многочлена, записать сумму полученных одночленов и привести подобные.*

Теорема 1.1. *Множество всех многочленов $K[x]$ над областью целостности K относительно сложения и умножения многочленов само является областью целостности.*

Доказательство. Поскольку при сложении многочленов складываются их соответствующие коэффициенты, то ассоциативность и коммутативность сложения многочленов вытекает из аналогичных свойств сложения элементов области целостности K. Нулем и единицей в $K[x]$ будут, соответственно, нулевой многочлен 0 и $1 \in K$.

Докажем ассоциативность умножения многочленов. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$, $g = b_n x^n + \ldots + b_1 x + b_0$, $h = c_n x^n + \ldots + c_1 x + c_0$ (здесь мы не предполагаем, что $a_n \neq 0$ и $b_n \neq 0$). Докажем, что $(f \cdot g) \cdot h = f \cdot (g \cdot h)$. Обозначим

$$f \cdot g = p = p_n x^n + \ldots + p_1 x + p_0,$$
$$(f \cdot g) \cdot h = p \cdot h = u = u_n x^n + \ldots + u_1 x + u_0,$$
$$g \cdot h = q = q_n x^n + \ldots + q_1 x + q_0,$$
$$f \cdot (g \cdot h) = f \cdot q = v = v_n x^n + \ldots + v_1 x + v_0.$$

Докажем, что $u = v$. Для этого вычислим коэффициенты этих многочленов с номером t, $t = 0, 1, \ldots$:

$$u_t = \sum_{r+k=t} p_r c_k = \sum_{r+k=t} \Big(\sum_{i+j=r} a_i b_j \Big) c_k = \sum_{i+j+k=t} a_i b_j c_k;$$

$$v_t = \sum_{i+s=t} a_i q_s = \sum_{i+s=t} a_i \Big(\sum_{j+k=s} b_j c_k = \Big) \sum_{i+j+k=t} a_i b_j c_k.$$

Результаты одинаковы, что и доказывает тождество ассоциативности.

Аналогично доказывается дистрибутивность умножения относительно сложения многочленов. Очевидно, умножение многочленов коммутативно. Таким образом, $K[x]$ является коммутативным кольцом с единицей, отличной от нуля. Докажем, что это кольцо не имеет делителей нуля. Предположим противное: пусть многочлены $f(x)$, $g(x) \in K[x]$ являются делителями нуля, т.е. $f(x) \neq 0$, $g(x) \neq 0$, но $f(x) \cdot g(x) = 0$. Тогда данные многочлены имеют определенные степени, а значит, их

произведение есть многочлен некоторой степени, в то время как 0 есть многочлен без степени. Пришли к противоречию. Теорема доказана.

Кольцо $K[x]$ называется *кольцом многочленов над областью целостности K*. Если $K = P$ — поле, то $P[x]$ называется *кольцом многочленов над полем P*. Например, $\mathbb{Z}[x]$ есть кольцо многочленов над кольцом целых чисел $\mathbb{Z}$, а $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ являются кольцами многочленов соответственно над полями $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.

В области целостности K, по определению, есть единица 1, поэтому можно рассматривать *обратимые* элементы области целостности. Напомним, что элемент $a \in K$ называется *обратимым*, если для него существует элемент $b \in K$, называемый *обратным* к a, такой что $a \cdot b = 1$. Множество всех обратимых элементов области целостности K будем обозначать K^*. Например, обратимыми в области целостности $\mathbb{Z}$ являются лишь 1 и -1. А вот в области целостности $\mathbb{Q}$, точнее, в поле $\mathbb{Q}$ для всякого отличного от нуля числа есть обратное число. Вообще, если P — поле, то $P^* = P \setminus \{0\}$.

Теорема 1.2. *В кольце многочленов $K[x]$ над областью целостности K обратимыми элементами являются лишь обратимые элементы кольца K, т.е. $(K[x])^* = K^*$.*

Доказательство. Пусть многочлен $d(x) \in K[x]$ является обратимым. Это означает существование многочлена $q(x) \in K[x]$, такого что $d(x) \cdot q(x) = 1$. Поскольку 1 есть многочлен степени 0, то многочлены $d(x)$ и $q(x)$ также должны иметь степень 0, т.е. $d(x) = d_0 \in K$ и $q(x) = q_0 \in K$. Тогда $d_0 \cdot q_0 = 1$, т.е. $d(x) = d_0$ является обратимым элементом кольца K. Теорема доказана.

Предположим, что $K = P$ — поле. Вспомним, что в поле всякий ненулевой элемент обратим, поэтому обратимые элементы кольца многочленов $P[x]$ над полем P есть в точности ненулевые элементы поля P. Таким образом, $(P[x])^* = P^* = P \setminus \{0\}$. Если же $K = \mathbb{Z}$, то $(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{1, -1\}$.

1.1.2. Уточнение понятия многочлена

Не довольствуясь введением многочлена как «выражения вида» $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, дадим формализованное определение этого понятия.

Определение 1.5. *Многочленом над областью целостности K* называется последовательность элементов из K, записываемая в виде $(\ldots, a_n, a_{n-1}, \ldots, a_1, a_0)$, причем число членов последовательности, отличных от нуля, конечно. Каждый член последовательности называется *коэффициентом* многочлена.

Если все коэффициенты равны нулю, то многочлен называется *нулевым*. Если же есть коэффициенты, отличные от нуля, то отличный от нуля коэффициент с наибольшим номером называется *старшим коэффициентом*, а его номер называется *степенью многочлена*. Коэффициент a_0 называется *свободным членом*.

Определение 1.6. Два многочлена называются *равными*, если равны их соответствующие коэффициенты.

Определение 1.7. *Сложение* и *умножение* многочленов определим равенствами

$$(..., a_n, ..., a_0) + (..., b_n, ..., b_0) = (..., a_n + b_n, ..., a_0 + b_0);$$

$$(..., a_n, ..., a_0) \cdot (..., b_n, ..., b_0) = (..., c_n, ..., c_0),$$

где $c_k = a_k b_0 + a_{k-1} b_1 + ... + a_1 b_{k-1} + a_0 b_k = \sum\limits_{i+j=k} a_i b_j$, $k = 0, 1, ...$.

Для получения привычной стандартной записи многочлена степени n обозначим $x = (..., 0, ..., 0, 1, 0)$ и $a = (..., 0, ..., 0, a)$ для любого элемента $a \in K$. В частности, нулевой многочлен имеет вид $0 = (..., 0, ..., 0, 0)$. Вычислим одночлены, используя правило умножения многочленов:

$$a_0 = (..., 0, ..., 0, a_0);$$

$$a_1 \cdot x = (..., 0, ..., 0, a_1) \cdot (..., 0, ..., 1, 0) = (..., 0, ..., a_1, 0);$$

.....

$$a_n \cdot x^n = (..., 0, ..., 0, a_n) \cdot (..., 0, ..., 0, 1, 0, ..., 0) = \\ = (..., 0, ..., 0, a_n, 0, ..., 0).$$

В последнем равенстве единица стоит на месте с номером n, считая справа налево с номера 0. Складывая одночлены, приходим к выводу, что

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

Таким образом, мы осмыслили стандартную запись многочлена, основываясь на новом, формальном его определении.

1.1.3. Кольцо многочленов $\mathbb{Z}_p[x]$

Построим кольцо многочленов над конечной областью целостности, которая в частных случаях оказывается полем.

Зафиксируем простое натуральное число p, скажем $p = 5$, и будем называть его модулем. При делении произвольного

целого числа на $p = 5$ возможны остатки 0, 1, 2. 3, 4, в общем случае получаем остатки 0, 1, ..., $p - 1$. Пусть целое число a при делении на p дает в остатке r, т.е. $a = pq + r$, где $0 \le r < p$.

Обозначим $\overline{a} = \{pn + r \mid n \in \mathbb{Z}\}$. Таким образом, $\overline{a}$ есть множество всех целых чисел, которые при делении на p дают один и тот же остаток r. Отсюда следует, что $\overline{a} = \overline{a}_1$ тогда и только тогда, когда $a - a_1 \vdots p$. В результате множество целых чисел $\mathbb{Z}$ распадается на следующие непересекающиеся классы целых чисел:

при $p = 5$	при произвольном простом p
$\overline{0} = \{5n \mid n \in \mathbb{Z}\}$	$\overline{0} = \{pn \mid n \in \mathbb{Z}\}$
$\overline{1} = \{5n + 1 \mid n \in \mathbb{Z}\}$	$\overline{1} = \{pn + 1 \mid n \in \mathbb{Z}\}$
$\overline{2} = \{5n + 2 \mid n \in \mathbb{Z}\}$	$\overline{2} = \{pn + 2 \mid n \in \mathbb{Z}\}$
$\overline{3} = \{5n + 3 \mid n \in \mathbb{Z}\}$	...
$\overline{4} = \{5n + 4 \mid n \in \mathbb{Z}\}$	$\overline{p-1} = \{pn + p - 1 \mid n \in \mathbb{Z}\}$

При $p = 5$ получаем $\overline{5} = \overline{0}$, $\overline{6} = \overline{1}$, $\overline{7} = \overline{2}$ и т.д. Каждый элемент класса называется *вычетом* этого класса, а сам класс называется *классом вычетов по модулю p*. Множество всех классов вычетов по модулю p обозначается $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$.

Определим сложение и умножение классов вычетов по модулю p, положив $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a} \cdot \overline{b} = \overline{ab}$ для любых $a, b \in \mathbb{Z}$. Докажем независимость сложения и умножения классов от выбора представителей этих классов. Пусть $\overline{a} = \overline{a}_1$, $\overline{b} = \overline{b}_1$. Тогда $a - a_1 \vdots p$, $b - b_1 \vdots p$, откуда $(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1) \vdots p$. Но тогда $a + b = a_1 + b_1$, откуда $\overline{a} + \overline{b} = \overline{a+b} = \overline{a_1 + b_1} = \overline{a}_1 + \overline{b}_1$. Аналогично доказывается, что $\overline{a} \cdot \overline{b} = \overline{a}_1 \cdot \overline{b}_1$. Таким образом, результаты сложения и умножения классов вычетов не зависят от выбора представителей этих классов.

Приведем таблицы сложения и умножения классов вычетов по модулю 5:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Заметим, что пока нигде мы не использовали простоту числа p и все сказанное верно при любом натуральном p. Легко показать, что множество $\mathbb{Z}_p$ относительно сложения и умножения классов вычетов по произвольному модулю p является кольцом. Только по простому модулю это кольцо является полем. Чтобы это установить, докажем предварительно ключевую лемму.

Лемма 1.1. *Если p — простое натуральное число, $\overline{a} \in \mathbb{Z}_p$ и $\overline{a} \neq \overline{0}$, то произведения $\overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{p-1}$ различны.*

Доказательство. Предположим противное, пусть $0 \leq i < j \leq p - 1$ и $\overline{a} \cdot \overline{i} = \overline{a} \cdot \overline{j}$. Тогда $\overline{a \cdot i} = \overline{a \cdot j}$. Это означает, что разность $aj - ai$ делится на p, а значит, $a \cdot (j - i) \vdots p$. Но $0 < j - i < p$, откуда $j - i$ не делится на простое число p. Следовательно, a должно делиться на p. Но это означает, что $\overline{a} = \overline{0}$, что противоречит условию. Лемма доказана.

Теорема 1.3. *Кольцо классов вычетов $\mathbb{Z}_p$ по простому модулю p является полем.*

Доказательство. По лемме 1.1 для любого класса вычетов $\overline{a} \neq \overline{0}$ произведения $\overline{a} \cdot \overline{1}, \overline{a} \cdot \overline{2}, \ldots, \overline{a} \cdot \overline{p-1}$ различны. Но этих произведений ровно $p - 1$ — столько же, сколько всех ненулевых классов вычетов по модулю p. Следовательно, среди них существует произведение $\overline{a} \cdot \overline{x}_0$, где $1 \leq x_0 \leq p - 1$, равное $\overline{1}$, т.е. $\overline{a} \cdot \overline{x}_0 = \overline{1}$. Но это и означает, что класс $\overline{a}$ обратим. Следовательно, кольцо $\mathbb{Z}_p$ является полем. Теорема доказана.

Приведем пример сложения и умножения многочленов в кольце $\mathbb{Z}_5[x]$.

Пример 1.1

Пусть $f(x) = \overline{2}x^3 + \overline{3}x^2 + x - \overline{1}$, $h(x) = \overline{2}x^2 + \overline{4}x + \overline{3}$. Тогда

$$f(x) + h(x) = (\overline{2}x^3 + \overline{3}x^2 + x - \overline{1}) + (\overline{0}x^3 + \overline{2}x^2 + \overline{4}x + \overline{3}) =$$
$$= (\overline{2} + \overline{0})x^3 + (\overline{3} + \overline{2})x^2 + (\overline{1} + \overline{4})x + (-\overline{1} + \overline{3}) =$$
$$= \overline{2}x^3 + \overline{0}x^2 + \overline{0}x + \overline{2} = \overline{2}x^3 + \overline{2};$$
$$f(x) \cdot h(x) = (\overline{2}x^3 + \overline{3}x^2 + x - \overline{1}) \cdot (\overline{2}x^2 + \overline{4}x + \overline{3}) =$$
$$= (\overline{2} \cdot \overline{2})x^5 + (\overline{2} \cdot \overline{4} + \overline{3} \cdot \overline{2})x^4 + (\overline{2} \cdot \overline{3} + \overline{3} \cdot \overline{4} + \overline{1} \cdot \overline{2})x^3 +$$
$$+ (\overline{3} \cdot \overline{3} + \overline{1} \cdot \overline{4} + (-\overline{1}) \cdot \overline{2})x^2 + (\overline{1} \cdot \overline{3} + (-\overline{1}) \cdot \overline{4})x + (-\overline{1}) \cdot \overline{3} =$$
$$= \overline{4}x^5 + \overline{4}x^4 + \overline{0}x^3 + x^2 - x - \overline{3} =$$
$$= -x^5 - x^4 + x^2 - x - \overline{3}.$$

Заметим, что $(x + \overline{2})^5 = x^5 + \overline{2}$ (проверьте!).

Контрольные вопросы

1. При каком условии область целостности является полем?
2. Является ли кольцом (областью целостности, полем) множество всех многочленов над данным полем с нулевым свободным членом?
3. Какова степень обратимого многочлена над данным полем?
4. Конечно ли кольцо многочленов над конечным полем?
5. Существуют ли многочлены разных степеней, значения которых совпадают для любого элемента поля, над которым они рассматриваются?

Задачи

1. Проверьте, является ли кольцом, областью целостности или полем каждое из следующих множеств относительно сложения и умножения:

$$\mathbb{Z},\ \mathbb{Q},\ 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\},$$

$$K = \{a + b\sqrt{2} \mid a, b \in S\},$$

где $S = \mathbb{Z}, \mathbb{Q}$; $K = \{a + bi \mid a, b \in T\}$, где $T = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

2. Приведите примеры двучленов первой, второй, третьей и четвертой степеней, квадратного трехчлена, приведенного квадратного трехчлена, многочлена степени 0, многочлена положительной степени, многочлена без степени.

3. Запишите в буквенном виде два многочлена соответственно степеней 3 и 4, сложите и перемножьте их.

4. В соответствии с формальным определением многочлена вычислите x^2, x^3, и для многочленов $f = (\ldots 0, 0, 2, 3)$, $h = (\ldots 0, 4, 5, 6)$ найдите $f + h, f \cdot h, f^2, f^3$.

5. В кольце многочленов $\mathbb{Z}_5[x]$ даны многочлены $f(x) = x^2 + \overline{3}x + \overline{2}$, $g(x) = \overline{4}x^2 + \overline{2}x + \overline{3}, h(x) = x^2 + \overline{2}x + \overline{2}$. Проверьте, что $f(x) + g(x) = \overline{0}$, откуда $f(x) = -g(x)$; $f(x) \cdot h(x) = x^4 - \overline{1}$.

6. Составьте таблицы сложения и умножения элементов поля Z_7. Придумайте два многочлена $f(x)$, $h(x) \in \mathbb{Z}_7[x]$ и найдите их сумму, разность и произведение.

7. Найдите произведение двучлена $x - c$ на многочлен $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ для $n = 0, 1, 2, 3, 4$.

8. Приведите примеры обратимых элементов в кольцах $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$.

9. Для многочленов $f(x) = x^2 + (1 - i)x + 2i$, $g(x) = ix^2 + x + 1 - 3i$ найдите их сумму, произведение, квадраты и кубы многочленов.

10. Докажите, что произведение $[x - (a + bi)] \cdot [x - (a - bi)]$ является многочленом с действительными коэффициентами.

11. Докажите, что для любого простого числа p в кольце многочленов $\mathbb{Z}_p[x]$ имеет место формула $(x + \overline{a})^p = x^p + \overline{a}^p$.

1.2. Деление многочлена на двучлен. Корни многочлена

1.2.1. Схема Горнера

Схема Горнера представляет собой алгоритм, позволяющий разделить с остатком данный многочлен на двучлен $x - c$.

Определение 1.8. *Разделить с остатком* многочлен $f(x) \in K[x]$ на многочлен $x - c$, где $c \in K$, — это значит найти такие многочлен $q(x) \in K[x]$ и элемент $r \in K$, что $f(x) = (x - c) \cdot q(x) + r$. При этом $q(x)$ называется *неполным частным*, а r — *остатком*. Если остаток $r = 0$, то будем говорить, что $f(x)$ *делится* на $x - c$, и писать $f(x) \vdots x - c$.

Пусть даны многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ степени n над областью целостности K и $c \in K$. Рассматривя равенство $f(x) = (x - c) \cdot q(x) + r$, заключаем, что степень многочлена $q(x)$ равна $n - 1$. Пусть $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$. Тогда

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = f(x) = (x - c) \cdot q(x) + r =$$

$$= (x - c) \cdot (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0) + r =$$

$$= b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + \ldots + (b_0 - cb_1)x + (r - cb_0).$$

Приравнивая соответствующие коэффициенты первого и последнего многочленов в этих равенствах, получаем

$$\begin{cases} a_n = b_{n-1}, \\ a_{n-1} = b_{n-2} - cb_{n-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_1 = b_0 - cb_1, \\ a_0 = r - cb_0 \end{cases} \Rightarrow \begin{cases} b_{n-1} = a_n, \\ b_{n-2} = cb_{n-1} + a_{n-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_0 = cb_1 + a_1, \\ r = cb_0 + a_0. \end{cases}$$

Практически вычисления искомых коэффициентов неполного частного $q(x)$ и остатка r удобно производить, заполняя последовательно следующую таблицу, которая называется *схемой Горнера*.

	a_n	a_{n-1}	...	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = cb_{n-1} + a_{n-1}$	...	b_0	$r = cb_0 + a_0$

Отсюда заключаем, что деление с остатком многочлена $f(x)$ на $x - c$ всегда возможно и однозначно.

Пример 1.2

Многочлен $f(x) = 31x^4 - 279x^2 + 10x + 35$ разделим с остатком на $x + 3$.

Решение. В нашем случае $c = -3$. Заполняем схему Горнера:

	31	0	–279	10	35
–3	31	–93	0	10	5

Ответ: $f(x) = (x + 3)(31x^3 - 93x^2 + 10) + 5$.

1.2.2*. Обобщение схемы Горнера

Аналогично определяется деление с остатком многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ степени $n \geq 2$ на многочлен $h(x) = x^2 - c_1 x - c_0$: $f(x) = h(x) \cdot q(x) + r(x)$, где неполное частное $q(x) = b_{n-2}x^{n-2} + b_{n-3}x^{n-3} + \ldots + b_1 x + b_0$ и остаток $r(x) = d_1 x + d_0$. Из равенства $f(x) = h(x) \cdot q(x) + r(x)$, приравнивая коэффициенты при одинаковых степенях переменной x, получаем

$$\begin{cases} a_n = b_{n-2}, \\ a_{n-1} = b_{n-3} - c_1 b_{n-2}, \\ a_{n-2} = b_{n-4} - c_1 b_{n-3} - c_0 b_{n-2}, \\ a_{n-3} = b_{n-5} - c_1 b_{n-4} - c_0 b_{n-3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_2 = b_0 - c_1 b_1 - c_0 b_2, \\ a_1 = d_1 - c_1 b_0 - c_0 b_1, \\ a_0 = d_0 - c_0 b_0 \end{cases} \Rightarrow \begin{cases} b_{n-2} = a_n, \\ b_{n-3} = c_1 b_{n-2} + a_{n-1}, \\ b_{n-4} = c_1 b_{n-3} + c_0 b_{n-2} + a_{n-2}, \\ b_{n-5} = c_1 b_{n-4} + c_0 b_{n-3} + a_{n-3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_0 = c_1 b_1 + c_0 b_2 + a_2, \\ d_1 = c_1 b_0 + c_0 b_1 + a_1, \\ d_0 = c_0 b_0 + a_0. \end{cases}$$

Коэффициенты искомых многочленов $q(x)$ и $r(x)$ находятся по следующей схеме.

	a_n	a_{n-1}	a_{n-2}	...
c_1	$b_{n-2} = a_n$	$b_{n-3} = c_1 b_{n-2} + a_{n-1}$	$b_{n-4} = c_1 b_{n-3} + c_0 b_{n-2} + a_{n-2}$	...
c_0		b_{n-2}	b_{n-3}	...

...	a_2	a_1	a_0
...	b_0	$d_1 = c_1 b_0 + c_0 b_1 + a_1$	$d_0 = c_0 b_0 + a_0$
...	b_1	b_0	

Верхняя строчка схемы заполняется коэффициентами данного многочлена $f(x)$. Вычисляются только числа строки, содержащей c_1. Если число b_i второй строки уже найдено, то оно записывается как в этой строке, так и со сдвигом вправо в последней строке. Лишь первая и последняя клетки второй строки заполняются не так, как остальные.

Пример 1.3

Найдем неполное частное и остаток при делении многочлена $f(x) = x^5 - 3x^4 + 2x^3 - 4x^2 + x + 5$ на многочлен $h(x) = x^2 - 2x + 5$.

Решение. Составляем обобщенную схему Горнера. В нашем случае $n = 5$, $a_5 = 1$, $a_4 = -3$, $a_3 = 2$, $a_2 = -4$, $a_1 = 1$, $a_0 = 5$; $c_1 = 2$, $c_0 = -5$.

	1	–3	2	–4	1	5
2	1	–1	–5	–9	8	50
–5		1	–1	–5	–9	

Ответ: $f(x) = h(x) \cdot (x^3 - x^2 - 5x - 9) + (8x + 50)$.

Упражнение 1.1. Получите аналогично обобщенную схему Горнера для деления многочлена $f(x)$ на $h(x) = x^3 - c_2x^2 - c_1x - c_0$ и приведите пример использования этой схемы.

Упражнение 1.2. Опишите обобщенную схему Горнера в общем случае.

1.2.3. Корни многочлена

Подставим в многочлен с целыми коэффициентами $f(x) = x^2 + x - 6$ вместо переменной x число 3 и выполним указанные действия: $f(3) = 3^2 + 3 - 6 = 6$. Аналогично находим $f(2) = 0$, $f(-3) = 0$. Рассмотрим эти действия в общей ситуации.

Определение 1.9. Пусть даны многочлен $f(x) = a_nx^n + \ldots + a_1x + a_0$ над областью целостности K и элемент $c \in K$. Подставим всюду вместо x элемент c и выполним все указанные действия. Полученный результат обозначается $f(c)$ и называется *значением многочлена $f(x)$ при $x = c$*.

Отметим, что $f(0) = a_0$ — свободный член многочлена $f(x)$, а $f(1) = a_n + \ldots + a_0$ — сумма коэффициентов данного многочлена.

Определение 1.10. *Корнем многочлена $f(x)$* над областью целостности K называется элемент $c \in K$, такой что $f(c) = 0$.

Пример 1.4

Очевидно, многочлен с целыми коэффициентами $f(x) = 2x^5 - x^4 - 2x^3 + x^2 - 4x + 2 = (x^2 + 1)(x^2 - 2)(2x - 1)$ не имеет целых корней. Если же этот многочлен рассматривать над полем рациональных чисел, т.е. $f(x) \in \mathbb{Q}[x]$, то он имеет рациональный корень $x_1 = 1/2$. Если его рассматривать над полем действительных чисел, т.е. $f(x) \in \mathbb{R}[x]$, то он имеет еще два действительных корня $x_{2,3} = \pm\sqrt{2}$, а в поле комплексных чисел к этим корням добавляются еще два корня $x_{4,5} = \pm i$. Таким образом, важно знать, над каким полем рассматривается данный многочлен.

Упражнение 1.3. Убедитесь, что $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, -\overline{1}, \overline{2}, -\overline{2}\}$, и перебором найдите все корни многочленов из $\mathbb{Z}_5[x]$: $x^5 - x$, $x^5 + x^4 - -x - \overline{1}$, $x^5 + x^3 - x^2 - \overline{1}$, $x^5 + x^2 - x - \overline{1}$, $x^5 - \overline{1}$, $x^5 + x^4 + + x^3 + x^2 + + x + \overline{1}$.

Теорема 1.4 (Безу). *Остаток от деления многочлена $f(x)$ на $x - c$ равен $f(c)$ — значению многочлена при $x = c$, т.е. $f(x) = (x - c)q(x) + f(c)$.*

Доказательство. В равенство $f(x) = (x - c)q(x) + r$ подставим значение $x = c$. Получим $f(c) = (c - c)q(c) + r$, откуда $r = f(c)$. Следовательно, $f(x) = (x - c)q(x) + f(c)$. Теорема доказана.

Теорема 1.5 (критерий корня). *Элемент $c \in K$ является корнем многочлена $f(x) \in K[x]$ тогда и только тогда, когда $f(x) \vdots (x - c)$.*

Доказательство. По теореме Безу $f(x) = (x - c)\ q(x) + f(c)$. Отсюда следует, что $f(x) \vdots (x - c) \Leftrightarrow f(c) = 0 \Leftrightarrow c$ является корнем многочлена $f(x)$.

Определение 1.11. Корень c многочлена $f(x)$ называется *корнем кратности k*, если $f(x)$ делится на $(x - c)^k$ но не делится на $(x - c)^{k+1}$.

Теорема 1.6. *Многочлен степени n имеет не более чем n различных корней.*

Доказательство. Пусть $c_1, c_2, \ldots, c_k$ — различные корни многочлена $f(x)$ степени n. Поскольку c_1 — корень многочлена $f(x)$, то по теореме 1.5 $f(x) \vdots (x - c_1)$, т.е. $f(x) = (x - c_1)q_1(x)$. Поскольку c_2 — корень многочлена $f(x)$, то $0 = f(c_2) = (c_2 - c_1)q_1(c_2)$. Из условия следует, что $c_2 - c_1 \neq 0$. Следовательно, $q_1(c_2) = 0$. Это означает, что c_2 — корень многочлена $q_1(x)$. По теореме 1.5 $q_1(x) \vdots (x - c_2)$, т.е. $q_1(x) = (x - c_2)q_2(x)$, откуда $f(x) = (x - c_1)(x - - c_2)q_2(x)$. Повторяя рассуждения, на k-м шаге будем иметь $f(x) = (x - c_1)(x - c_2)\ldots(x - c_k)q_k(x)$, откуда $k \leq n$.

1.2.4. Примеры задач, решаемых с помощью схемы Горнера

Рассмотрим примеры решения задач.

Пример 1.5

Даны многочлен $f(x) = x^5 + 8x^4 + 19x^3 + 9x^2 - 27$ и число $c = -3$ (в общем случае это может быть некоторый элемент из области целостности K). Разделим $f(x)$ на $x - c$.

Решение. Воспользуемся схемой Горнера.

	1	8	19	9	0	–27
–3	1	5	4	–3	9	–54

Ответ: $f(x) = (x + 3)(x^4 + 5x^3 + 4x^2 - 3x + 9) - 54$.

Пример 1.6

Найдем значение многочлена $f(x) = x^5 + 8x^4 + 19x^3 + 9x^2 - 27$ при $x = -3$.

Решение. Воспользовавшись решением предыдущего примера, получаем ответ: $f(-3) = -54$.

Пример 1.7

Проверим, является ли число –3 корнем многочлена $h(x) = x^5 + 8x^4 + 19x^3 + 9x^2 + 27$, и если да, то найдем его кратность.

Решение. Воспользуемся схемой Горнера.

	1	8	19	9	0	27	
–3	1	5	4	–3	9	0	$\Rightarrow x = -3$ — корень $f(x)$
–3	1	2	–2	3	0		$\Rightarrow x = -3$ — корень кратности ≥ 2
–3	1	–1	1	0			$\Rightarrow x = -3$ — корень кратности ≥ 3
–3	1	–4	$\neq 0$				$\Rightarrow x = -3$ — корень кратности 3

Ответ: –3 является корнем многочлена $f(x)$ кратности 3.

Пример 1.8

Разложим многочлен $f(x) = 2x^4 - 3x^3 + 5$ по степеням $x - 1$.

Решение. Ответ должен выглядеть так:

$$f(x) = a_4(x-1)^4 + a_3(x-1)^3 + a_2(x-1)^2 + a_1(x-1) + a_0.$$

Перепишем это по-другому:

$$f(x) = (((a_4(x-1)+a_3)(x-1)+a_2)(x-1)+a_1)(x-1)+a_0 =$$
$$= q_1(x)(x-1)+a_0,$$

$$q_1(x) = ((a_4(x-1)+a_3)(x-1)+a_2)(x-1)+a_1 = q_2(x)(x-1)+a_1,$$
$$q_2(x) = (a_4(x-1)+a_3)(x-1)+a_2 = q_3(x)(x-1)+a_2,$$
$$q_3(x) = a_4(x-1)+a_3.$$

Видим, что a_0 есть остаток от деления многочлена $f(x)$ на $(x-1)$, a_1 есть остаток от деления полученного неполного частного $q_1(x)$ на $(x-1)$ и т.д. Следовательно, искомые коэффициенты можно получить с помощью схемы Горнера.

	2	–3	0	0	5	$\Rightarrow f(x) = (x-1)\overbrace{(2x^3-x^2-x-1)}^{q_1(x)}+4$
1	2	–1	–1	–1	4	
1	2	1	0	–1		$\Rightarrow q_1(x) = (x-1)(2x^2+x)-1 =$ $= (x-1)q_2(x)-1$
1	2	3	3			$\Rightarrow q_2(x) = (x-1)(2x+3)+3 =$ $= (x-1)q_3(x)+3$
1	2	5				$\Rightarrow q_3(x) = (x-1)2+5$

Ответ: $f(x) = 2(x-1)^4 + 5(x-1)^3 + 3(x-1)^2 - (x-1) + 4$.

Пример 1.9

Найдем значение многочлена $f(x) = 31x^5 - 423x^4 + 2185x^3 - 5439x^2 + 6670x - 3293$ при $x = 2{,}1$.

Решение. Разложим многочлен $f(x)$ по степеням $x-2$.

	31	–423	2185	–5439	6670	–3293
2	31	–361	1463	–2513	1644	–5
2	31	–299	865	–783	78	
2	31	–237	391	–1		
2	31	–175	41			
2	31	–113				
2	31					

Таким образом,

$$f(x) = 31(x-2)^5 - 113(x-2)^4 + 41(x-2)^3 - (x-2)^2 + 78(x-2) - 5,$$

$$f(2{,}1) = 31 \cdot (0{,}1)^5 - 113 \cdot (0{,}1)^4 + 41 \cdot (0{,}1)^3 - (0{,}1)^2 + 78 \cdot (0{,}1) - 5 =$$

$$= 0{,}00031 - 0{,}0113 + 0{,}041 - 0{,}01 + 7{,}8 - 5 = 2{,}82001.$$

Пример 1.10

Дан многочлен $f(x) = 2x^4 + 16x^3 + 47x^2 + 63x + 41$. Найдите значения многочлена и всех его производных при $x = -2$ (пользуясь определением производной, известным из математического анализа, см. также определение 2.13).

Решение. Используя схему Горнера, разложим данный многочлен по степеням $x + 2$. Получим $f(x) = 2(x+2)^4 - (x+2)^2 + 3(x+2) + 7$ (проверьте!). Тогда $f(-2) = 7$. Найдем производную: $f'(x) = 8(x+2)^3 - 2(x+2) + 3$, откуда $f'(-2) = 3$. Далее, $f''(x) = 24(x+2)^2 - 2$, откуда $f''(-2) = -2$. Теперь находим $f'''(x) = 48(x+2)$, откуда $f'''(-2) = 0$. Наконец, $f^{IV}(x) = 48$, а значит, $f^{IV}(-2) = 48$.

Обобщим решение последнего примера. Рассмотрим в общем виде разложение многочлена $f(x)$ по степеням $(x - c)$:

$$f(x) = b_n(x-c)^n + b_{n-1}(x-c)^{n-1} + \ldots + b_1(x-c) + b_0.$$

Отсюда $f(c) = b_0$. Найдем производную:

$$f'(x) = b_n n(x-c)^{n-1} + b_{n-1}(n-1)(x-c)^{n-2} + \ldots + b_2 2(x-c) + b_1.$$

Отсюда $f'(c) = b_1$. Найдем вторую производную:

$$f''(x) = b_n n(n-1)(x-c)^{n-2} + \ldots + b_3 3 \cdot 2(x-c) + 2b_2.$$

Отсюда $f''(c) = 2b_2$. Аналогично получаем $f'''(c) = 3 \cdot 2 \cdot b_3$, и т.д., $f^{(n)}(c) = n \cdot (n-1) \cdot \ldots \cdot 3 \cdot 2 \cdot b_n$. Таким образом, имеем $f(c) = b_0, f'(c) = b_1, f''(c) = 2!b_2, \ldots, f^{(n)}(c) = n!b_n$, откуда получаем *формулу Тейлора*:

$$f(x) = \frac{f^{(n)}(c)}{n!}(x-c)^n + \frac{f^{(n-1)}(c)}{(n-1)!}(x-c)^{n-1} + \ldots + f'(c)(x-c) + f(c).$$

Заметим, что теперь пример 1.10 можно решить по-другому: сначала с помощью схемы Горнера найти разложение данного многочлена $f(x)$ по степеням $(x + 2)$, а затем вычислить значения многочлена и всех его производных при $x = -2$ по найденным формулам: $f(-2) = b_0 = 7, f'(-2) = b_1 = 3, f''(-2) = 2!b_2 =$

$= 2! \cdot (-1) = -2$, $f'''(-2) = 3!b_3 = 3! \cdot 0 = 0$, $f^{IV}(-2) = 4!b_4 = 4! \cdot 2 = 48$.

1.2.5*. Корни многочленов кольца $\mathbb{Z}_p[x]$

Рассмотрим кольцо многочленов $\mathbb{Z}_p[x]$ над полем классов вычетов $\mathbb{Z}_p$ по простому модулю p и корни одного многочлена над этим полем. В качестве приложения получим утверждение из теории чисел.

Теорема 1.6. *Если p — простое число, то классы вычетов $\overline{1}$, $\overline{2}$, ... , $\overline{p-1}$ являются различными корнями многочлена $x^{p-1} - \overline{1}$.*

Доказательство. Пусть $\overline{a}$ — один из названных в теореме классов вычетов по простому модулю p. По лемме 1.1 классы вычетов $\overline{b_1} = \overline{1} \cdot \overline{a}$, $\overline{b_2} = \overline{2} \cdot \overline{a}$, ... , $\overline{b_{p-1}} = \overline{p-1} \cdot \overline{a}$ различны, а значит, совпадают с классами вычетов $\overline{1}$, $\overline{2}$, ... , $\overline{p-1}$ в некотором порядке. Следовательно,

$$\overline{b_1} \cdot \overline{b_2} \cdot \ldots \cdot \overline{b_{p-1}} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} = \overline{(p-1)!}.$$

С другой стороны,

$$\overline{b_1} \cdot \overline{b_2} \cdot \ldots \cdot \overline{b_{p-1}} = \overline{a} \cdot (\overline{2} \cdot \overline{a}) \cdot \ldots \cdot (\overline{p-1} \cdot \overline{a}) = \overline{(p-1)! \cdot a^{p-1}}.$$

Таким образом,

$$\overline{(p-1)!} = \overline{(p-1)! \cdot a^{p-1}} \Rightarrow$$
$$\Rightarrow \overline{(p-1)! \cdot a^{p-1}} - \overline{(p-1)!} = \overline{0} \Rightarrow$$
$$\Rightarrow \overline{(p-1)! \cdot (a^{p-1} - 1)} = \overline{0}.$$

Следовательно, $(p-1)! \cdot (a^{p-1} - 1) \vdots p$, а так как $(p-1)!$ не делится на p, то $(a^{p-1} - 1) \vdots p$. Отсюда $\overline{a^{p-1} - 1} = \overline{0} \Rightarrow \overline{a}^{p-1} - \overline{1} = \overline{0}$. Но это и означает, что класс вычетов $\overline{a}$ является корнем многочлена $x^{p-1} - \overline{1} = \overline{0}$.

Следствие 1. $x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) \ldots (x - \overline{(p-1)})$.

***Следствие 2* (*критерий Вильсона*).** Натуральное число p является простым тогда и только тогда, когда $(p-1)! + 1 \vdots p$.

Доказательство. ($\Rightarrow$) Если $p = 2$, то утверждение очевидно. Пусть p — нечетное простое число. Рассмотрим равенство из следствия 1 и приравняем свободные члены многочленов:

$$-\overline{1} = (-1)^{p-1} \cdot \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} = \overline{(p-1)!}.$$

Отсюда $\overline{(p-1)!} + \overline{1} = \overline{0}$, следовательно, $(p-1)! + 1 \vdots p$.

($\Leftarrow$) Пусть $(p-1)! + 1 \vdots p$. Предположим противное доказываемому, пусть число p составное и пусть $p \vdots d$, $1 < d < p$. Тогда $(p-1)! \vdots d$, а так как $(p-1)! + 1 \vdots p$, то $1 \vdots d$ — противоречие. Следовательно, p — простое число.

1.2.6. Многочлен как функция

Пусть дан многочлен $f(x) \in K[x]$. Сопоставляя всякому элементу $c \in K$ элемент $f(c) \in K$, получаем функцию с областью определения K и множеством значений в K.

Рассматривая всякий многочлен как функцию, мы можем говорить о *функциональном равенстве многочленов*: многочлены $f(x)$ и $h(x)$ с коэффициентами из кольца K равны функционально (т.е. как функции), если для любого $c \in K$ имеем $f(c) = h(c)$, т.е. при одинаковых значениях аргумента значения функций совпадают. Очевидно, из алгебраического равенства двух многочленов следует их функциональное равенство. Спрашивается, если два многочлена равны функционально, то будут ли они равны в алгебраическом смысле, т.е. будут ли равны их соответствующие коэффициенты? Приведем пример, показывающий, что, вообще говоря, это не так.

Пример 1.11

Непосредственной проверкой легко установить, что в кольце $\mathbb{Z}_5[x]$ различные в алгебраическом смысле многочлены $\overline{2}x + \overline{1}$, $\overline{2}x^5 + \overline{1}$, $\overline{2}x^6 + \overline{3}x^2 + \overline{2}x + \overline{1}$ равны функционально, т.е. при одних и тех же значениях переменной принимают одинаковые значения.

Вместе с тем имеет место следующая теорема.

Теорема 1.7. *Если область целостности K бесконечна, то в кольце многочленов $K[x]$ из функционального равенства многочленов следует их алгебраическое равенство.*

Доказательство. Пусть многочлены $f(x)$ и $h(x)$ из кольца $K[x]$ равны функционально. Если предположить, что разность $f(x) - h(x)$ является ненулевым многочленом, то этот многочлен имеет некоторую определенную степень n. Выберем в K различные элементы $c_1, c_2, \ldots, c_{n+1}$. Из функционального равенства многочленов следует, что $f(c_i) - h(c_i) = 0$ для любого $i = 1, 2, \ldots, n+1$. Но это означает, что многочлен $f(x) - h(x)$ имеет $n+1$ различных корней, что противоречит теореме 1.6. Следовательно, $f(x) - h(x)$ — нулевой многочлен, откуда $f(x) = h(x)$ в алгебраическом смысле. Теорема доказана.

Контрольные вопросы

1. Существует ли многочлен, имеющий бесконечное множество корней?
2. Что устанавливает теорема Безу?
3. Что такое кратность корня?
4. Может ли кратность корня превосходить его степень?
5. Какие типы задач можно решать с помощью схемы Горнера?
6. Сколько клеток в верхнем ряду схемы Горнера для многочлена степени семь, содержащего четыре члена?
7. Критерий Вильсона простоты числа является необходимым, достаточным или необходимым и достаточным условием?

Задачи

1. Для приведенных ниже многочлена $f(x)$ и числа c решите следующие задачи с использованием схемы Горнера:
   1) разделите с остатком $f(x)$ на $(x - c)$;
   2) разложите многочлен $f(x)$ по степеням $(x - c)$;
   3) найдите значения многочлена $f(x)$ и всех его производных при $x = c$.
   а) $f(x) = 2x^4 + 8x^3 - 5x^2 + 3x - 1$, $c = 2$;
   б) $f(x) = 5x^5 - 2x^4 + 8x - 7$, $c = 3$;
   в) $f(x) = 15x^5 - 12x^4 + 8x^2 - 5$, $c = -2$;
   г) $f(x) = 2ix^4 + (1 - 2i)x^3 + i$, $c = 1 - i$;
   д) $f(x) \in Z_5[x]$, $f(x) = \overline{2}x^5 - \overline{2}x^4 + x^2 - \overline{3}$, $c = \overline{2}$.
2. Пользуясь схемой Горнера, найдите все значения многочлена и его корни: а) $x^5 + \overline{2}x^4 - x^2 - \overline{3} \in \mathbb{Z}_7[x]$; б) $x^5 - \overline{3}x^4 + x + \overline{3} \in \mathbb{Z}_{11}[x]$.
3. Для данного многочлена $f(x)$ с помощью разложения его по степеням $(x - c)$ при подходящем c найдите $f(d)$:
   а) $f(x) = 27x^5 - 307x^4 + 1463x^3 - 3570x^2 + 4388x - 2231$, $d = 0{,}99$;
   б) $f(x) = 45x^5 - 648x^4 + 3726x^3 - 10715x^2 + 15448x - 8973$, $d = 2{,}99$;
   в) $f(x) = 45x^5 + 702x^4 + 4351x^3 + 13402x^2 + 20526x + 12501{,}99993$, $d = -3{,}01$.
4. Найдите коэффициент k многочлена $f(x) = 3x^4 - kx^2 + 6$, если $f(-2) = 6$.
5. Пусть $f(x) \in \mathbb{Z}[x]$, $a, b \in \mathbb{Z}$ и $a \neq b$. Докажите, что $f(a) - f(b) \vdots a - b$.
6. Докажите, что $a^{2n} - b^{2n}$ делится на $a + b$ при любых целых a и b, $a \neq -b$.
7. Докажите, что $a^{2n-1} + b^{2n-1}$ делится на $a + b$ при любых целых a и b, где $a \neq -b$.
8. Найдите остаток от деления $64x^4 + 32x^3 - 8x^2 - 72x + 8$ на $2x - 1$.
9. Определите, при каком a многочлен $x^4 + ax^3 + 3x^2 - 4x - 4$ делится на $x - 2$.

10. Определите, при каких a и b многочлен $ax^3 + bx^2 - 73x + 102$ делится на $x^2 - 5x + 6$.

11. Определите a и b так, чтобы многочлен $x^5 + ax^2 + bx + 1$ имел корень -2 кратности по крайней мере 2.

12. Установите функциональное равенство многочленов и найдите их корни: $x^7 + \overline{2}x^6 - x^5 + \overline{2}x^3 - x^2 + x + \overline{1}$ и $\overline{3}x^3 + x^2 + \overline{1}$ в $\mathbb{Z}_5[x]$.

Глава 2
ТЕОРИЯ ДЕЛИМОСТИ МНОГОЧЛЕНОВ

2.1. Делимость в кольце многочленов над областью целостности

2.1.1. Основные понятия теории делимости многочленов

Распространим понятие делимости целых чисел на многочлены.

Определение 2.1. Пусть K — область целостности. Будем говорить, что многочлен $f(x)$ из кольца многочленов $K[x]$ *делится* на ненулевой многочлен $h(x) \in K[x]$ и писать $f(x) \vdots h(x)$, если существует многочлен $q(x) \in K[x]$, такой что $f(x) = h(x) \cdot q(x)$. При этом $h(x)$ будем называть *делителем многочлена* $f(x)$, а многочлен $f(x)$ — *кратным многочлена* $h(x)$.

Рассмотрим основные свойства делимости многочленов.

1. *Свойство транзитивности*: *если* $f(x) \vdots g(x)$ и $g(x) \vdots h(x)$, то $f(x) \vdots h(x)$.

Доказательство. Из условия следует существование многочленов $q(x), k(x) \in K[x]$, таких что $f(x) = g(x)q(x)$, $g(x) = h(x)k(x)$. Следовательно, $f(x) = g(x)q(x) = h(x)k(x)q(x)$, откуда $f(x) \vdots h(x)$.

2. *Свойство рефлексивности*: *для любого* $f(x) \neq 0$, $f(x) \vdots f(x)$.

Доказательство. Очевидно, $f(x) = f(x) \cdot 1$, отсюда $f(x) \vdots f(x)$.

3. Если $f(x) \vdots h(x)$ и $g(x) \vdots h(x)$, то $(f(x) + g(x)) \vdots h(x)$, и если $f(x) \vdots h(x)$, то $f(x) \cdot u(x) \vdots h(x)$ для любого многочлена $u(x)$.

Упражнение 2.1. Докажите свойство 3.

4. *Делителями единицы в кольце многочленов* $K[x]$ *над областью целостности* K *являются лишь обратимые элементы из* K. *В частности, делители единицы кольца многочленов* $\mathbb{Z}[x]$ *есть* 1 *и* -1, *а кольца многочленов* $P[x]$ *над полем* P *есть в точности ненулевые элементы поля* P.

Доказательство. Пусть многочлен $d(x)$ является делителем единицы. Это означает существование многочлена $q(x)$, такого что $d(x) \cdot q(x) = 1$. Отсюда следует, что $d(x) = d_0 \in K \setminus \{0\}$, $q(x) =$

$= q_0 \in K \setminus \{0\}$ и $d_0 q_0 = 1$. Но это и означает, что элемент d_0 обратим.

5. *Если $f(x) \vdots g(x)$ и $g(x) \vdots f(x)$, то существует делитель единицы (обратимый элемент) $k \in K$, такой что $f(x) = k \cdot g(x)$. В частности, если $K = \mathbb{Z}$, то $k = \pm 1$, а если $K = P$ — поле, то k — ненулевой элемент поля.*

Доказательство. Из условия следует существование многочленов $k(x)$, $q(x) \in K[x]$, таких что $f(x) = g(x)k(x)$, $g(x) = f(x)q(x)$. Отсюда $f(x) = f(x)q(x)k(x)$ и $q(x)k(x) = 1$. Следовательно, $k(x)$ — делитель единицы и по свойству 4 $k(x) = k$ — обратимый элемент кольца K. В то же время $f(x) = k \cdot g(x)$.

2.1.2. Наибольший общий делитель двух многочленов

Перенесем на многочлены известные для натуральных чисел понятия общего и наибольшего общего делителя.

Определение 2.2. В кольце многочленов $K[x]$ над областью целостности K многочлен $d(x)$ называется *общим делителем многочленов* $f(x)$ и $h(x)$, если $f(x) \vdots d(x)$ и $h(x) \vdots d(x)$.

Определение 2.3. В кольце многочленов $K[x]$ над областью целостности K *наибольшим общим делителем двух многочленов* $f(x)$ и $h(x)$ называется такой их общий делитель $d(x)$, который делится на любой другой общий делитель данных многочленов. Обозначение: НОД$(f(x), h(x)) = d(x)$.

Обратим внимание на смысл последнего равенства. Подобно тому как мы пишем $x = x_0$, понимая под этим, что переменная x принимает значение x_0, мы будем писать НОД$(f(x), h(x)) = d(x)$, понимая под этим, что $d(x)$ есть *один из* наибольших общих делителей данных многочленов. Например, в кольце целых чисел НОД$(2, 3) = \pm 1$, а в кольце $\mathbb{Q}[x]$ НОД$(x^2 - 1, x^3 - 1) = q \cdot (x - 1)$ при любом $0 \neq q \in \mathbb{Q}$.

Теорема 2.1. *Пусть K — область целостности и $f(x), h(x) \in K[x]$. Если* НОД$(f(x), h(x)) = d(x)$, *то* НОД$(f(x), h(x)) = d_1(x)$ *тогда и только тогда, когда $d_1(x) = k \cdot d(x)$, где k — делитель единицы (обратимый элемент) кольца K.*

Доказательство. ($\Rightarrow$) Пусть $d(x)$ и $d_1(x)$ — два наибольших общих делителя многочленов $f(x)$ и $h(x)$. По определению, наибольший общий делитель делится на любой общий делитель, поэтому $d_1(x) \vdots d(x)$. Аналогично $d(x) \vdots d_1(x)$. По свойству 5 делимости многочленов существует обратимый элемент (или делитель единицы) $k \in K$, такой что $d_1(x) = k \cdot d(x)$.

($\Leftarrow$) Пусть НОД($f(x)$, $h(x)$) = $d(x)$ и $d_1(x) = k \cdot d(x)$, где k — обратимый элемент из K. Поскольку $f(x) \vdots d(x)$, то существует многочлен $q(x) \in K[x]$, такой что $f(x) = d(x)q(x)$. Но тогда $f(x) = kd(x)k^{-1}q(x) = d_1(x)q_1(x)$, где $q_1(x) = k^{-1}q(x) \in K[x]$. Следовательно, $f(x) \vdots d_1(x)$. Аналогично $h(x) \vdots d_1(x)$. Таким образом, $d_1(x)$ является общим делителем многочленов $f(x)$ и $h(x)$. Пусть $d_2(x)$ является общим делителем многочленов $f(x)$ и $h(x)$. Поскольку НОД($f(x)$, $h(x)$) = $d(x)$, то $d(x) \vdots d_2(x)$, откуда $d_1(x) = kd(x) \vdots d_2(x)$. Итак, $d_1(x)$ является общим делителем многочленов $f(x)$ и $h(x)$, который делится на любой общий делитель этих многочленов. Следовательно, НОД($f(x)$, $h(x)$) = $d_1(x)$. Теорема доказана.

Таким образом, наибольший общий делитель двух данных многочленов над областью целостности K определяется однозначно с точностью до обратимого элемента кольца K. В частности, в кольце многочленов $\mathbb{Z}[x]$ наибольший общий делитель определяется однозначно с точностью до знака, а в кольце $\mathbb{Q}[x]$ — однозначно с точностью до $0 \neq k \in \mathbb{Q}$. Если мы обнаружили, что наибольшим общим делителем многочленов $f(x)$, $h(x) \in \mathbb{Q}[x]$ является число $d \in \mathbb{Q}$, то 1 является наибольшим общим делителем этих многочленов и мы пишем НОД($f(x)$, $h(x)$) = 1.

Легко доказать, что НОД(НОД($f_1(x), f_2(x)$), $f_3(x)$)= НОД($f_1(x)$, НОД($f_2(x)$, $f_3(x)$)). Это позволяет рассматривать наибольший общий делитель n многочленов ($n > 2$), который обозначается НОД($f_1(x), f_2(x)$, ..., $f_n(x)$).

Контрольные вопросы

1. Является ли отношение делимости для многочленов отношением эквивалентности?
2. Любой ли многочлен можно взять в качестве делителя?
3. Верно ли, что если первый многочлен делится на второй, то степень первого многочлена больше степени второго?
4. Верно ли, что в кольце $\mathbb{Q}[x]$ всякий многочлен делится на всякий многочлен нулевой степени? Тот же вопрос для кольца многочленов $\mathbb{Z}[x]$.
5. Пусть в кольце $\mathbb{Z}[x]$ имеем НОД($f(x)$, $h(x)$) = $d(x)$. Верно ли, что НОД($f(x)$, $h(x)$) = $3d(x)$? Тот же вопрос в кольце $\mathbb{Q}[x]$.
6. Можно ли получить определение НОД двух целых чисел из определения НОД двух многочленов?
7. Какие делители имеет простое число в кольце многочленов над полем рациональных чисел?

Задачи

1. Опишите обратимые элементы (делители единицы) в кольцах многочленов $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.
2. В кольце $\mathbb{Z}[x]$ опишите все делители многочлена $x^4 - 1$. Опишите все делители этого многочлена в кольце $\mathbb{R}[x]$.
3. Даны два многочлена $f(x), g(x) \in \mathbb{Q}[x]$. Как изменится НОД($f(x)$, $g(x)$), если: а) один из многочленов умножить на $x - 3$; б) каждый многочлен умножить на $x - 3$?
4. Опишите все НОД двух многочленов первой степени в кольце $\mathbb{Z}[x]$.
5. Докажите, что НОД($f(x) \cdot g(x), h(x) \cdot g(x)) = g(x) \cdot$ НОД($f(x), h(x)$).

2.2. Делимость многочленов над полем

2.2.1. Деление с остатком в кольце многочленов над полем

Перенесем известное для целых чисел понятие деления с остатком на многочлены с коэффициентами из произвольного поля P.

Определение 2.4. Пусть P — поле и $f(x), h(x) \in P[x]$, причем $h(x) \neq 0$. *Разделить с остатком* многочлен $f(x)$ на ненулевой многочлен $h(x)$ — это значит найти многочлены $q(x)$ и $r(x)$, такие что $f(x) = h(x) \cdot q(x) + r(x)$, причем $r(x)$ — либо нулевой многочлен, либо его степень меньше степени $h(x)$. Многочлен $f(x)$ называют *делимым*, $h(x)$ — *делителем*, $q(x)$ — *неполным частным*, $r(x)$ — *остатком*.

Пример 2.1

Разделим «уголком» многочлен $f(x) = 3x^4 + 5x^3 - x^2 + 2$ на многочлен меньшей степени $h(x) = x^2 + 3x + 1$:

$$f(x) = 3x^4 + 5x^3 - x^2 + 2 \;\Big|\; \underline{x^2 + 3x + 1 = h(x)}$$

Решение. 1. Уравняем старшие члены данных многочленов, для чего многочлен $h(x)$ умножим на $3x^2$, а затем найдем разность $f_1(x) = f(x) - h(x) \cdot 3x^2$:

$$\begin{array}{l} f(x) = \_\,3x^4 + 5x^3 - x^2 + 2 \;\Big|\; \underline{x^2 + 3x + 1 = h(x)} \\ \underline{3x^4 + 9x^3 + 3x^2} \;\Big|\; 3x^2 \\ f_1(x) = -4x^3 - 4x^2 + 2 \end{array}$$

Таким образом, $f(x) = h(x) \cdot 3x^2 + f_1(x)$. Степень многочлена $f_1(x)$ больше степени делителя $h(x)$, поэтому повторим шаг деления «уголком».

2. Уравняем старшие члены многочленов $f_1(x)$ и $h(x)$, для чего многочлен $h(x)$ умножим на $-4x$, а затем найдем разность $f_2(x) = f_1(x) - h(x) \cdot (-4x)$:

$$\begin{array}{rl|l} f(x) = & 3x^4 + 5x^3 - x^2 + 2 & x^2 + 3x + 1 = h(x) \\ \underline{\quad} & \underline{3x^4 + 9x^3 + 3x^2} & \\ f_1(x) = & -4x^3 - 4x^2 + 2 & \\ & \underline{-4x^3 - 12x^2 - 4x} & \\ & f_2(x) = 8x^2 + 4x + 2 & \end{array} \qquad 3x^2 - 4x$$

Таким образом, получаем $f_1(x) = h(x) \cdot (-4x) + f_2(x)$, откуда $f(x) = h(x) \cdot 3x^2 + h(x) \cdot (-4x) + f_2(x) = h(x)(3x^2 - 4x) + f_2(x)$. Степень многочлена $f_2(x)$ равна степени делителя $h(x)$, поэтому еще раз повторим шаг деления.

3. Уравняем старшие члены многочленов $f_2(x)$ и $h(x)$, для чего $h(x)$ умножим на 8, и найдем разность $f_2(x) - h(x) \cdot 8$:

$$\begin{array}{rl|l} f(x) = & 3x^4 + 5x^3 - x^2 + 2 & x^2 + 3x + 1 = h(x) \\ \underline{\quad} & \underline{3x^4 + 9x^3 + 3x^2} & \\ f_1(x) = & -4x^3 - 4x^2 + 2 & \\ & \underline{-4x^3 - 12x^2 - 4x} & \\ & f_2(x) = 8x^2 + 4x + 2 & \\ & \underline{8x^2 + 24x + 8} & \\ & r(x) = -20x - 6 & \end{array} \qquad 3x^2 - 4x + 8 = q(x)$$

Степень разности $r(x) = f_2(x) - h(x) \cdot 8 = -20x - 6$ меньше степени делителя $h(x)$, поэтому деление «уголком» закончено. Таким образом, $f_2(x) = h(x) \cdot 8 + r(x)$, откуда $f(x) = h(x)(3x^2 - 4x) + f_2(x) = h(x)(3x^2 - 4x) + h(x) \cdot 8 + r(x) = h(x)(3x^2 - 4x + 8) + r(x)$.

В итоге получаем неполное частное $q(x) = 3x^2 - 4x + 8$ и остаток $r(x) = -20x - 6$.

Придадим этим рассуждениям общий характер и рассмотрим деление с остатком в кольце многочленов $P[x]$ над полем P.

Теорема 2.2. *Для любых многочленов $f(x)$ и $h(x) \neq 0$ с коэффициентами из поля P существуют единственные многочлены $q(x)$ и $r(x)$ с коэффициентами из того же поля, такие что $f(x) = h(x) \cdot q(x) + r(x)$, причем $r(x)$ либо нулевой многочлен, либо его степень меньше степени делителя $h(x)$.*

Доказательство. Существование. Если $f(x)$ нулевой многочлен или его степень меньше степени делителя $h(x)$, то $f(x) = h(x) \cdot 0 + f(x)$ и, положив $q(x) = 0$, $r(x) = f(x)$, получим требуемое.

Предположим теперь, что степень $f(x)$ больше или равна степени $h(x)$. Начнем деление «уголком» $f(x)$ на $h(x)$. Пусть $f(x) = a_n x^n + a_{n-1}x_{n-1} + \ldots + a_1 x + a_0$, $h(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ и $b_m \neq 0$, $n \geq m$. Уравняем старшие члены этих многочленов, для чего $h(x)$ умножим на $\frac{a_n}{b_m}x^{n-m}$, а затем найдем разность $f_1(x) = f(x) - h(x)\cdot\frac{a_n}{b_m}x^{n-m}$:

$$\begin{array}{r|l} f(x) & h(x) \\ \hline h(x)\cdot\frac{a_n}{b_n}x^{n-m} & \frac{a_n}{b_m}x^{n-m} \\ \hline f_1(x) & \end{array}$$

Получаем $f(x) = h(x)\cdot\frac{a_n}{b_m}x^{n-m} + f_1(x)$. Если $f_1(x)$ нулевой многочлен или его степень меньше степени делителя, то, обозначив $q(x) = \frac{a_n}{b_m}x^{n-m}$, $r(x) = f_1(x)$, получим требуемое. Если же степень $f_1(x)$ не меньше степени $h(x)$, то продолжим деление «уголком». Пусть $f_1(x) = c_k x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_0$, $c_k \neq 0$, $k \geq m$. На втором шаге деления получаем

$$\begin{array}{r|l} f(x) & h(x) \\ \hline h(x)\cdot\frac{a_n}{b_n}x^{n-m} & \frac{a_n}{b_m}x^{n-m} + \frac{c_k}{b_m}x^{k-m} \\ \hline f_1(x) & \\ \hline h(x)\cdot\frac{c_k}{b_m}x^{k-m} & \\ \hline f_2(x) & \end{array}$$

Следовательно, $f_2(x) = f_1(x) - h(x)\cdot\frac{c_k}{b_m}x^{k-m}$, откуда $f_1(x) = h(x)\cdot\frac{c_k}{b_m}x^{k-m} + f_2(x)$. Таким образом,

$$f(x) = h(x)\cdot\frac{a_n}{b_m}x^{n-m} + f_1(x) = h(x)\cdot\frac{a_n}{b_m}x^{n-m} + h(x)\cdot\frac{c_k}{b_m}x^{k-m} + f_2(x) =$$
$$= h(x)\left(\frac{a_n}{b_m}x^{n-m} + \frac{c_k}{b_m}x^{k-m}\right) + f_2(x).$$

Если $f_2(x)$ нулевой многочлен или его степень меньше степени делителя $h(x)$, то, положив $q(x) = \frac{a_n}{b_m}x^{n-m} + \frac{c_k}{b_m}x^{k-m}$, $r(x) = f_2(x)$, получим $f(x) = h(x) \cdot q(x) + r(x)$, что и требовалось доказать. Если же степень $f_2(x)$ не меньше степени $h(x)$, то продолжим деление «уголком». Поскольку степени многочленов $f(x), f_1(x), f_2(x)$, ... убывают, то процесс деления «уголком» конечен и на конечном шаге мы получим требуемое равенство.

Единственность. Предположим, что $f(x) = h(x) \cdot q(x) + r(x)$ и $f(x) = h(x) \cdot q_1(x) + r_1(x)$, где многочлены $r(x)$ и $r_1(x)$ либо нулевые, либо их степени меньше степени многочлена $h(x)$. Тогда $h(x) \cdot q(x) + r(x) = h(x) \cdot q_1(x) + r_1(x)$, откуда $r(x) - r_1(x) = h(x)(q_1(x) - q(x))$. Если предположить, что многочлен $r(x) - r_1(x)$ ненулевой, то его степень меньше степени многочлена $h(x)$, в то время как в правой части равенства стоит многочлен, степень которого не меньше степени многочлена $h(x)$. Из полученного противоречия делаем вывод, что $r(x) - r_1(x) = 0$, откуда $r(x) = r_1(x)$. Но тогда $h(x)(q_1(x) - q(x)) = 0$, а так как $h(x) \neq 0$, то $q_1(x) - q(x) = 0$ и $q_1(x) = q(x)$. Теорема доказана.

2.2.2. Алгоритм Евклида

Определение 2.5. Пусть даны многочлены $f(x)$ и $h(x) \neq 0$ над полем P. *Алгоритмом Евклида* называется следующая последовательность действий.

1. (*Начало алгоритма*). Многочлен $f(x)$ делим с остатком на многочлен $h(x)$.

2. (*Шаг алгоритма*). Если полученный остаток не равен нулю, то делитель делим на остаток. Если полученный остаток равен нулю, то алгоритм прекращается.

Выпишем последовательно шаги алгоритма Евклида:

$f(x) = h(x) \cdot q_1(x) + r_1(x)$, степень $r_1(x) <$ степени $h(x)$;

$h(x) = r_1(x) \cdot q_2(x) + r_2(x)$, степень $r_2(x) <$ степени $r_1(x)$;

$r_1(x) = r_2(x) \cdot q_3(x) + r_3(x)$, степень $r_3(x) <$ степени $r_2(x)$;

.....

$r_{n-2}(x) = r_{n-1}(x) \cdot q_n(x) + r_n(x)$, степень $r_n(x) <$ степени $r_{n-1}(x)$;

$r_{n-1}(x) = r_n(x) \cdot q_{n+1}(x) + r_{n+1}(x)$, $r_{n+1}(x) = 0$.

Поскольку степени остатков в алгоритме Евклида строго убывают, а целые неотрицательные числа бесконечно убывать не могут, то через конечное число шагов получим остаток, равный нулю. Это доказывает конечность алгоритма Евклида.

Теорема 2.3. *Пусть даны многочлены $f(x)$ и $h(x) \neq 0$ над полем P. Если $f(x) \vdots h(x)$, то* НОД$(f(x), h(x)) = h(x)$. *Если же $f(x)$*

не делится на $h(x)$, то последний отличный от нуля остаток в алгоритме Евклида, примененном к этим многочленам, является их наибольшим общим делителем.

Доказательство. Если $f(x) \vdots h(x)$, то, очевидно, $h(x)$ является общим делителем многочленов $f(x)$ и $h(x)$, который делится на любой общий делитель данных многочленов. Но это и означает, что НОД$(f(x), h(x)) = h(x)$.

Предположим теперь, что $f(x)$ не делится на $h(x)$. Применим к данным многочленам алгоритм Евклида и рассмотрим записанные выше шаги алгоритма снизу вверх. Из последнего равенства $r_{n-1}(x) = r_n(x) \cdot q_{n+1}(x)$ видим, что $r_{n-1}(x) \vdots r_n(x)$. Тогда из предпоследнего равенства $r_{n-2}(x) = r_{n-1}(x) \cdot q_n(x) + r_n(x)$ заключаем, что $r_{n-2}(x) \vdots r_n(x)$. И т.д., поднимаясь все выше, мы докажем, что $r_2(x) \vdots r_n(x)$ и $r_1(x) \vdots r_n(x)$, а из равенства $h(x) = r_1(x) \cdot q_2(x) + r_2(x)$ получаем $h(x) \vdots r_n(x)$. Наконец, из первого равенства $f(x) = h(x) \cdot q_1(x) + r_1(x)$ заключаем, что $f(x) \vdots r_n(x)$. Таким образом, $r_n(x)$ является общим делителем многочленов $f(x)$ и $h(x)$.

Пусть теперь $d(x)$ является общим делителем многочленов $f(x)$ и $h(x)$. Тогда из первого равенства $f(x) = h(x) \cdot q_1(x) + r_1(x)$ делаем вывод, что $r_1(x) \vdots d(x)$. Продвигаясь последовательно по равенствам сверху вниз, выводим, что $r_n(x) \vdots d(x)$. Таким образом, в соответствии с определением заключаем, что $r_n(x)$ является наибольшим общим делителем многочленов $f(x)$ и $h(x)$.

Теорема 2.4. *Пусть P — поле и $f(x), h(x) \in P[x]$. Если* НОД$(f(x), h(x)) = d(x)$, *то существуют многочлены $u(x), v(x) \in P[x]$, такие что $f(x) \cdot u(x) + h(x) \cdot v(x) = d(x)$.*

Доказательство. Рассмотрим шаги алгоритма Евклида и, спускаясь по равенствам сверху вниз, будем последовательно остатки выражать через данные многочлены $f(x)$ и $h(x)$. Используя для краткости упрощенную запись многочленов, из первой строчки алгоритма Евклида получаем $r_1 = f - h \cdot q_1 = f \cdot 1 + h \cdot (-q_1)$. Из второй строчки $r_2 = h - r_1 \cdot q_2 = h - (f - hq_1)q_2 = f(-1) + h(1 + q_1q_2)$ и т.д. На последнем шаге будем иметь $r_n(x) = f(x) \cdot u(x) + h(x) \cdot v(x)$ при некоторых $u(x), v(x) \in P[x]$. Если наибольший общий делитель $d(x)$ совпадает с наибольшим общим делителем $r_n(x)$, то теорема доказана. Если же нет, то, по теореме 2.1 $d(x) = k \cdot r_n(x)$ при некотором $0 \neq k \in P$. Но тогда $d(x) = k \cdot r_n(x) = f(x) \cdot k \cdot u(x) + h(x) \cdot k \cdot v(x) = f(x) \cdot u_1(x) + h(x) \cdot v_1(x)$.

Определение 2.6. Запись наибольшего общего делителя $d(x)$ многочленов $f(x)$ и $h(x)$ в виде $d(x) = f(x) \cdot u(x) + h(x) \cdot v(x)$ при некоторых $u(x), v(x) \in P[x]$ называется его *линейной формой.*

Поскольку наибольший общий делитель двух многочленов над полем находится с точностью до постоянного множителя, то при нахождении с помощью алгоритма Евклида наибольшего общего делителя многочленов с целыми коэффициентами можно избежать дробей, умножая на любом шаге алгоритма, если надо, делимое и делитель на подходящее целое число. Однако заметим, что при этом преобразовании «портятся» неполные частные, так что если нам нужна линейная форма наибольшего общего делителя, то нужны неполные частные, а значит, указанное преобразование недопустимо.

Пример 2.2

Упростим выражение $\dfrac{2x^3+x^2-x+3}{3x^5-5x^4+5x^3-5x^2+3x-3}$.

Решение. С помощью алгоритма Евклида найдем наибольший общий делитель числителя $f(x)$ и знаменателя $g(x)$, а затем произведем сокращение. Чтобы избежать дробей, воспользуемся сделанным выше замечанием и многочлены $f(x)$ и $g(x)$ заменим на соответственно $3f(x)$ и $2g(x)$. Подобные преобразования в дальнейшем будем отмечать двумя чертами:

$$
\begin{array}{l|l}
\_\,6x^5-10x^4+10x^3-10x^2+6x-6 & \underline{6x^3+3x^2-3x+9} \\
\underline{6x^5+3x^4\ -\ 3x^3+\ 9x^2} & \quad x^2\,||-13x||+39 \\
\underline{\underline{-13x^4+13x^3-19x^2+6x-6}} & \\
\_\,-78x^4+78x^3-114x^2+36x-36 & \\
\underline{-78x^4-39x^3+39x^2-117x} & \\
\underline{\underline{117x^3-153x^2+153x-36}} & \\
\_\,234x^3-306x^2+306x-72 & \\
\underline{234x^3+117x^2-117x+351} & \\
\underline{\underline{-423x^2+423x-423}} & \\
\_\,2x^3+x^2-x+3 \quad \Big| \quad \underline{x^2-x+1} & \\
\underline{2x^3-2x^2+2x} \quad\ \Big| \quad 2x+3 & \\
\_\,3x^2-3x+3 & \\
\underline{3x^2-3x+3} & \\
0 &
\end{array}
$$

Следовательно, НОД$(f(x), g(x)) = x^2 - x + 1$. Произведя сокращение, получим

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

Пример 2.3

Докажем, что не имеет решения система уравнений

$$\begin{cases} 2x^3 + x^2 - x + 3 = 0, \\ 3x^5 - 5x^4 + 5x^3 - 5x^2 + 3x - 3 = 0, \\ 2x^4 - x^3 + 5 = 0. \end{cases}$$

Решение (*доказательство*). Обозначим многочлены системы соответственно $f(x)$, $g(x)$, $h(x)$. Воспользовавшись предыдущим примером, получаем НОД$(f(x), g(x)) = x^2 - x + 1$. Далее устанавливаем, что НОД$(f(x), g(x), h(x)) = 1$. Следовательно, данные многочлены не имеют общего множителя положительной степени, а значит, не имеют и общего корня.

2.2.3. Взаимно простые многочлены

Определение 2.7. Многочлены $f(x)$ и $h(x)$ называются *взаимно простыми*, если НОД$(f(x), h(x)) = 1$.

Теорема 2.5 (критерий взаимной простоты двух многочленов). *Многочлены $f(x)$ и $h(x)$ взаимно просты тогда и только тогда, когда существуют многочлены $u(x)$ и $v(x)$, такие что $f(x) \cdot u(x) + h(x) \cdot v(x) = 1$.*

Доказательство. ($\Rightarrow$) Если многочлены $f(x)$ и $h(x)$ взаимно просты, то, по определению, один из их наибольших общих делителей равен 1. Его линейная форма (найденная из алгоритма Евклида) имеет указанный в теореме вид.

($\Leftarrow$) Пусть $f(x) \cdot u(x) + h(x) \cdot v(x) = 1$. Обозначим НОД$(f(x), h(x)) = d(x)$. Поскольку $f(x) \vdots d(x)$ и $h(x) \vdots d(x)$, то $1 \vdots d(x)$. Отсюда следует, что степень многочлена $d(x)$ равна 0 и $d(x) = d_0 \in \in P \setminus \{0\}$. Следовательно, одним из наибольших общих делителей данных многочленов является 1. Но это и означает, что данные многочлены взаимно просты.

Рассмотрим основные свойства взаимно простых многочленов.

1. *Если произведение многочленов $f(x) \cdot g(x)$ делится на многочлен $h(x)$ и* НОД$(f(x), h(x)) = 1$, *то многочлен $g(x)$ делится на $h(x)$.*

Доказательство. Из условия взаимной простоты многочленов $f(x)$ и $h(x)$ по критерию взаимной простоты (теорема 2.5) существуют многочлены $u(x)$ и $v(x)$, такие что $f(x) \cdot u(x) + + h(x) \cdot v(x) = 1$. Умножив обе части равенства на $g(x)$, получим $f(x)g(x) \cdot u(x) + h(x)g(x) \cdot v(x) = g(x)$. Поскольку оба слагаемых делятся на $h(x)$, то и их сумма, равная $g(x)$, делится на $h(x)$.

2. *Для многочленов* $f(x)$, $g(x) \in P(x)$ *если* НОД$(f(x), g(x)) = d(x)$, *то существуют многочлены* $f_1(x)$, $g_1(x) \in P(x)$, *такие что* $f(x) = f_1(x)d(x)$, $g(x) = g_1(x)d(x)$ и НОД$(f_1(x), g_1(x)) = 1$.

Доказательство. Из того, что НОД$(f(x), g(x)) = d(x)$, следует существование многочленов $f_1(x)$, $g_1(x) \in P(x)$, таких что $f(x) = f_1(x)d(x)$ и $g(x) = g_1(x)d(x)$. С другой стороны, существуют многочлены $u(x)$, $v(x) \in P(x)$, такие что $f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$. Тогда $f_1(x)d(x)u(x) + g_1(x)d(x)v(x) = d(x)$, откуда $f_1(x) \cdot u(x) + g_1(x) \cdot v(x) = 1$. Следовательно, НОД$(f_1(x), h_1(x)) = 1$.

3. *Если каждый из многочленов* $f_1(x)$ *и* $f_2(x)$ *взаимно прост с многочленом* $g(x)$, *то и произведение* $f_1(x) \cdot f_2(x)$ *взаимно просто с многочленом* $g(x)$.

Доказательство. Воспользуемся краткой записью многочленов. По условию, НОД$(f_1, g) = 1$ и НОД$(f_2, g) = 1$. Следовательно, существуют многочлены $u_1(x)$, $v_1(x)$ и $u_2(x)$, $v_2(x)$, такие что $f_1u_1 + gv_1 = 1$ и $f_2u_2 + gv_2 = 1$. Перемножив эти равенства, получим $f_1f_2u_1u_2 + g(f_1u_1v_2 + f_2u_2v_1 + gv_1v_2) = 1$. Следовательно, $(f_1f_2, g) = 1$.

Многократным применением этого свойства можно доказать, что если каждый из многочленов $f_1(x)$, ..., $f_k(x)$ взаимно прост с каждым из многочленов $g_1(x)$, ..., $g_m(x)$, то произведения $f_1(x) \cdot \ldots \cdot f_k(x)$ и $g_1(x) \cdot \ldots \cdot g_m(x)$ взаимно просты. Отсюда следует, что из взаимной простоты многочленов $f(x)$ и $g(x)$ следует взаимная простота их степеней.

Контрольные вопросы

1. Пусть при делении с остатком одного многочлена на другой степени делимого, делителя, неполного частного и остатка равны соответственно n, m, k, l. Какое из соотвношений является верным: а) $n = mk + l$; б) $n = m + k + l$; в) $n = m + k$?
2. Алгоритм Евклида применяется к многочленам $f(x)$, $h(x)$ степеней n и m, причем $m < n$. Каково наибольшее (наименьшее) возможное число шагов алгоритма?
3. Что представляет собой линейная форма НОД двух многочленов?
4. Изменится ли НОД двух многочленов над полем $\mathbb{Q}$, если один из них умножить на 5? Умножить на x? Оба умножить на x?
5. Если целые числа взаимно просты, то будут ли они взаимно простыми как многочлены?
6. Если два многочлена нулевой степени над кольцом целых чисел взаимно просты как многочлены, то будут ли они взаимно простыми числами?
7. Какие из свойств взаимно простых многочленов справедливы и для чисел?

Задачи

1. Найдите $d(x) = \text{НОД}(f(x), h(x))$, если:

а) $f(x) = x^6 + 8x^5 + 22x^4 + 43x^3 + 70x^2 + 57x + 39$, $h(x) = x^4 + 7x^3 + 14x^2 + 21x + 33$;

б) $f(x) = 2x^7 + x^6 - x^5 + 9x^4 - 3x^3 - 8x - 7$, $h(x) = 2x^6 - x^5 + 11x^3 - 10x^2 + x - 9$;

в) $f(x) = 6x^5 + x^4 + 12x^3 - 42x^2 + 30x + 25$, $h(x) = 2x^4 - x^3 + 4x^2 - 17x + 20$.

2. Найдите линейную форму $\text{НОД}(f(x), h(x))$, если:

а) $f(x) = x^6 - x^5 - 10x^2 + 9x - 3$, $h(x) = x^4 + x^3 + 2x^2 + 3x - 3$;

б) $f(x) = 3x^6 - 8x^5 + 5x^4 - 11x^3 - 10x^2 - 21x + 31$, $h(x) = x^5 - 2x^4 - 4x^2 - 7x - 13$;

в) $f(x) = x^5 - 2x^4 - 3x^3 + 5x^2 - 4x - 2$, $h(x) = x^4 - x^3 - 4x^2 - 3$.

3. Упростите выражения:

а) $\dfrac{2x^5+11x^4+5x^3-2x^2-11x-5}{x^3+4x^2+4x+3}$;

б) $\dfrac{x^5+x^4+10x^2-6x+9}{x^6-x^5+3x^4+3x^3+4x^2+2x+21}$;

в) $\dfrac{x^5-6x^3+5x^2-9x+9}{2x^6+4x^5-9x^4-6x^3+14x^2+10x-15}$;

г) $\dfrac{2x^5+x^4-19x^3+29x^2-26x+8}{x^3+x^2-x+2}$.

2.3. Разложение на множители в кольце многочленов над полем

2.3.1. Неприводимые многочлены

Подобно тому как всякое натуральное число, отличное от единицы, можно разложить на простые множители, так и всякий многочлен степени $n \geq 1$ можно представить в виде произведения многочленов, которые дальше уже нельзя разложить на множители нетривиальным образом. Для уточнения этого факта введем понятие, являющееся аналогом простого числа.

Определение 2.8. Многочлен $p(x)$ с коэффициентами из поля P называется *неприводимым над полем P*, если его степень ≥ 1 и он не представим в виде произведения многочленов из $P[x]$ степени ≥ 1. Многочлен $f(x) \in P[x]$ называется *приводимым над полем P*, если он представим в виде произведения многочленов степени ≥ 1 из $P[x]$.

Таким образом, кольцо многочленов $P[x]$ состоит из элементов поля P — это нулевой многочлен и многочлены степени 0,

а остальные многочлены из $P[x]$ подразделяются на неприводимые и приводимые.

Пример 2.4

Приведем примеры неприводимости.

1. Понятно, что всякий многочлен первой степени из $P[x]$ неприводим над полем P, так как его нельзя представить в виде произведения многочленов степени ≥ 1.

2. Многочлен $x^2 - 2$ неприводим над полем $\mathbb{Q}$, но приводим над полем действительных чисел $\mathbb{R}$, так как $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$.

3. Многочлен $x^2 + 1$ неприводим над полем действительных чисел $\mathbb{R}$, но приводим над полем комплексных чисел $\mathbb{C}$, так как $x^2 + 1 = (x + i)(x - i)$.

Рассмотренные примеры показывают, что, вообще говоря, неприводимость многочлена зависит от того, над каким полем он рассматривается.

2.3.2. Основные свойства неприводимых над данным полем многочленов

1. *Делителями неприводимого над полем P многочлена $p(x)$ являются лишь всякий ненулевой элемент $k \in P$ и $kp(x)$.*

Доказательство. Очевидно, ненулевой элемент $k \in P$ и $kp(x)$ являются делителями многочлена $p(x)$. Пусть $p(x) \vdots d(x)$, тогда $p(x) = d(x) \cdot q(x)$ при некотором $q(x) \in P[x]$. Но многочлен $p(x)$ неприводим, а значит, не представим в виде произведения многочленов степени ≥ 1. Следовательно, один из многочленов $d(x)$ или $q(x)$ должен иметь нулевую степень. Если $d(x) = k \in P \setminus \{0\}$, то утверждение в этом случае доказано. Если же $q(x) = q$, где $0 \neq q \in P$, то существует q^{-1}, и из равенства $p(x) = d(x) \cdot q$ находим $d(x) = q^{-1} \cdot p(x)$. Свойство доказано.

2. *Если многочлены $p(x)$, $q(x) \in P[x]$ неприводимы над полем P и $p(x) \vdots q(x)$, то $q(x) = kp(x)$ при некотором $0 \neq k \in P$, откуда $p(x) = k^{-1}q(x)$.*

Доказательство. По предыдущему свойству делители неприводимого многочлена $p(x)$ исчерпываются элементами $0 \neq k \in P$ и многочленами вида $kp(x)$. Поскольку многочлен $q(x)$ имеет степень не меньше 1 и является делителем многочлена $p(x)$, то он совпадает с одним из многочленов вида $kp(x)$.

3. *Если многочлен $p(x) \in P[x]$ неприводим над полем P, то для любого многочлена $f(x) \in P[x]$ либо $f(x) \vdots p(x)$, либо $f(x)$ и $p(x)$ взаимно просты.*

Доказательство. Пусть НОД($f(x), p(x)$) = $d(x)$. Тогда $p(x) \vdots d(x)$ и по свойству 1 либо $d(x) = k \neq 0$, откуда НОД($f(x), p(x)$) = 1, либо $d(x) = kp(x)$, и тогда $f(x) \vdots d(x) \vdots p(x)$.

4. *Если многочлен $p(x) \in P[x]$ неприводим над полем P и для многочленов $f(x), h(x) \in P[x]$ произведение $f(x) \cdot h(x) \vdots p(x)$, то хотя бы один из сомножителей $f(x)$ или $h(x)$ делится на $p(x)$.*

Доказательство. Если $f(x) \vdots p(x)$, то доказывать нечего. Если же $f(x)$ не делится на $p(x)$, то по свойству 3 НОД($f(x), p(x)$) = 1 и по свойству 1 взаимно простых многочленов получаем, что $h(x) \vdots p(x)$.

2.3.3. Разложение многочлена в произведение неприводимых множителей

Основная теорема арифметики гласит: *всякое натуральное число, отличное от единицы, либо является простым, либо представимо в виде произведения простых множителей, причем однозначно, если не обращать внимания на порядок следования сомножителей.* Докажем аналог этой теоремы для кольца многочленов $P[x]$ над полем P. Разложение чисел или многочленов на множители называется факторизацией, отсюда название теоремы.

Теорема 2.6 (о факторизации в кольце многочленов над полем). *Всякий многочлен $f(x) \in P[x]$ степени $n \geq 1$ либо неприводим над полем P, либо представим в виде произведения неприводимых над полем P многочленов, причем однозначно с точностью до порядка следования сомножителей и ненулевых элементов поля P, т.е. между неприводимыми множителями двух разложений данного многочлена можно установить взаимно однозначное соответствие, при котором соответствующие неприводимые множители могут отличаться лишь на ненулевой элемент поля P.*

Доказательство. Сначала докажем возможность разложения многочлена $f(x)$ на неприводимые множители. Если многочлен $f(x)$ неприводим, то утверждение доказано. Если же он приводим, то $f(x) = g(x) \cdot h(x)$, где степени сомножителей ≥ 1. Если оба сомножителя неприводимы, то утверждение доказано. Если же нет, то продолжим разложение на множители. Поскольку в этих рассуждениях степени сомножителей строго убывают, а целые неотрицательные числа бесконечно убывать не могут, то через конечное число шагов получим искомое разложение многочлена $f(x)$ в произведение неприводимых множителей.

Пусть имеем два разложения многочлена $f(x)$ в произведение неприводимых над данным полем многочленов:

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_m(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_n(x).$$

Докажем, что $m = n$ и множители этих двух разложений можно так сопоставить друг другу, что соответствующие многочлены будут либо равны, либо отличаться один от другого лишь на ненулевой элемент поля P.

Видим, что правая часть равенства делится на неприводимый многочлен $q_1(x)$, а значит, произведение $p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_m(x)$ делится на $q_1(x)$. По свойству 4 неприводимых многочленов отсюда следует, что один из сомножителей должен делиться на $q_1(x)$. Пусть $p_1(x) \vdots q_1(x)$, тогда по свойству 2 $q_1(x) = k_1 p_1(x)$ при некотором $0 \neq k_1 \in P$ и мы получаем

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_m(x) = k_1 p_1(x) \cdot q_2(x) \cdot \ldots \cdot q_n(x).$$

Отсюда $p_2(x) \cdot \ldots \cdot p_m(x) = k_1 q_2(x) \cdot \ldots \cdot q_n(x)$ и повторяем рассуждения. Если предположить, что $m \neq n$, то, не нарушая общности, можно считать, что $m > n$. Тогда на n-м шаге будем иметь $p_{n+1}(x) \cdot p_{n+2}(x) \cdot \ldots \cdot p_m(x) = k_1 k_2 \cdot \ldots \cdot k_n$, чего не может быть, поскольку в правой части равенства стоит многочлен степени 0, а степень многочлена в левой части ≥ 1. Следовательно, $m = n$ и можно считать, что для любого $i = 1, 2, \ldots, n$, $q_i(x) = k_i p_i(x)$, где $0 \neq k_i \in P$. Теорема доказана.

Определение 2.9. *Каноническим разложением многочлена* $f(x) \in P[x]$ будем называть представление его в виде произведения степеней неприводимых над полем P взаимно простых множителей: $f(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_n^{\alpha_n}(x)$, где $\alpha_i > 0$, $i = 1, \ldots, n$.

Например, каноническим разложением на неприводимые над полем $\mathbb{R}$ множители многочлена $f(x) = (x^4 - 1)^2(x + 1)$ является представление его в виде $f(x) = (x^2 + 1)^2(x - 1)^2(x + 1)^2$.

Введем для многочленов аналог наименьшего общего кратного натуральных чисел.

Определение 2.10. Многочлен $m(x)$ называется *наименьшим общим кратным многочленов* $f(x)$ *и* $h(x)$, если $m(x)$ является общим кратным данных многочленов, т.е. делится на каждый из них, и любое общее кратное данных многочленов делится на $m(x)$. Обозначение: НОК$(f(x), h(x)) = m(x)$.

Как и в случае наибольшего общего делителя, равенство НОК$(f(x), h(x)) = m(x)$ означает, что $m(x)$ — одно из наименьших общих кратных данных многочленов. Легко видеть, что

наименьшее общее кратное двух многочленов находится однозначно с точностью до ненулевого элемента поля P.

Пусть даны представления многочленов в виде произведения степеней взаимно простых неприводимых множителей:

$$f(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_n^{\alpha_n}(x), h(x) = p_1^{\beta_1}(x) \cdot p_2^{\beta_2}(x) \cdot \ldots \cdot p_n^{\beta_n}(x),$$

где $\alpha_i \geq 0$ и $\beta_i \geq 0$ для $i = 1, 2, \ldots, n$. Тогда НОД($f(x)$, $h(x)$) = $= p_1^{\gamma_1}(x) \cdot p_2^{\gamma_2}(x) \cdot \ldots \cdot p_n^{\gamma_n}(x)$, где $\gamma_i = \min\{\alpha_i, \beta_i\}$, НОК($f(x)$, $h(x)$) = $= p_1^{\delta_1}(x) \cdot p_2^{\delta_2}(x) \cdot \ldots \cdot p_n^{\delta_n}(x)$, где $\delta_i = \max\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, n$.

Другими словами, чтобы найти наибольший общий делитель многочленов $f(x)$ и $h(x)$, достаточно выписать все одинаковые неприводимые множители данных многочленов и найти их произведение. Чтобы найти наименьшее общее кратное данных многочленов, нужно выписать все неприводимые множители из разложения $f(x)$ и приписать к ним недостающие неприводимые множители из разложения $h(x)$. Произведение выписанных многочленов и является наименьшим общим кратным данных многочленов.

Теорема 2.7. *Для многочленов $f(x)$ и $h(x)$ можно так выбрать наименьшее общее кратное $m(x)$ и наибольший общий делитель $d(x)$, что $m(x) \cdot d(x) = f(x) \cdot h(x)$.*

Доказательство. Рассмотрим разложения данных многочленов в произведение неприводимых множителей:

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_k(x) \cdot q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_m(x);$$

$$h(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_m(x) \cdot r_1(x) \cdot r_2(x) \cdot \ldots \cdot r_n(x),$$

где разными буквами обозначены взаимно простые многочлены. Используя краткую запись многочленов, получаем $f = p_1 p_2 \cdots p_k \cdot q_1 q_2 \cdots q_m$ и $h = q_1 q_2 \cdots q_m \cdot r_1 r_2 \cdots r_n$. Тогда

$$m(x) = \text{НОК}(f, h) = p_1 p_2 \cdots p_k \cdot q_1 q_2 \cdots q_m \cdot r_1 r_2 \cdots r_n;$$

$$d(x) = \text{НОД}(f, h) = q_1 q_2 \cdots q_m;$$

$$m(x) \cdot d(x) = p_1 p_2 \cdots p_k \cdot q_1 q_2 \cdots q_m \cdot r_1 r_2 \cdots r_n \cdot q_1 q_2 \cdots q_m = f(x) \cdot h(x).$$

Теорема доказана.

2.3.4. Кратные неприводимые множители

Определение 2.11. Для многочлена $f(x) \in P[x]$ неприводимый над полем P многочлен $p(x)$ называется *неприводимым*

множителем кратности α, если $f(x) \vdots p^{\alpha}(x)$, но $f(x)$ не делится на $p^{\alpha+1}(x)$ (другими словами, если $f(x) = p^{\alpha}(x) \cdot h(x)$, где НОД$(p(x), h(x)) = 1$).

Вспоминая определение кратного корня, можно теперь сказать, что корень c многочлена $f(x)$ имеет кратность α, если $x - c$ является неприводимым множителем кратности α для $f(x)$.

Если дано каноническое разложение многочлена на неприводимые множители $f(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_n^{\alpha_n}(x)$, то для любого $i = 1, 2, \ldots$ показатель степени α_i показывает кратность неприводимого множителя $p_i(x)$ для $f(x)$.

Определение 2.12. Будем говорить, что многочлен $f(x)$ *не имеет кратных множителей*, если всякий его неприводимый множитель имеет кратность 1. В противном случае будем говорить, что *многочлен имеет кратные множители.*

Например, многочлен $f(x) = (x^2 + 1)(x - 1)$ не имеет кратных множителей, а многочлен $h(x) = (x^2 - 1)(x - 1)$ имеет кратный множитель $x - 1$ кратности 2.

Для распознавания существования у данного многочлена кратных множителей нам понадобится понятие производной многочлена. При этом мы ограничимся рассмотрением многочленов над числовыми полями. Таковы, например, поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. До конца этого параграфа P будет обозначать числовое поле.

Определение 2.13. Пусть P — числовое поле. *Производной* многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in P[x]$ называется многочлен $f'(x) = a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \ldots + a_1$.

Пользуясь определением 2.13, легко доказать следующие *правила дифференцирования многочленов*, известные из математического анализа:

1) $(f(x) + g(x))' = f'(x) + g'(x)$;
2) $(ax^n \cdot bx^m)' = (ax^n)' \cdot (bx^m) + (ax^n) \cdot (bx^m)'$, где $a, b \in P$;
3) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$;
4) $(f^n(x))' = n f^{n-1}(x) f'(x)$, $n \in \mathbb{N}$.

Равенства 1) и 2) легко доказываются непосредственным вычислением левой и правой частей равенств. Для доказательства равенства 3) можно сначала индукцией по степени многочлена $h(x)$ доказать равенство $(ax^n \cdot h(x))' = (ax^n)' \cdot h(x) + ax^n \cdot h'(x)$, а затем доказать (3) индукцией по степени многочлена $f(x)$. Равенство (4) легко доказывается индукцией по n.

Теорема 2.8. *Если для многочлена $f(x)$ над числовым полем P многочлен $p(x)$ над тем же полем является неприводимым*

множителем кратности α, *то для производной* $f'(x)$ *он будет неприводимым множителем кратности* $\alpha - 1$.

Доказательство. По условию, $f(x) = p^{\alpha}(x) \cdot h(x)$, где НОД$(p(x), h(x)) = 1$. Используя правила дифференцирования, получаем $f'(x) = \alpha p^{\alpha-1}(x) \cdot p'(x) \cdot h(x) + p^{\alpha}(x) \cdot h'(x) = p^{\alpha-1}(x)\ (\alpha p'(x) \cdot h(x) + p(x) \cdot h'(x))$. Следовательно, $f'(x) \vdots p^{\alpha-1}(x)$. Если предположить, что $f'(x) \vdots p^{\alpha}(x)$, то сумма $\alpha p'(x) \cdot h(x) + p(x) \cdot h'(x)$ должна делиться на $p(x)$. Поскольку второе слагаемое этой суммы также делится на $p(x)$, то $\alpha p'(x) \cdot h(x) \vdots p(x)$. Отсюда следует, что один из сомножителей должен делиться на $p(x)$. Но $p'(x)$ не может делиться на $p(x)$, так как степень многочлена больше степени его производной, а $h(x)$ не может делиться на $p(x)$ по условию. Пришли к противоречию. Таким образом, кратность неприводимого множителя $p(x)$ для производной $f'(x)$ равна $\alpha - 1$.

Из доказанной теоремы выведем ряд полезных следствий. Первое следствие непосредственно вытекает из теоремы 2.8, из него вытекает второе, а из второго — третье. Четвертое следствие непосредственно следует из первого. Оно является основным для следующего подпараграфа 2.3.5.

Следствие 1. Если $f(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_n^{\alpha_n}(x)$ — каноническое разложение многочлена на неприводимые множители, то $f'(x) = p_1^{\alpha_1-1}(x) \cdot p_2^{\alpha_2-1}(x) \cdot \ldots \cdot p_n^{\alpha_n-1}(x) \cdot q(x)$, где $f(x)$ и $q(x)$ взаимно просты.

Следствие 2. Многочлен $f(x)$ не имеет кратных множителей тогда и только тогда, когда он взаимно прост со своей производной.

Следствие 3. Элемент $c \in P$ является кратным корнем многочлена $f(x) \in P[x]$ тогда и только тогда, когда c является корнем производной $f'(x)$.

Следствие 4. Если $f(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \ldots \cdot p_n^{\alpha_n}(x)$ — каноническое разложение многочлена на неприводимые множители, то НОД$(f(x), f'(x)) = p_1^{\alpha_1-1}(x) \cdot p_2^{\alpha_2-1}(x) \cdot \ldots \cdot p_n^{\alpha_n-1}(x)$.

2.3.5. Алгоритм отделения кратных множителей

Пусть известно разложение многочлена $f(x)$ в произведение неприводимых множителей. Обозначим через $F_1(x)$ произведение всех неприводимых множителей многочлена $f(x)$ кратности 1, через $F_2(x)$ — произведение всех неприводимых множителей многочлена $f(x)$ кратности 2 и т.д., $F_m(x)$ — произведение всех неприводимых множителей многочлена $f(x)$ наибольшей кратности m. Тогда $f(x) = F_1(x) \cdot F_2^2(x) \cdot \ldots \cdot F_m^m(x)$.

Пример 2.5

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

Тогда $F_1(x) = x^2 + 1$, $F_2(x) = x^2 - 1$, $F_3(x) = 3x - 2$ и $f(x) = F_1(x) \cdot F_2^2(x) \cdot F_3^3(x)$.

Разложение многочлена в произведение неприводимых множителей — очень трудная задача. Нет общего алгоритма ее решения. Однако есть алгоритм, позволяющий найти по данному многочлену $f(x)$ многочлены $F_1(x), F_2(x), ..., F_m(x)$ и представить данный многочлен в виде произведения $f(x) = F_1(x) \cdot F_2^2(x) \cdot ... \cdot F_m^m(x)$. Тем самым он позволяет *отделить* одно от другого произведения неприводимых множителей одинаковой кратности. Рассмотрим этот *алгоритм отделения кратных множителей.*

Пусть дан многочлен $f(x)$ над числовым полем P.

Первый шаг алгоритма. Полагаем $d_0(x) = f(x)$ и, пользуясь следствием 4 из теоремы 2.8, находим последовательно:

$$d_1(x) = \text{НОД}(d_0(x), d_0'(x)) =$$
$$= \text{НОД}(f(x), f'(x)) = F_2(x) \cdot F_3^2(x) \cdot ... \cdot F_m^{m-1}(x);$$

$$d_2(x) = \text{НОД}(d_1(x), d_1'(x)) = F_3(x) \cdot F_4^2(x) \cdot ... \cdot F_m^{m-2}(x);$$

.....

$$d_{m-1}(x) = \text{НОД}(d_{m-2}(x), d_{m-2}'(x)) = F_m(x).$$

Полагаем $d_m(x) = 1$.

Второй шаг алгоритма. Находим последовательно:

$$D_1(x) = \frac{d_0(x)}{d_1(x)} = F_1(x) \cdot F_2(x) \cdot ... \cdot F_m(x);$$

$$D_2(x) = \frac{d_1(x)}{d_2(x)} = F_2(x) \cdot F_3(x) \cdot ... \cdot F_m(x);$$

.....

$$D_m(x) = \frac{d_{m-1}(x)}{d_m(x)} = F_m(x).$$

Полагаем $D_{m+1}(x) = 1$.

Третий шаг алгоритма. Находим последовательно:

$$\frac{D_1(x)}{D_2(x)} = F_1(x), \frac{D_2(x)}{D_3(x)} = F_2(x), ..., \frac{D_m(x)}{D_{m+1}(x)} = F_m(x).$$

Если теперь неизвестно разложение многочлена $f(x)$ в произведение неприводимых множителей, мы, следуя алгоритму, можем, тем не менее, представить его в виде $f(x) = F_1(x)\cdot F_2^2(x)\cdot\ldots\cdot F_m^m(x)$.

Пример 2.6

Дан многочлен $f(x) = x^5 - x^3 - 4x^2 - 3x - 2$. Отделим кратные множители.

Решение. 1-й шаг. Полагаем $d_0(x) = f(x)$ и находим $f'(x) = 5x^4 - 3x^2 - 8x - 3$. Пользуясь алгоритмом Евклида, находим НОД$d_1(x) = (f(x), f'(x))$. Чтобы избежать дробей, используем возможность умножения делимого, делителя и остатка на любое рациональное число. При этом, как и раньше, изменения неполного частного будем отмечать значком ||.

Запуская алгоритм Евклида, сначала нужно $f(x)$ разделить «уголком» на $f'(x)$. Чтобы избежать дробей, умножим $f(x)$ на 5:

$$\begin{array}{l|l} 5x^5-5x^3-20x^2-15x-10 & 5x^4-3x^2-8x-3 \\ \underline{5x^5-3x^3-8x^2-3x} & x \\ -2x^3-12x^2-12x-10 & \end{array}$$

Теперь нужно делитель разделить на остаток (но предварительно остаток разделим на –2):

$$\begin{array}{l|l} 5x^4-3x^2-8x-3 & x^3+6x^2+6x+5 \\ \underline{5x^4+30x^3+30x^2+25x} & 5x\,||+10 \\ \underline{-30x^3-33x^2-33x-3} & \\ 10x^3+11x^2+11x+1 & \\ \underline{10x^3+60x^2+60x+50} & \\ \underline{-49x^2-49x-49} & \\ x^2+x+1 & \end{array}$$

Снова делитель делим на остаток:

$$\begin{array}{l|l} x^3+6x^2+6x+5 & x^2+x+1 \\ \underline{x^3+x^2+x} & x+5 \\ 5x^2+5x+5 & \\ \underline{5x^2+5x+5} & \\ 0 & \end{array}$$

Итак, $d_1(x) = \text{НОД}(f(x), f'(x)) = x^2 + x + 1$. Находим $d_1'(x) = 2x + 1$ и $d_2(x) = \text{НОД}(d_1(x), d_1'(x))$. Легко видеть, что $d_2(x) = 1$.

2-й шаг. Находим (путем деления «уголком»):

$$D_1(x) = \frac{d_0(x)}{d_1(x)} = \frac{x^5 - x^3 - 4x^2 - 3x - 2}{x^2 + x + 1} = x^3 - x^2 - x - 2,$$

$$D_2(x)=\frac{d_1(x)}{d_2(x)}=x^2+x+1$$

и полагаем $D_3(x)=1$.

3-й шаг. Находим

$$F_1(x)=\frac{D_1(x)}{D_2(x)}=x-2,\ F_2(x)=\frac{D_2(x)}{D_3(x)}=x^2+x+1.$$

Ответ: $f(x)=(x-2)(x^2+x+1)^2$.

Заметим, что если данный многочлен $f(x)$ рассматривать над полем действительных чисел, то, желая лишь отделить кратные множители, мы достигли большего: получили разложение данного многочлена в произведение неприводимых над полем действительных чисел множителей. Если же мы хотим получить разложение многочлена $f(x)$ в произведение неприводимых множителей над полем комплексных чисел, то нужно предпринять дополнительные усилия и разложить многочлен x^2+x+1 на линейные множители. Для этого находим корни $x_1=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $x_2=-\frac{1}{2}-i\frac{\sqrt{3}}{2}$, тогда

$$x^2+x+1=(x-x_1)(x-x_2)=\left(x+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\left(x+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right).$$

В итоге получаем

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

2.3.6. Представление отношений многочленов в виде суммы простейших дробей

В математическом анализе рассматривается интегрирование *рациональных дробей* или *отношений многочленов* вида $\frac{f(x)}{h(x)}$, где в числителе и знаменателе стоят многочлены над некоторым числовым полем P. Отодвигая строгую теорию отношений многочленов на конец параграфа 2.3, будем опираться на школьные представления о них. Нашей главной целью является показать как на практике «работает» теория делимости многочленов.

Как обычно, считаем, что для любых многочленов $a(x)$, $b(x)\neq 0$, $c(x)$, $d(x)\neq 0$, $k(x)\neq 0$ над полем P

$$a(x)=\frac{a(x)}{1},\ \frac{a(x)}{b(x)}=\frac{c(x)}{d(x)}\ \Leftrightarrow\ a(x)\cdot d(x)=b(x)\cdot c(x),$$

$$\frac{k(x)\cdot a(x)}{k(x)\cdot b(x)}=\frac{a(x)}{b(x)},$$

$$\frac{a(x)}{b(x)}+\frac{c(x)}{d(x)}=\frac{a(x)\cdot d(x)+b(x)\cdot c(x)}{b(x)\cdot d(x)},$$

$$\frac{a(x)}{b(x)}\cdot\frac{c(x)}{d(x)}=\frac{a(x)\cdot c(x)}{b(x)\cdot d(x)}.$$

В связи с интегрированием отношений многочленов важную роль играет представление их в виде суммы некоторого многочлена из $P[x]$ и так называемых *простейших дробей*, т.е. выражений вида $\frac{g(x)}{p^n(x)}$, где $p(x)$ — неприводимый над полем P многочлен, а степень числителя $g(x)$ меньше степени $p(x)$. Докажем, что такое представление всегда возможно и даже единственно.

Теорема 2.9. *Всякое отношение двух многочленов* $\frac{f(x)}{h(x)}$ *представимо в виде суммы некоторого многочлена и некоторых простейших дробей, причем такое представление единственно.*

Доказательство. 1. Разделим числитель данного отношения на знаменатель с остатком: $f(x) = h(x) \cdot q(x) + r(x)$, где либо $r(x) = 0$, либо степень $r(x)$ меньше степени многочлена $h(x)$. Если $r(x) = 0$, то получаем $\frac{f(x)}{h(x)}=q(x)$, что и требовалось. Во втором случае $\frac{f(x)}{h(x)}=q(x)+\frac{r(x)}{h(x)}$ и задача сводится к рассмотрению отношения $\frac{r(x)}{h(x)}$, где степень многочлена в числителе меньше степени многочлена в знаменателе. Из однозначности деления с остатком вытекает, что многочлен $q(x)$ и отношение $\frac{r(x)}{h(x)}$ определяются однозначно.

2. Для отношения $\frac{r(x)}{h(x)}$ возможны два случая: либо знаменатель можно представить в виде произведения двух взаимно простых многочленов, либо знаменатель представляет собой степень неприводимого многочлена. Рассмотрим оба случая.

2.1. Пусть знаменатель можно разложить на взаимно простые множители: $h(x) = h_1(x) \cdot h_2(x)$, где степени сомножителей меньше степени многочлена $h(x)$ и НОД$(h_1(x), h_2(x)) = 1$.

Существуют многочлены $u(x)$ и $v(x)$, такие что $h_1(x) \cdot u(x) + h_2(x) \cdot v(x) = 1$. Умножив это равенство на $r(x)$, получим $r(x) \cdot h_1(x) \cdot u(x) + r(x) \cdot h_2(x) \cdot v(x) = r(x)$. Подставляя в числитель дроби, будем иметь

$$\frac{r(x)}{h(x)} = \frac{r(x) \cdot h_1(x) \cdot u(x) + r(x) \cdot h_2(x) \cdot v(x)}{h_1(x) \cdot h_2(x)} = \frac{r(x) \cdot u(x)}{h_2(x)} + \frac{r(x) \cdot v(x)}{h_1(x)}.$$

Для каждого из слагаемых разделим числитель на знаменатель: $r(x) \cdot u(x) = h_2(x)\, q_2(x) + r_2(x)$, $r(x) \cdot v(x) = h_1(x)\, q_1(x) + r_1(x)$, где степени остатков $r_1(x)$, $r_2(x)$ меньше степеней делителей соответственно $h_1(x)$ и $h_2(x)$. Тогда получаем

$$\frac{f(x)}{h(x)} = q(x) + \frac{h_2(x) q_2(x) + r_2(x)}{h_2(x)} + \frac{h_1(x) q_1(x) + r_1(x)}{h_1(x)} =$$

$$= q(x) + q_2(x) + \frac{r_2(x)}{h_2(x)} + q_1(x) + \frac{r_1(x)}{h_1(x)}.$$

Из единственности представления $\frac{f(x)}{h(x)} = q(x) + \frac{r(x)}{h(x)}$ заключаем, что $q_2(x) + q_1(x) = 0$ и $\frac{f(x)}{h(x)} = q(x) + \frac{r_1(x)}{h_1(x)} + \frac{r_2(x)}{h_2(x)}$. Здесь для каждого отношения в числителе стоит многочлен меньшей степени, чем в знаменателе. Если какой-то из знаменателей $h_1(x)$, $h_2(x)$ снова нетривиальным образом раскладывается в произведение взаимно простых сомножителей, то повторим рассуждения. Через конечное число шагов получим дробные слагаемые, у которых знаменатели представляют собой степени неприводимых многочленов, т.е. приходим к рассмотрению второго случая.

2.2. Пусть в отношении $\frac{r(x)}{h(x)}$ знаменатель $h(x)$ представляет собой степень неприводимого многочлена: $h(x) = p^n(x)$. Напомним, что степень числителя меньше степени знаменателя. Сначала $r(x)$ разделим с остатком на $p^{n-1}(x)$, затем полученный остаток делим на $p^{n-2}(x) p^{n-2}(x)$ и т.д. Положив $r_0(x) = r(x)$, получаем:

$$r_0(x) = p^{n-1}(x) \cdot q_1(x) + r_1(x),$$

$$r_1(x) = p^{n-2}(x) \cdot q_2(x) + r_2(x),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2}(x) = p(x) \cdot q_{n-1}(x) + r_{n-1}(x).$$

Степени неполных частных, а также остатка $r_{n-1}(x)$, меньше степени $p(x)$ и

$$\frac{r(x)}{h(x)}=\frac{r_0(x)}{p^n(x)}=\frac{p^{n-1}(x)\cdot q_1(x)+r_1(x)}{p^n(x)}=$$
$$=\frac{q_1(x)}{p(x)}+\frac{r_1(x)}{p^n(x)}=\frac{q_1(x)}{p(x)}+\frac{p^{n-2}(x)\cdot q_2(x)+r_2(x)}{p^n(x)}=$$
$$=\frac{q_1(x)}{p(x)}+\frac{q_2(x)}{p^2(x)}+\frac{r_2(x)}{p^n(x)}=\ldots=$$
$$=\frac{q_1(x)}{p(x)}+\frac{q_2(x)}{p^2(x)}+\ldots+\frac{q_{n-1}(x)}{p^{n-1}(x)}+\frac{r_{n-1}(x)}{p^n(x)}.$$

Обозначим $q_n(x)=r_{n-1}(x)$. В итоге получаем

$$\frac{f(x)}{h(x)}=q(x)+\frac{q_1(x)}{p(x)}+\frac{q_2(x)}{p^2(x)}+\ldots+\frac{q_{n-1}(x)}{p^{n-1}(x)}+\frac{q_n(x)}{p^n(x)}.$$

Замечаем, что однозначность представления вытекает из однозначности делений с остатком. Теорема доказана.

Пример 2.7

Представим в виде суммы простейших дробей отношение

$$\frac{f(x)}{h(x)}=\frac{2x^2+2x+37}{x^5-x^3-4x^2-3x-2}.$$

Решение. Способ 1. Сначала для знаменателя запускаем алгоритм отделения кратных множителей (см. пример предыдущего подпараграфа) и находим, что

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

Таким образом,

$$\frac{f(x)}{h(x)}=\frac{2x^2+2x+37}{(x-2)(x^2+x+1)^2}.$$

В нашем случае $h(x)=h_1(x)\cdot h_2(x)$, где $h_1(x)=x-2$, $h_2(x)=(x^2+x+1)^2=x^4+2x^3+3x^2+2x+1$. Находим НОД$(h_1(x), h_2(x))$. Уже деление $h_2(x)$ на $h_1(x)$ дает $h_2(x)=h_1(x)\cdot(x^3+4x^2+11x+24)+49$ (проверьте!). Отсюда получаем НОД$(h_1(x), h_2(x))=49$. Линейная форма наибольшего общего делителя имеет вид

$$49=h_2(x)-h_1(x)\cdot(x^3+4x^2+11x+24).$$

Умножив это равенство на $f(x)$, получим

$$49f(x)=f(x)\cdot h_2(x)-f(x)\cdot h_1(x)\cdot(x^3+4x^2+11x+24),$$

отсюда

$$\frac{f(x)}{h(x)}=\frac{1}{49}\frac{f(x)\cdot h_2(x)-f(x)\cdot h_1(x)\cdot(x^3+4x^2+11x+24)}{h_1(x)\cdot h_2(x)}=$$

$$=\frac{1}{49}\left(\frac{f(x)}{h_1(x)}-\frac{f(x)\cdot(x^3+4x^2+11x+24)}{h_2(x)}\right);$$

$$\frac{f(x)}{h_1(x)}=\frac{2x^2+2x+37}{x-2}=\frac{(x-2)(2x+6)+49}{x-2}=2x+6+\frac{49}{x-2};$$

$$\frac{f(x)\cdot(x^3+4x^2+11x+24)}{h_2(x)}=\frac{(2x^2+2x+37)\cdot(x^3+4x^2+11x+24)}{(x^2+x+1)^2}=$$

$$=\frac{2x^5+10x^4+67x^3+218x^2+455x+888}{x^4+2x^3+3x^2+2x+1}=$$

$$=\frac{(x^4+2x^3+3x^2+2x+1)(2x+6)+49x^3+196x^2+441x+882}{x^4+2x^3+3x^2+2x+1}=$$

$$=2x+6+49\frac{x^3+4x^2+9x+18}{(x^2+x+1)^2}.$$

Представим последнюю дробь в виде суммы простейших дробей:

$$\begin{array}{l} x^3+4x^2+9x+18 \\ \underline{x^3+x^2+x} \\ 3x^2+8x+18 \\ \underline{3x^2+3x+3} \\ 5x+15 \end{array} \quad \Big| \; \underline{x^2+x+1} \\ x+3$$

Следовательно, $x^3+4x^2+9x+18=(x^2+x+1)(x+3)+5x+15$ и

$$\frac{x^3+4x^2+9x+18}{(x^2+x+1)^2}=\frac{(x^2+x+1)(x+3)+5x+15}{(x^2+x+1)^2}=$$

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

Окончательно получаем

$$\frac{f(x)}{h(x)}=\frac{1}{49}\left(\frac{f(x)}{h_1(x)}-\frac{f(x)\cdot(x^3+4x^2+11x+24}{h_2(x)}\right)=$$

$$=\frac{1}{49}\left\{2x+6+\frac{49}{x-2}-\left[2x+6+49\left(\frac{x+3}{x^2+x+1}+5\frac{x+3}{(x^2+x+1)^2}\right)\right]\right\}=$$

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

Способ 2 (методом неопределенных коэффициентов). Записываем ожидаемый ответ с неопределенными коэффициентами:

$$\frac{f(x)}{h(x)}=\frac{2x^2+2x+37}{(x-2)(x^2+x+1)^2}=\frac{A}{x-2}+\frac{Bx+C}{x^2+x+1}+\frac{Dx+E}{(x^2+x+1)^2}=$$

$$= \frac{A(x^2+x+1)^2 + (Bx+C)(x-2)(x^2+x+1) + (Dx+E)(x-2)}{(x-2)(x^2+x+1)^2}.$$

Отсюда

$$2x^2 + 2x + 37 = (A+B)x^4 + (2A - B + C)x^3 + (3A - B - C + D)x^2 +$$

$$+ (2A - 2B - C - 2D + E)x + (A - 2C - 2E).$$

Приравнивая соответствующие коэффициенты, получаем систему линейных уравнений, решая которую, находим $A = 1$, $B = -1$, $C = -3$, $D = -5$, $E = -15$.

2.3.7*. Поле отношений кольца многочленов

До сих пор мы оперировали с отношениями многочленов на базе школьных навыков работы с ними по примеру действий с обыкновенными дробями, не задумываясь над законностью этих операций. Дадим математическое обоснование этим действиям.

Пусть дана произвольная область целостности K. В частности, K может быть как кольцом целых чисел, так и кольцом многочленов $P[x]$ над полем P. Наша задача — построить поле отношений области целостности K. В случае $K = \mathbb{Z}$ полем отношений будет поле рациональных чисел $\mathbb{Q}$, а в случае $K = P[x]$ мы получим поле отношений кольца многочленов $P[x]$ над полем P.

Рассмотрим множество всех упорядоченных пар вида (a, b), где $a, b \in K$ и вторая компонента пары $b \neq 0$. Обозначим $F_0 = \{(a, b) \mid a, b \in K, b \neq 0\}$. В случае $K = \mathbb{Z}$ это будут пары типа $(2, 3)$, «моделирующие» дробь $\frac{2}{3}$, а в случае $K = P[x]$ — пары многочленов типа $(f(x), h(x))$, где $f(x), h(x) \in P[x]$, «моделирующие» отношение $\frac{f(x)}{h(x)}$. Поскольку, например, $\frac{2}{3} = \frac{4}{6} = \frac{6}{9} = \ldots$, то одно и то же рациональное число «моделируется» упорядоченной парой неоднозначно. Так как для дробей имеет место равенство $\frac{a}{b} = \frac{c}{d}$ тогда и только тогда, когда $ad = bc$, то в случае произвольной области целостности K для любых элементов $a, b, c, d \in K$, где $b \neq 0$ и $d \neq 0$, определим $(a, b) \sim (c, d)$ тогда и только тогда, когда $ad = bc$.

Докажем, что отношение $\sim$ является отношением эквивалентности на множестве пар F_0. Рефлексивность и симметрич-

ность очевидны. Докажем транзитивность. Пусть для пар (a, b), (c, d), $(m, n) \in F_0$ имеем $(a, b) \sim (c, d)$ и $(c, d) \sim (m, n)$. Тогда

$$\left.\begin{array}{l}(a,b)\sim(c,d)\Rightarrow ad=bc\Rightarrow adn=bcn\\(c,d)\sim(m,n)\Rightarrow cn=dm\Rightarrow bcn=bdm\end{array}\right|\Rightarrow adn=bdm\Rightarrow$$
$$\Rightarrow an=bm\Rightarrow(a,b)\sim(m,n).$$

Здесь мы использовали то, что $d \neq 0$. По отношению эквивалентности $\sim$ множество всех пар F_0 распадается на классы эквивалентных пар. Класс пар, эквивалентных упорядоченной паре (a, b), обозначим $\overline{(a,b)}$. Множество всех классов обозначим через F.

Определим на F операции сложения и умножения классов эквивалентных пар, положив

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(ad+bc,bd)},\ \overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac,bd)}.$$

Заметим, что в области целостности K из того, что $b \neq 0$, $d \neq 0$, следует $bd \neq 0$, так что результаты сложения и умножения принадлежат F.

Докажем независимость суммы классов от выбора пар — представителей классов (аналогично для умножения классов). Пусть $\overline{(a,b)}=\overline{(a_1,b_1)}$ и $\overline{(c,d)}=\overline{(c_1,d_1)}$, докажем, что $\overline{(a,b)}+$ $+\overline{(c,d)}=\overline{(a_1,b_1)}+\overline{(c_1,d_1)}$. Имеем:

$$\overline{(a,b)}=\overline{(a_1,b_1)}\Rightarrow ab_1=ba_1,$$

$$\overline{(c,d)}=\overline{(c_1,d_1)}\Rightarrow cd_1=dc_1,$$

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(a_1,b_1)}+\overline{(c_1,d_1)}\ \Leftrightarrow$$

$$\Leftrightarrow\overline{(ad+bc,bd)}=\overline{(a_1d_1+b_1c_1,b_1d_1)}\Leftrightarrow$$

$$\Leftrightarrow(ad+bc)b_1d_1=bd(a_1d_1+b_1c_1).$$

Но, как легко видеть, из равенств $ab_1 = ba_1$ и $cd_1 = dc_1$ следует равенство $(ad + bc)b_1d_1 = bd(a_1d_1 + b_1c_1)$. Это и доказывает утверждение.

Итак, сложение и умножение классов эквивалентных пар являются бинарными операциями на множестве F. Пользуясь свойствами сложения и умножения элементов области целостности K, легко доказать, что обе операции на F ассоциативны, коммутативны и умножение дистрибутивно относительно сложения. Нулем будет класс $\overline{(0,1)}$, а единицей — класс $\overline{(1,1)}$,

где 1 — единица в K. Легко проверить, что $-\overline{(a,b)} = \overline{(-a,b)}$ и если $\overline{(a,b)} \neq \overline{(0,1)}$, то $(\overline{(a,b)})^{-1} = \overline{(b,a)}$. Следовательно, система $\langle F, +, \cdot \rangle$ является полем.

Введем привычные обозначения и класс $\overline{(a,b)}$ будем записывать в виде $\frac{a}{b}$, называя его *дробью* или *отношением*. При этом a называется *числителем* дроби, а b — ее *знаменателем*. В этих обозначениях поле F называется *полем отношений области целостности* K. Это поле содержит K в виде отношений (или дробей) вида $\frac{a}{1}$, когда a пробегает все множество K. Строго говоря, здесь надо говорить об изоморфном вложении K в F, но оставим эти тонкости до следующего семестра, где подробно будет рассмотрена теория делимости в произвольной области целостности (см. работу [8]). В частности, если $K = \mathbb{Z}$, то $F = Q = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$, а если $K = P[x]$, то получаем поле отношений $F = \left\{ \frac{f(x)}{h(x)} \mid f(x), h(x) \in P[x], h(x) \neq 0 \right\}$ кольца многочленов $P[x]$. Используя принятые обозначения и условие равенства классов эквивалентных пар, получаем условие равенства дробей:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow \overline{(a,b)} = \overline{(c,d)} \Leftrightarrow (a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Правила сложения и умножения классов эквивалентных пар превращаются в привычные правила действий с дробями:

$$\frac{a}{b} + \frac{c}{d} = \overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)} = \frac{ad+bc}{bd};$$

$$\frac{a}{b} \cdot \frac{c}{d} = \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)} = \frac{ac}{bd}.$$

Основное свойство дроби:

$$\frac{ac}{bc} = \overline{(ac,bc)} = \overline{(a,b)} = \frac{a}{b}.$$

Таким образом, мы обосновали действия с отношениями многочленов, которые ранее использовали на базе школьных знаний.

Контрольные вопросы

1. Над каким полем неприводимы многочлены:
а) $2x^2 + x - 6$;
б) $3x^2 - 5x + 5$;
в) $x^2 + 6x + 7$;
г) $2x^2 - 11x + 9$;
д) $x^4 - x^2 - 2x - 1$?
2. Если многочлен $p(x)$ неприводим над полем $\mathbb{Q}$, то будут ли неприводимыми над этим полем многочдены $3p(x)$, $xp(x)$, $(p(x))^2$?
3. Какова связь между НОД и НОК двух данных многочленов?
4. В каком случае алгоритм отделения кратных множителей приводит к разложению данного многочлена в произведение неприводимых множителей?
5. Будут ли простейшими дроби $\frac{3x+2}{2x^2-3}$, $\frac{3x^2-2}{2x+3}$, $\frac{2x+3}{3x+2}$?

Задачи

1. Приведите примеры и контрпримеры неприводимых над данным полем многочленов.
2. Найдите наибольший общий делитель и наименьшее общее кратное пар многочленов:
а) $f(x) = (x - 1)^5(x^2 + 1)^2(x^4 + x^2 + 1)^3$, $h(x) = (x^2 - 1)^2(x^2 + 2x + 1)(x^4 - 1)$;
б) $f(x) = (x - \sqrt{3})^2(3x + \sqrt{2})^3$, $h(x) = (2x + 1)^2(x^2 + 1)(x^2 - 3)$;
в) $f(x) = (2x^2 - 3x + 9)(x - 3)^3$, $h(x) = (3x - 4)^2(2x - 1)$;
г) $f(x) = (x - 3)^3(x - 1 + i)^3$, $h(x) = (x - 1 - i\sqrt{2})^2 x(x - 1 + i)^2$.
3. Найдите наибольший общий делитель многочлена и его производной:
а) $(x - 2)^3(x + 1)^2(x - 3)$;
б) $(x^4 - 1)(1 - x)^3(x^2 - 1)^2(x - 1)^3$;
в) $x^4 - 8x^3 + 12x^2 - 6x + 2$.
4. Отделите кратные множители многочленов:
а) $x^5 + 5x^4 - 40x^2 - 80x - 48$;
б) $x^5 - 5x^4 - 5x^3 + 45x^2 - 108$;
в) $x^6 + 6x^5 + 9x^4 - 8x^3 - 24x^2 + 16$;
г) $x^6 + 4x^5 + 5x^4 - 5x^2 - 4x - 1$;
д) $x^6 + 4x^5 + 4x^4 - 6x^3 - 12x^2 + 9$.
5. Докажите, что многочлен $x^n - 1$ не имеет кратных корней.
6. Отделите кратные множители многочленов и найдите их корни:
а) $x^5 - 5x^4 - 5x^3 + 25x^2 + 40x + 16$;
б) $x^5 + 5x^4 + 3x^3 - 13x^2 - 8x + 12$;
в) $2x^6 + 6x^5 + 6x^4 + x^3 - 3x^2 - 3x - 1$;
г) $x^5 - 6ix^4 - 14x^3 + 16ix^2 + 9x - 2i$;
д) $x^7 + 3x^6 - 5x^5 - 7x^4 + 15x^3 - 19x^2 + 21x - 9$.

7. Представьте в виде суммы простейших дробей:

а) $\dfrac{2x^2-3x+9}{(x-3)^5}$;

б) $\dfrac{x^4+3x^3-11x^2-16x+24}{(x+4)^6}$;

в) $\dfrac{5x^2-14x-23}{(x-1)^3(x-3)^2(x-4)}$;

г) $\dfrac{2x-3}{x^2(x^2-x+1)^2(x-1)}$.

Глава 3
МНОГОЧЛЕНЫ НАД ЧИСЛОВЫМИ КОЛЬЦАМИ И ПОЛЯМИ

Напомним, что *числовым полем* называется всякое подполе поля комплексных чисел. Таким образом, «самым большим» числовым полем является поле комплексных чисел $\mathbb{C}$, а «самым маленьким» — поле рациональных чисел $\mathbb{Q}$. Помимо колец многочленов над числовыми полями $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$ мы рассмотрим также кольцо многочленов $\mathbb{Z}[x]$ над кольцом целых чисел $\mathbb{Z}$. В первую очередь мы будем интересоваться видом неприводимых многочленов в этих кольцах многочленов, чтобы установить, как выглядит разложение произвольного многочлена в произведение неприводимых множителей. Кроме того, будут рассмотрены вопросы, связанные с нахождением корней многочленов.

3.1. Многочлены над полем комплексных чисел

3.1.1. Основная теорема алгебры. Неприводимые многочлены над полем комплексных чисел

Каковы неприводимые многочлены над полями $\mathbb{C}$ и $\mathbb{R}$? Ключевой в этом вопросе является следующая теорема, которая носит название *основной теоремы алгебры* (теперь ее называют более скромно: основной теоремой алгебры комплексных чисел).

Теорема 3.1. *Всякий многочлен с комплексными коэффициентами степени $n \geq 1$ имеет по крайней мере один комплексный корень.*

Доказательство этой теоремы будет дано в подпараграфе 4.2.4. Здесь же приведем основные следствия из нее. По традиции комплексную переменную будем обозначать буквой z, оставляя x и y за обозначениями действительной и мнимой части в записи $z = x + yi$.

Теорема 3.2. *Неприводимыми над полем* $\mathbb{C}$ *являются многочлены первой степени и только они.*

Доказательство. Ясно, что всякий многочлен первой степени неприводим над полем $\mathbb{C}$. Пусть $f(z) \in \mathbb{C}[z]$ и степень $f(z)$ больше 1. По теореме 3.1 $f(z)$ имеет корень $c \in \mathbb{C}$, а по следствию из теоремы Безу $f(z) \vdots (z - c)$, т.е. $f(z) = (z - c) \cdot q(z)$ при некотором $q(z) \in \mathbb{C}[z]$. Поскольку степень $f(z)$ больше 1, то степень $q(z)$ больше либо равна 1. Следовательно, многочлен $f(z)$ приводим. Теорема доказана.

Следствие 1. Всякий многочлен $f(z) \in \mathbb{C}[z]$ степени $n \geq 1$ представим в виде $f(z) = a_n(z - c_1)(z - c_2)\cdots(z - c_n)$.

Доказательство. Многочлен $f(z)$ представим в виде произведения неприводимых множителей, которые по теореме 3.2 имеют степень 1. Следовательно,

$$f(z) = (k_1 z + m_1)(k_2 z + m_2)\cdots(k_n z + m_n) =$$

$$= k_1 k_2 \cdots k_n \left(z - \frac{m_1}{k_1}\right)\left(z - \frac{m_2}{k_2}\right)\cdots\left(z - \frac{m_n}{k_n}\right) = a_n(z - c_1)(z - c_2)\cdots(z - c_n),$$

где $a_n = k_1 k_2 \cdots k_n$, $c_i = \dfrac{m_i}{k_i}$, $i = 1, 2, \ldots, n$. Следствие доказано.

Следствие 2. Всякий многочлен $f(z)$ с комплексными коэффициентами представим в виде

$$f(z) = a_n(z - c_1)^{m_1}(z - c_2)^{m_2}\cdots(z - c_k)^{m_k},$$

где корни $c_1, c_2, \ldots, c_k$ различны и $m_1 + m_2 + \ldots + m_k = n$.

Следствие 3. Многочлен с комплексными коэффициентами степени n имеет n комплексных корней, если каждый корень считать столько раз, какова его кратность.

Пример 3.1

Найдите приведенный многочлен наименьшей степени, имеющий двукратные корни 2 и $1 + i$.

Решение. Искомым будет многочлен

$$f(z) = (z - 2)^2[z - (1+i)]^2 = z^4 - 2(3 + i)z^3 + 2(4 + 5i)\, z^2 - 8(1 + 2i)\, z + 8i.$$

3.1.2. Формулы Виета

Пусть $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = a_n(z - c_1)(z - c_2)\cdots$ $\cdots(z - c_n)$.

Используя это равенство, выведем формулы, связывающие корни данного многочлена с его коэффициентами. Они называются *формулами Виета* по имени французского математика Франсуа Виета (1540—1603).

Рассмотрим сначала случай $n = 2$. Имеем

$$f(z) = a_2z^2 + a_1z + a_0 = a_2(z - c_1)(z - c_2) =$$

$$= a_2z^2 + a_2(-c_1 - c_2)z + a_2c_1c_2.$$

Приравнивая соответствующие коэффициенты, получаем $a_1 = a_2(-c_1 - c_2)$, $a_0 = a_2c_1c_2$. Отсюда выводим *формулы Виета для квадратного трехчлена*:

$$c_1 + c_2 = -\frac{a_1}{a_2},\ c_1c_2 = \frac{a_0}{a_2}.$$

Если данный многочлен приведенный, т.е. старший коэффициент равен 1, то $f(z) = z^2 + pz + q$ и *формулы Виета для приведенного квадратного трехчлена* имеют простой вид: $c_1 + c_2 = -p$, $c_1c_2 = q$.

Словами: *сумма корней приведенного квадратного трехчлена равна второму коэффициенту, взятому с противоположным знаком, а произведение корней равно свободному члену.*

Теперь рассмотрим многочлен третьей степени:

$$f(z) = a_3z^3 + a_2z^2 + a_1z + a_0 = a_3(z - c_1)(z - c_2)(z - c_3) =$$

$$= a_3(z^2 + (-c_1 - c_2)z + c_1c_2)(z - c_3) =$$

$$= a_3z^3 + a_3(-c_1 - c_2 - c_3)z^2 + a_3(c_1c_2 + c_1c_3 + c_2c_3)z - a_3c_1c_2c_3.$$

Приравнивая соответствующие коэффициенты, получаем $a_2 = a_3(-c_1 - c_2 - c_3)$, $a_1 = a_3(c_1c_2 + c_1c_3 + c_2c_3)$, $a_0 = -a_3c_1c_2c_3$. Отсюда получаем *формулы Виета для многочлена 3-й степени*:

$$c_1 + c_2 + c_3 = -\frac{a_2}{a_3},$$

$$c_1c_2 + c_1c_3 + c_2c_3 = \frac{a_1}{a_3},$$

$$c_1c_2c_3 = -\frac{a_0}{a_3}.$$

Аналогично в общем случае, приравнивая соответствующие коэффициенты, получаем *формулы Виета для многочлена n-й степени*:

$$c_1 + c_2 + \ldots + c_n = -\frac{a_{n-1}}{a_n},$$

$$c_1c_2 + c_1c_3 + \ldots + c_{n-1}c_n = \frac{a_{n-2}}{a_n}, \ldots,$$

$$c_1c_2 \cdots c_n = (-1)^n \frac{a_0}{a_n}.$$

Контрольные вопросы

1. Что говорит основная теорема алгебры о многочленах над полем комплексных чисел?
2. Как выглядит разложение многочлена с комплексными коэффициентами в произведение неприводимых над полем комплексных чисел сомножителей?
3. В чем смысл формул Виета?
4. Как формулируются формулы Виета для (приведенного) квадратного трехчлена, для многочленов степени 3 и 4?
5. Верно ли, что сумма и произведение всех корней данного многочлена над некоторым числовым полем принадлежат этому полю, даже если не все его корни принадлежат данному полю?

Задачи

1. Разложите многочлены в произведение неприводимых множителей над полем комплексных чисел: а) $x^2 + 4$; б) $x^4 + 4$; в) $x^6 - 1$; г) $x^8 - 8$; д) $x^3 + x^2 - 2$; е) $x^4 + x^2 + 1$.
2. Составьте приведенный многочлен наименьшей степени, имеющий данный набор корней: а) $x_1 = x_2 = 2$, $x_3 = i$, $x_4 = 1 - i$; б) $x_{1,2} = 1 \pm i$, $x_{3,4} = 1 \pm \sqrt{2}$; в) $x_{1,2} = i$, $x_{3,4} = -i$; г) $x_{1,2} = 2$, $x_{3,4} = 1 - 3i$; д) $x_{1,2} = \pm c$, $x_{3,4} = \pm\frac{1}{c}$, $c \in \mathbb{C}$; е) $x_1 = c$, $x_2 = \frac{1}{c}$, $x_3 = 1 - c$, $x_4 = \frac{1}{1-c}$, $c \in \mathbb{C}$.
3. Пользуясь формулами Виета, составьте многочлен, имеющий данные корни: а) $x_1 = x_2 = 2$, $x_{3,4} = 1 - i$; б) $x_{1,2} = 1 \pm i$, $x_{3,4} = -i$; в) $x_{1,2} = 1 \pm \sqrt{2}$, $x_3 = i$.
4. Дан многочлен $5x^3 - 3x^3 + 7x - \lambda$. Найдите λ, если известно, что сумма двух корней данного многочлена равна -1.
5. Известно, что отличные от нуля числа c_1, c_2, ..., c_n являются корнями многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Составьте

многочлен, корнями которого являются: а) числа, противоположные данным; б) числа, обратные данным.

6. Найдите многочлен третьей степени со старшим коэффициентом 3, корни которого x_1, x_2, x_3 удовлетворяют условиям $\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}=3$, $\frac{1}{x_1x_2}+\frac{1}{x_1x_3}+\frac{1}{x_2x_3}=9$, $\frac{1}{x_1x_2x_3}=27$.

7. Найдите соотношение, связывающее коэффициенты уравнения $x^4 + ax^3 + bx^2 + cx + d = 0$, если известно, что корни уравнения связаны соотношением: а) $x_1 + x_2 = x_3 + x_4$; б) $x_1 \cdot x_2 = x_3 \cdot x_4$.

3.2. Многочлены над полем действительных чисел

3.2.1. Неприводимые многочлены над полем действительных чисел

Выясним вид неприводимого над полем действительных чисел многочлена. Предварительно докажем теорему, которая имеет и самостоятельное значение.

Теорема 3.3. *Если комплексное число α является корнем многочлена $f(x)$ с действительными коэффициентами, то сопряженное число $\overline{\alpha}$ также является корнем этого многочлена.*

Доказательство. Напомним, что если $\alpha = a + bi$, то сопряженное число $\overline{\alpha} = a - bi$. Легко видеть, что для любого действительного числа a имеем $\overline{a} = a$. Для любых $\alpha, \beta \in \mathbb{C}$ $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$ и $\overline{\alpha\cdot\beta}=\overline{\alpha}\cdot\overline{\beta}$. Пусть $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{R}[x]$ и комплексное число α является корнем этого многочлена. Тогда $f(\alpha) = 0$ и, используя свойства сопряженных комплексных чисел, последовательно получаем:

$$f(\overline{\alpha}) = a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \ldots + a_1\overline{\alpha} + a_0 = \overline{a}_n\overline{\alpha}^n + \overline{a}_{n-1}\overline{\alpha}^{n-1} + \ldots + \overline{a}_1\overline{\alpha} + \overline{a}_0 =$$
$$= \overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \ldots + \overline{a_1\alpha} + \overline{a_0} =$$
$$= \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0} = \overline{0} = 0.$$

Следовательно, $\overline{\alpha}$ является корнем многочлена $f(x)$. Теорема доказана.

Напомним, что комплексное число, не являющееся действительным, называется *мнимым*.

Следствие 1. Мнимые корни многочлена с действительными коэффициентами попарно сопряжены, а значит, их количество четно.

Следствие 2. Многочлен с действительными коэффициентами нечетной степени имеет по крайней мере один действительный корень.

Доказательство. Пусть степень данного многочлена $f(x) \in \mathbb{R}[x]$ равна $n \geq 1$. Тогда он имеет n комплексных корней, и если предположить, что все они мнимые, то по следствию 1 число n должно быть четным, что, по условию, не так. Следовательно, среди корней есть действительный корень.

Теорема 3.4. *Неприводимыми над полем действительных чисел являются только многочлены первой степени и многочлены второй степени с отрицательными дискриминантами.*

Доказательство. Очевидно, что всякий многочлен первой степени из $\mathbb{R}[x]$ неприводим над $\mathbb{R}$. Многочлен второй степени из $\mathbb{R}[x]$ неприводим над полем $\mathbb{R} \Leftrightarrow$ он не представим в виде произведения двух многочленов первой степени с действительными коэффициентами $\Leftrightarrow$ многочлен не имеет действительных корней $\Leftrightarrow$ дискриминант многочлена отрицательный.

Докажем, что многочлен $f(x) \in \mathbb{R}[x]$ степени $n > 2$ приводим над полем $\mathbb{R}$. По основной теореме алгебры $f(x)$ имеет хотя бы один комплексный корень c. Тогда $f(x) \vdots (x - c)$. Если $c \in \mathbb{R}$, то $f(x) = (x - c)q(x)$, где $q(x) \in \mathbb{R}[x]$, откуда следует приводимость $f(x)$ над полем $\mathbb{R}$.

Если же число c мнимое, то сопряженное число $\overline{c}$ также является корнем данного многочлена и $f(x) \vdots (x - \overline{c})$, а так как $x - c$ и $x - \overline{c}$ взаимно просты, то $f(x) \vdots (x - c)(x - \overline{c})$. Но $h(x) = (x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c \cdot \overline{c}$ — многочлен с действительными коэффициентами, имеющий степень 2, и $f(x) \vdots h(x)$. Следовательно, $f(x) = h(x) \cdot q_1(x)$ при некотором $q_1(x) \in \mathbb{R}[x]$. Поскольку степень $f(x)$ больше 2, то $q_1(x)$ — многочлен степени ≥ 1. Отсюда следует, что многочлен $f(x)$ приводим над полем $\mathbb{R}$. Теорема доказана.

Следствие. Всякий многочлен $f(x) \in \mathbb{R}[x]$ степени $n \geq 1$ представим в виде

$$f(x) = a_n(x - c_1)^{\alpha_1} \cdots (x - c_k)^{\alpha_k}(x^2 + p_1x + q_1)^{\beta_1} \cdots (x^2 + p_mx + q_m)^{\beta_m},$$

где $\alpha_1 + \alpha_2 + \ldots + \alpha_k + 2\beta_1 + 2\beta_2 + \ldots + 2\beta_m = n$ и дискриминант каждого множителя второй степени отрицателен.

Пример 3.2

Составьте приведенный многочлен с действительными коэффициентами наименьшей степени, имеющий корни 2 и $1 + i$.

Решение. Поскольку комплексное число $1 + i$ является корнем искомого многочлена, то и сопряженное число $1 - i$ также должно быть его корнем. Следовательно, искомым будет многочлен $f(x) = (x - 2)[x - (1 + i)][x - (1 - i)] = x^3 - 4x^2 + 6x - 4$.

3.2.2. Границы действительных корней многочлена с действительными коэффициентами

Чтобы установить границы действительных корней многочлена с действительными коэффициентами, докажем вспомогательное утверждение.

***Лемма 3.1* (*о модуле старшего члена*).** *Пусть дан многочлен с действительными коэффициентами* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *степени* $n \geq 1$ *и* $A = \max\{|a_{n-1}|, \ldots, |a_1|, |a_0|\}$. *Для любого действительного числа* $k > 0$ *если* $|x| > 1 + k\dfrac{A}{|a_n|}$, *то*

$$|a_n x^n| > k|a_{n-1}x^{n-1} + \ldots + a_1 x + a_0|.$$

Доказательство. Используя условие, получаем

$$|a_{n-1}x^{n-1} + \ldots + a_1 x + a_0| \leq |a_{n-1}x^{n-1}| + \ldots + |a_1 x| + |a_0| =$$
$$= |a_{n-1}| \cdot |x|^{n-1} + \ldots + |a_1| \cdot |x| + |a_0| \leq A \cdot |x|^{n-1} + \ldots + A \cdot |x| + A =$$
$$= A(|x|^{n-1} + \ldots + |x| + 1) = A\frac{|x|^n - 1}{|x| - 1} = A\left(\frac{|x|^n}{|x| - 1} - \frac{1}{|x| - 1}\right).$$

Возьмем $|x| > 1$, тогда $\dfrac{1}{|x| - 1} > 0$ и $\dfrac{|x|^n}{|x| - 1} - \dfrac{1}{|x| - 1} < \dfrac{|x|^n}{|x| - 1}$. Следовательно,

$$|a_{n-1}x^{n-1} + \ldots + a_1 x + a_0| < A\frac{|x|^n}{|x| - 1}.$$

Поскольку $k > 0$, то

$$k|a_{n-1}x^{n-1} + \ldots + a_1 x + a_0| < kA\frac{|x|^n}{|x| - 1}.$$

Требуемое неравенство будет выполняться, если $kA\dfrac{|x|^n}{|x| - 1} < |a_n x^n|$. Отсюда находим условие на $|x|$:

$$kA\frac{|x|^n}{|x| - 1} < |a_n x^n| \Leftrightarrow kA\frac{|x|^n}{|x| - 1} < |a_n| \cdot |x|^n \Leftrightarrow |x| > 1 + k\frac{A}{|a_n|}.$$

Таким образом, при выполнении последнего условия на $|x|$ получим $|a_n x^n| > k|a_{n-1}x^{n-1} + \ldots + a_1 x + a_0|$. Лемма доказана.

Из доказанной леммы вытекает, что для достаточно больших $|x|$ модуль старшего члена многочлена во сколько угодно раз больше модуля суммы остальных членов этого многочлена.

Следствие 1. Для многочлена $f(x)$ с действительными коэффициентами при достаточно больших значениях $|x|$ знак значения многочлена совпадает со знаком значения его старшего члена.

Следствие 2 (о границах корней). Все действительные корни многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ с действительными коэффициентами принадлежат отрезку $\left[-1 - \frac{A}{|a_n|}; 1 + \frac{A}{|a_n|}\right]$, где $A = \max\{|a_{n-1}|, \ldots, |a_1|, |a_0|\}$.

Доказательство. Предположим противное, пусть действительное число x_0 является корнем многочлена $f(x)$ и не принадлежит указанному отрезку. Первое означает, что $f(x_0) = a_n x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0 = 0$, откуда $|a_n x_0^n| = |a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0|$. Второе означает, что $|x_0| > 1 + \frac{A}{|a_n|}$, откуда по лемме о модуле старшего члена (при $k = 1$) $|a_n x_0^n| > |a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0|$ — пришли к противоречию. Следствие доказано.

3.2.3. Отделение действительных корней многочлена методом Штурма

Рассмотрим алгоритм, позволяющий отделять один от другого действительные корни многочлена с действительными коэффициентами, т.е. находить непересекающиеся отрезки, содержащие все действительные корни по одному в каждом отрезке.

Пусть дан многочлен $f(x)$ с действительными коэффициентами. С помощью алгоритма отделения кратных множителей его можно представить в виде произведения многочленов, не имеющих кратных множителей. Следовательно, в вопросах нахождения корней многочлена можно ограничиться рассмотрением случая, когда данный многочлен $f(x)$ не имеет кратных множителей. Это означает, что НОД$(f(x), f'(x)) = 1$.

Обозначим $f_0(x) = f(x)$, $f_1(x) = f'(x)$. К многочленам $f_0(x)$ и $f_1(x)$ применим несколько измененный алгоритм Евклида — делитель будем делить на остаток, взятый с противоположным знаком:

$$f_0(x) = f_1(x) \cdot q_1(x) + r_1(x), f_2(x) = -r_1(x);$$

$$f_1(x) = f_2(x) \cdot q_2(x) + r_2(x), f_3(x) = -r_2(x);$$

.....

$$f_{n-2}(x) = f_{n-1}(x) \cdot q_{n-1}(x) + r_{n-1}(x), f_n(x) = -r_{n-1}(x);$$

$$f_{n-1}(x) = f_n(x) \cdot q_n(x) + 0, r_n(x) = 0.$$

Таким образом, получаем равенства

$$f_0(x) = f_1(x) \cdot q_1(x) - f_2(x),$$

$$f_1(x) = f_2(x) \cdot q_2(x) - f_3(x),$$

.....

$$f_{n-2}(x) = f_{n-1}(x) \cdot q_{n-1}(x) - f_n(x),$$

$$f_{n-1}(x) = f_n(x) \cdot q_n(x).$$

Здесь $-f_n(x)$ есть последний отличный от нуля остаток. По условию, НОД($f_0(x)$, $f_1(x)$) = 1. Следовательно, $f_n(x)$ есть многочлен нулевой степени, т.е. ненулевое действительное число. Построенная таким образом последовательность многочленов $f_0(x), f_1(x), ..., f_n(x)$ называется *стандартной системой многочленов Штурма*. Мы рассмотрим основные свойства этой системы и на базе выявленных свойств дадим общее определение *системы многочленов Штурма*. Из него будет ясно, что кроме этой системы многочленов возможны и другие системы многочленов Штурма.

1. Никакие два соседних многочлена системы многочленов Штурма $f_0(x), f_1(x), ..., f_n(x)$ не имеют общих корней.

Доказательство. Предположим противное, пусть действительное число c является общим корнем соседних многочленов $f_k(x)$ и $f_{k+1}(x)$, где $0 \le k < n$. Рассмотрим равенство, связывающее эти многочлены: $f_{k-1}(x) = f_k(x) \cdot q_k(x) - f_{k+1}(x)$. При $x = c$ получаем $f_{k-1}(c) = f_k(c) \cdot q_k(c) - f_{k+1}(c)$. По предположению, $f_k(c) = 0$ и $f_{k+1}(c) = 0$. Отсюда $f_{k-1}(c) = 0$. Следовательно, c является общим корнем соседних многочленов $f_{k-1}(x)$ и $f_k(x)$. Рассуждая дальше таким же образом, приходим к выводу о том, что c является общим корнем соседних многочленов $f_0(x) = f(x)$ и $f_1(x) = f'(x)$. Но тогда они имеют общий множитель $x - c$, что

противоречит условию взаимной простоты многочленов $f(x)$ и $f'(x)$. Свойство доказано.

2. Если c является корнем промежуточного многочлена $f_k(x)$, $0 < k < n$, то числа $f_{k-1}(c)$ и $f_{k+1}(c)$ имеют разные знаки.

Доказательство. Равенство $f_{k-1}(x) = f_k(x) \cdot q_k(x) - f_{k+1}(x)$ при $x = c$ приобретает вид $f_{k-1}(c) = -f_{k+1}(c)$, поскольку, по условию, $f_k(c) = 0$. Следовательно, числа $f_{k-1}(c)$ и $f_{k+1}(c)$ имеют разные знаки. Свойство доказано.

3. Если $x = c$ является корнем многочлена $f_0(x) = f(x)$, то существует промежуток $(c - \varepsilon; c + \varepsilon)$, при прохождении которого переменной x произведение $f_0(x) \cdot f_1(x)$ меняет знак с «минуса» на «плюс».

Доказательство. Напомним, что мы рассматриваем случай, когда многочлен $f(x)$ не имеет кратных множителей, а значит, взаимно прост со своей производной. Отсюда следует, что многочлены $f(x)$ и $f'(x)$ не имеют общих корней. По условию, $f(c) = 0$, а значит, $f'(c) \neq 0$. Многочлен — непрерывная функция, следовательно, существует промежуток $(c - \varepsilon; c + \varepsilon)$, на котором производная $f'(x)$ сохраняет свой знак, т.е. при возрастании x на этом промежутке функция $f'(x)$ либо все время положительна, либо все время отрицательна. Но тогда сама функция на этом промежутке либо все время возрастает, либо все время убывает. Рассмотрим оба случая.

А. Пусть на промежутке $(c - \varepsilon, c + \varepsilon)$ функция $f_1(x) = f'(x)$ положительна, а значит, $f(x)$ возрастает.

По условию $f(c) = 0$, значит, $f(x)$ на данном промежутке меняет свой знак с «минуса» на «плюс» (рис. 3.1):

x	$f_0(x)$	$f_1(x)$
$(c - \varepsilon; c)$	–	+
$(c; c + \varepsilon)$	+	+

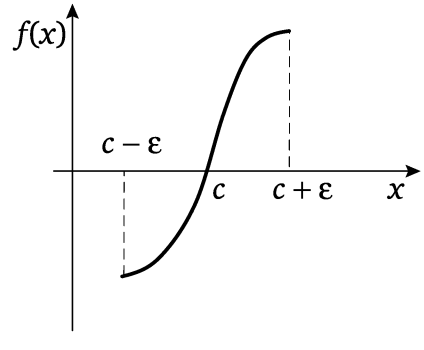

Рис. 3.1

Поскольку знак $f_1(x) = f'(x)$ положителен, а знак $f_0(x) = f(x)$ меняется с «минуса» на «плюс», то произведение $f_0(x) \cdot f_1(x) = f(x) \cdot f'(x)$ также меняет свой знак с «минуса» на «плюс».

Б. Пусть на промежутке $(c - \varepsilon; c + \varepsilon)$ функция $f_1(x) = f'(x)$ отрицательна, а значит, функция $f(x)$ убывает. По условию $f(c) = 0$, значит, $f(x)$ на данном промежутке меняет свой знак с «плюса» на «минус» (рис. 3.2):

x	$f_0(x)$	$f_1(x)$
$(c - \varepsilon; c)$	+	–
$(c; c + \varepsilon)$	–	–

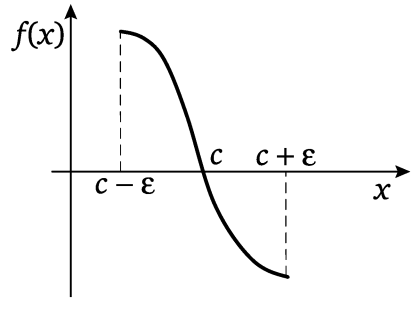

Рис. 3.2

Поскольку знак $f_1(x) = f'(x)$ отрицателен, а знак $f_0(x) = f(x)$ меняется с «плюса» на «минус», то произведение $f_0(x) \cdot f_1(x) = f(x) \cdot f'(x)$ меняет свой знак с «минуса» на «плюс». Свойство доказано.

4. Последний многочлен системы Штурма $f_n(x)$ не имеет действительных корней.

Доказательство. Выше уже отмечалось, что $f_n(x)$ есть многочлен нулевой степени, т.е. ненулевое действительное число. Но такой многочлен не имеет корней.

Определение 3.1. *Системой многочленов Штурма* для многочлена $f(x) \in \mathbb{R}[x]$ называется всякая последовательность многочленов $f_0(x), f_1(x), \ldots, f_n(x)$, обладающая сформулированными выше свойствами 1—4.

Из этого определения вытекает, что если любой из многочленов системы Штурма умножить на положительное число, то получим снова систему многочленов Штурма. Это часто используется при нахождении данной системы многочленов.

Пример 3.3

Найдем систему многочленов Штурма для многочлена $f(x) = x^4 - x - 3$.

Решение. Полагаем $f_0(x) = f(x)$ и находим $f_1(x) = f'(x) = 4x^3 - 1$. Теперь нам предстоит делить (уголком) $f_0(x) = f(x)$ на $f_1(x) = f'(x)$. Чтобы избежать дробей, воспользуемся возможностью умножить любой многочлен Штурма на положительное число и $4f(x) = 4x^4 - 4x - 12$ будем делить на $4x^3 - 1$. В остатке получим $-3x - 12$ (проверьте!). Согласно алгоритму нужно взять $f_2(x) = -r_1(x) = 3x + 12$. Но мы, пользуясь возможностью умножать любой многочлен Штурма на положительное число, возьмем $f_2(x) = x + 4$. Теперь делим $f_1(x)$ на $f_2(x)$ с остатком (уголком) и получаем в остатке число -257 (проверьте!). Следовательно, можно взять $f_3(x) = 1$. Одновременно мы убеждаемся, что НОД$(f(x), f'(x)) = 1$, а значит, данный многочлен не имеет кратных множителей.

Ответ: $f_0(x) = x^4 - x - 3, f_1(x) = 4x^3 - 1, f_2(x) = x + 4, f_3(x) = 1$ — система многочленов Штурма для данного многочлена $f(x)$.

Введем ключевое понятие для определения количества корней многочлена с действительными коэффициентами на данном промежутке.

Определение 3.2. Пусть дана конечная последовательность действительных чисел $a_1, a_2, \ldots, a_k$. *Переменой знака* в данной последовательности называется пара либо рядом стоящих, либо разделенных нулями членов последовательности, имеющих разные знаки. Количество всех таких перемен знаков называется *числом перемен знаков* данной последовательности.

Например, в последовательности 1, 2, –3, 4, 0, 0, –5 перемены знаков образуют пары (2, –3), (–3, 4) и (4, –5), а число перемен знаков данной последовательности равно 3.

Определение 3.3. Пусть даны многочлен $f(x) \in \mathbb{R}[x]$ и его система многочленов Штурма $f_0(x), f_1(x), \ldots, f_n(x)$. Для любого действительного числа c определим *значение* $W(c)$ как число перемен знаков в последовательности $f_0(c), f_1(c), \ldots, f_n(c)$.

Например, для многочлена $f(x)$ из примера 3.3 при $x = c = 0$ имеем $f_0(0) = -3, f_1(0) = -1, f_2(0) = 4, f_3(x) = 1$. Следовательно, $W(0) = 1$, ибо в последовательности –3, –1, 4, 1 одна перемена знаков.

Заметим, что для вычисления $W(c)$ при данном c необязательно вычислять значения $f_0(c), f_1(c), f_2(c), f_3(c)$, достаточно определить знак каждого из этих чисел. Данные вычислений удобно заносить в таблицу знаков. Приведем пример такой таблицы. Вспомним, что для достаточно больших $|x|$ знак $f(x)$ совпадает со знаком старшего члена данного многочлена (см. следствие 1 из леммы о модуле старшего члена многочлена). При достаточно больших значениях $|x| = c$ в таблице вместо

значения $x = c$ пишем знак $+\infty$, а вместо значения $x = -c$ пишем знак $-\infty$. Вот как выглядит таблица знаков для данного многочлена $f(x)$.

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$W(x)$
$-\infty$	+	−	−	+	2
0	−	−	+	+	1
$+\infty$	+	+	+	+	0

Замечаем, что для достаточно больших $|x| = c$ на отрезках $[-c; 0]$ и $[0; c]$ происходит по одной потере перемен знаков: $W(-c) - W(0) = 2 - 1 = 1$ и $W(0) - W(c) = 1 - 0 = 1$. Как будет доказано ниже, это сигнализирует о том, что данный многочлен имеет один отрицательный и один положительный корень.

Теорема 3.5 (Штурма). *Пусть дан ненулевой многочлен $f(x)$ с действительными коэффициентами, не имеющий кратных множителей. Если действительные числа a и b, где $a < b$, не являются корнями данного многочлена, то число корней многочлена на отрезке $[a; b]$ равно $W(a) - W(b)$.*

Доказательство. Пусть $f_0(x), f_1(x), \ldots, f_n(x)$ — система многочленов Штурма для многочлена $f(x)$. Отрезок $[a; b]$ так разделим точками $a_0 = a, a_1, \ldots, a_m = b$, что ни одна из точек деления не является корнем ни одного из многочленов данной системы многочленов Штурма и на каждом отрезке $[a_i; a_{i+1}]$, где $i = 0, 1, \ldots, m - 1$, содержится не более одного корня многочленов этой системы. Рассмотрим возможные случаи расположения x относительно данных отрезков.

1. $x \in [a_i; a_{i+1}]$, и этот отрезок не содержит корней многочленов системы Штурма. Поскольку многочлен — непрерывная функция и на данном отрезке график функции для каждого многочлена системы Штурма не пересекает ось абсцисс, то на этом отрезке график каждого многочлена либо целиком выше оси, либо ниже ее. Следовательно, на рассматриваемом отрезке в последовательности $f_0(x), f_1(x), \ldots, f_n(x)$ не происходит перемен знаков, а значит, значение $W(x)$ остается неизменным.

2. $x \in [a_i; a_{i+1}]$, причем этот отрезок содержит корень c промежуточного многочлена системы Штурма $f_k(x)$, $0 < k < n$. По первому свойству многочленов системы Штурма $f_{k-1}(c) \neq 0$ и $f_{k+1}(c) \neq 0$, а по второму свойству $f_{k-1}(c)$ и $f_{k+1}(c)$ имеют разные знаки. Для определенности положим $f_{k-1}(c) < 0$, тогда $f_{k+1}(c) > 0$. Рассмотрим таблицу знаков.

x	...	$f_{k-1}(x)$	$f_k(x)$	$f_{k+1}(x)$	...
$a_i \le x < c$		$-$		$+$	
$c < x \le a_{i+1}$		$-$		$+$	

Поскольку при переходе переменной x через корень c знак $f_k(x)$ изменяется на противоположный, то в столбце $f_k(x)$ должно стоять либо сочетание знаков $\begin{pmatrix} + \\ - \end{pmatrix}$, либо $\begin{pmatrix} - \\ + \end{pmatrix}$. В любом случае число перемен знаков между $f_{k-1}(x)$ и $f_{k+1}(x)$ в строках сохраняется. Поскольку, по условию, данный промежуток не содержит корней других многочленов Штурма, то, по рассмотренному случаю 1, остальные знаки в строках таблицы знаков сохраняются. Следовательно, при переходе от одной строчки к другой происходит только перераспределение знаков, а $W(x)$ не изменяется.

3. $x \in [a_i; a_{i+1}]$, причем этот отрезок содержит корень c данного многочлена $f_0(x) = f(x)$. В этом случае по третьему свойству системы многочленов Штурма при переходе x через корень $x = c$ произведение $f_0(x) \cdot f_1(x)$ меняет знак с «минуса» на «плюс», а значит, левее корня $f_0(x)$ и $f_1(x)$ разных знаков, а правее — одинаковых. Остальные знаки в строках таблицы знаков сохраняются, так как, по условию, данный промежуток не содержит корней других многочленов системы Штурма. Таблица знаков имеет следующий вид.

x	$f_0(x)$	$f_1(x)$	...
$a_i \le x < c$	$\pm$	$\mp$	
$c < x \le a_{i+1}$	$\mp$	$\mp$	

При переходе от одной строчки к другой теряется одна перемена знаков, $W(x)$ убывает на единицу.

Итак, в таблице знаков при переходе от одной строчки к другой (сверху вниз) теряется одна перемена знаков (вследствие чего $W(x)$ уменьшается на единицу) лишь в том случае, когда x проходит отрезок, содержащий корень данного многочлена. Отсюда следует, что число всех корней многочлена $f(x)$ на отрезке $[a; b]$ равно разности $W(a) - W(b)$. Теорема доказана.

Сам Ж. Штурм, излагая эту теорему студентам, после доказательства теоремы говорил: «Итак, доказана теорема, имя которой я ношу».

Пример 3.4

Продолжим рассмотрение приведенного выше многочлена $f(x) = x^4 - x - 3$. Мы уже установили, что этот многочлен имеет один положительный и один отрицательный корень. Найдем более тесные границы положительного корня. Для этого составим следующую таблицу знаков.

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$W(x)$
0	–	–	+	+	1
1	–	+	+	+	1
2	+	+	+	+	0

Видим, что потеря одной перемены знака произошла между значениями $x = 1$ и $x = 2$. Следовательно, искомый корень удовлетворяет неравенству $1 < x_1 < 2$. Для нахождения первой десятичной цифры корня x_1 делим отрезок [1; 2] пополам и составляем таблицу знаков для значений переменной 1,1; 1,2; 1,3; 1,4; 1,5. В итоге обнаруживаем потерю перемен знаков между $x = 1{,}4$ и $x = 1{,}5$ (проверьте!). Следовательно, $1{,}4 < x_1 < 1{,}5$, т.е. $x_1 = 1{,}4\ldots$. Таким образом, можно найти корень x_1 с любой наперед заданной точностью. Читателю предлагается найти подобные границы для отрицательного корня.

Контрольные вопросы

1. Существуют ли неприводимые над полем действительных чисел многочлены степени 3? Степени 4?
2. Будут ли неприводимыми над полем $\mathbb{R}$ следующие многочлены: а) $3x^2 - 7x + 5$; б) $3x^3 - 7x - 5$; в) $\sqrt{2}x - 7\sqrt[3]{5}$; г) $f(x) = 37$; д) нулевой многочлен?
3. Пересекает ли ось абсцисс график любого многочлена $f(x) \in \mathbb{R}[x]$ нечетной степени?
4. В каком случае существует горизонтальная прямая, пересекающая график многочлена $f(x) \in \mathbb{R}[x]$ в единственной точке? Ровно в двух точках?
5. Пусть корни многочлена $f(x) \in \mathbb{R}[x]$ принадлежат отрезку $[a, b]$. Как характеризуется график данного многочлена вне вертикальной полосы, ограниченной прямыми $x = a$ и $x = b$, в зависимости от четности степени многочлена и знака его старшего коэффициента? Сделайте схематичные рисунки.
6. Опишите процесс нахождения методом Штурма корня данного многочлена $f(x) \in \mathbb{R}[x]$ с точностью до двух десятичных знаков после запятой.

Задачи

1. Составьте приведенный многочлен с действительными коэффициентами наименьшей степени, среди корней которого содержатся корни:

а) $x_1 = 2, x_2 = 2i, x_3 = 1 - i$;

б) $x_{1,2} = -2, x_3 = -i$;

в) $x_1 = 3, x_{2,3} = 2 - 3i$;

г) $x_1 = 1 + \sqrt{2}, x_2 = 1 - \sqrt{2}, x_3 = 1 + 2i$;

д) $x_1 = -3i, x_2 = 2i, x_3 = 1 + i$.

2. Зная, что многочлен $x^4 - 4x^3 + 11x^2 - 14x + 10$ имеет корень $1 - 2i$, найдите остальные его корни.

3. Найдите границы действительных корней многочленов:

а) $x^4 - 4x^3 + 7x^2 - 20x + 31$;

б) $2x^5 + 3x^3 - 7x + 12$;

в) $x^4 - 4x^3 + 7x^2 - 20x + 31$;

г) $x^4 + x^2 - 14x + 15$; д) $5x^4 + 10x^3 - 7$.

4. Найдите число положительных и число отрицательных корней многочленов:

а) $x^4 + 4x^3 + 6x^2 + 3x - 1$;

б) $2x^4 - 7x^3 - 4x^2 + 27x - 18$;

в) $x^4 - 4x^3 + 7x^2 - 6x + 1$;

г) $2x^4 + 3x^4 - 2x - 3$.

5. Найдите количество действительных корней данного многочлена в заданном промежутке:

а) $x^3 - 3x^2 - 7x + 4$, $[4; 5]$;

б) $x^4 - x^3 + x^2 - 2x - 2$, $[1; 2]$;

в) $x^4 - 2x^3 - 3$, $[2; 3]$;

г) $x^4 - 4x^3 - 4x^2 + 12$, $[-1; 1]$, $[1; 2]$;

д) $x^4 - 5x^3 + 21x - 27$, $[-3; -2]$;

е) $6x^4 - 17x^3 + 18x^2 - 17x + 12$, $[2; 3]$.

6. Методом Штурма отделите действительные корни многочленов:

а) $x^4 - 6x^3 + 13x^2 - 14x + 7$;

б) $2x^5 - 10x^4 + 10x^3 + 10x^2 - 10x - 5$;

в) $x^4 - 4x^3 + 10x^2 - 12x + 4$;

г) $x^4 + 2x^3 + 3x^2 - 5x - 6$;

д) $x^4 + 2x^3 + 2x^2 - 4x - 4$;

е) $x^5 - 10x^3 + 30x^2 - 40x + 16$.

7. Вычислите с точностью до 0,01 действительные корни многочленов:

а) $x^4 - x^3 - 3x^2 + x + 1$;

б) $x^4 - x^3 - 4x^2 + 4x + 1$;

в) $x^4 - 2x^3 + x^2 + 2x + 1$;

г) $x^4 - x^3 + 2x - 1$;

д) $x^4 - 4x^3 - 20x^2 - 8x + 4$;

е) $x^4 + 2x^3 - 6x^2 - 10x + 1$.

8. Пользуясь теоремой Штурма, определите число действительных корней многочлена $x^3 + px + q$ при действительных p и q.

3.3. Кольца многочленов $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$

3.3.1. Нахождение рациональных корней многочлена с целыми коэффициентами

Кольца многочленов $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$ тесно связаны между собой. Если $f(x)$ — многочлен с рациональными коэффициентами и m — наименьшее общее кратное знаменателей всех его коэффициентов, то $m \cdot f(x)$ есть многочлен с целыми коэффициентами. Понятно, что число c является корнем многочлена $f(x)$ тогда и только тогда, когда c является корнем многочлена $m \cdot f(x)$. Следовательно, вопрос о нахождении рациональных корней многочленов с рациональными коэффициентами сводится к рассмотрению многочленов с целыми коэффициентами.

Пусть дан многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ с целыми коэффициентами и несократимая дробь $\frac{p}{q}$ является его корнем. Тогда $a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1 \frac{p}{q} + a_0 = 0$. Умножая равенство на q^n, получим $a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n = 0$. Отсюда $a_n p^n = -a_{n-1}p^{n-1}q - \ldots - a_1 pq^{n-1} - a_0 q^n$. Поскольку правая часть равенства делится на q, то $a_n p^n \vdots q$. Но, по условию, НОД$(p, q) = 1$, значит, $a_n \vdots q$. Аналогично получаем равенство $a_0 q^n = -a_n p^n - a_{n-1}p^{n-1}q - \ldots - a_1 pq^{n-1}$, из которого заключаем, что $a_0 q^n \vdots p$, а так как НОД$(q^n, p) = 1$, то $a_0 \vdots p$. Таким образом, доказана следующая теорема.

Теорема 3.6. *Если несократимая дробь $\frac{p}{q}$ является корнем многочлена $f(x)$ с целыми коэффициентами, то ее числитель p является делителем свободного члена, а знаменатель q — делителем старшего коэффициента.*

Следствие. Если старший коэффициент многочлена с целыми коэффициентами равен единице, то всякий рациональный корень многочлена является целым и находится среди делителей свободного члена.

Итак, для нахождения рациональных корней многочлена с целыми коэффициентами нужно выписать все делители свободного члена — и это будут «кандидаты» в числитель корня. Затем нужно выписать все натуральные делители старшего

коэффициента — и это будут «кандидаты» в знаменатель корня. После этого, сочетая числители и знаменатели, получаем «кандидатов» в корни, и остается только проверить (подстановкой в многочлен или по схеме Горнера), является ли очередной «кандидат» корнем данного многочлена. Таким образом, за конечное число шагов можно либо найти все рациональные корни, либо убедиться, что таковых нет.

Помогает отсеивать не корни следующая теорема.

Теорема 3.7. *Если несократимая дробь* $\frac{p}{q}$ *является корнем многочлена* $f(x)$ *с целыми коэффициентами, то для любого целого числа* k *число* $\frac{f(k)}{qk-p}$ *целое.*

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. По условию, $f\left(\frac{p}{q}\right) = 0$. Следовательно,

$$q^n f(k) = q^n f(k) - q^n f\left(\frac{p}{q}\right) =$$

$$= q^n(a_n k^n + a_{n-1}k^{n-1} + \ldots + a_1 k + a_0) -$$

$$- q^n\left[a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\frac{p}{q} + a_0\right] =$$

$$= q^n a_n k^n + q^n a_{n-1}k^{n-1} + \ldots + q^n a_1 k + q^n a_0 - a_n p^n -$$

$$- a_{n-1}qp^{n-1} - \ldots - a_1 q^{n-1}p - q^n a_0 =$$

$$= a_n(q^n k^n - p^n) + a_{n-1}q(q^{n-1}k^{n-1} - p^{n-1}) + \ldots + a_1 q^{n-1}(qk-p) \vdots (qk-p),$$

так как каждое слагаемое делится на $qk - p$. Итак, $q^n f(k) \vdots (qk-p)$. Но НОД$(p, q) = 1$, отсюда НОД$(q^n, qk - p) = 1$. Следовательно, $f(k) \vdots (qk - p)$, а значит, число $\frac{f(k)}{qk-p}$ целое. Теорема доказана.

Заметим, что имеет место и обратное: *если для многочлена с целыми коэффициентами* $f(x)$ *и несократимой дроби* $\frac{p}{q}$ *выражение* $\frac{f(k)}{qk-p}$ *является целым при любом натуральном* k*, то* $\frac{p}{q}$ *является корнем данного многочлена.*

В самом деле, выше доказано, что $q^n f(k) - q^n f\left(\frac{p}{q}\right) \vdots (qk-p)$. Но из условия следует, что первое слагаемое делится на $qk - p$.

Следовательно, $q^n f\left(\frac{p}{q}\right) \vdots (qk-p)$, а так как НОД($q^n$, $qk - p$) = 1, то $f\left(\frac{p}{q}\right) \vdots (qk-p)$ при любом натуральном k. Но это может быть лишь в случае, когда $f\left(\frac{p}{q}\right)=0$.

Пример 3.5

Найдем рациональные корни многочлена $f(x) = 2x^4 + 7x^3 - x^2 - 17x - 6$.

Решение. Если несократимая дробь $\frac{p}{q}$ является искомым корнем данного многочлена, то то $6 \vdots p$ и $2 \vdots q$. Имеем: $6 \vdots \pm1, \pm2, \pm3, \pm6$; $2 \vdots 1, 2$, поэтому «кандидатами» в корни данного многочлена являются $\pm1, \pm2, \pm3, \pm6, \pm\frac{1}{2}, \pm\frac{3}{2}$. Устранить лишних «кандидатов» помогает проверка выражений $\frac{f(1)}{p-q}$ и $\frac{f(-1)}{p+q}$ — для корня $\frac{p}{q}$ оба выражения должны быть целыми. Имеем: $f(1) = -12$, $f(-1) = 5$. Составляем таблицу и вносим в нее буквы «ц» — целое и «д» — дробь. При этом если в первой заполняемой строке появилась буква «д», то клетку под ней можно не заполнять.

$\frac{p}{q}$	2	–2	3	–3	6	–6	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$
$f(1)/(p-q)$	ц	ц	д	д	ц	д	ц	ц	ц	ц
$f(-1)/(p-q)$	д	ц	—	—	д	—	д	ц	ц	ц

Видим, что «кандидатами» в корни являются $-2, -\frac{1}{2}, \frac{3}{2}$ и $-\frac{3}{2}$. Испытание подстановкой выдерживают только первый и третий «кандидаты».

Иногда для нахождения рациональных корней многочлена с целыми коэффициентами $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ бывает удобно умножить этот многочлен на a_n^{n-1} и ввести новую переменную $y = a_n x^n$:

$$a_n^{n-1} f(x) = a_n^n x^n + a_{n-1}a_n^{n-1}x^{n-1} + \ldots + a_1 a_n^{n-1} x + a_0 a_n^{n-1} =$$
$$= (a_n x)^n + a_{n-1}(a_n x)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n x) + a_0 a_n^{n-1} =$$
$$= y^n + a_{n-1}y^{n-1} + \ldots + a_1 a_n^{n-2} y + a_0 a_n^{n-1} = h(y).$$

Рациональные корни полученного многочлена $h(y)$ являются целыми и находятся среди делителей свободного члена.

Пример 3.6

Решим еще раз пример 3.5. Умножим данный многочлен на 8 и введем новую переменную $y = 2x$:

$$8 \cdot f(x) = (2x)^4 + 7(2x)^3 - 2(2x)^2 - 68(2x) - 48 =$$

$$= y^4 + 7y^3 - 2y^2 - 68y - 48 = h(y).$$

Рациональные корни многочлена $h(y)$ являются целыми и находятся среди делителей свободного члена: $48 \vdots \pm1, \pm2, \pm3, \pm4, \pm6, \pm8, \pm12, \pm16, \pm24, \pm48$. Далее, $h(1) = -110$, $h(-1) = 12$. Для «кандидатов» в корни вида $\frac{p}{1}$ выражения $\frac{h(1)}{p-1}$ и $\frac{h(-1)}{p+1}$ являются оба целыми лишь для $p = 2, -4, 3$. Выдерживают испытание подстановкой лишь $y_1 = -4$, $y_2 = 3$. По формуле $x = \frac{y}{2}$ находим корни данного многочлена: $x_1 = -2$, $x_2 = \frac{3}{2}$.

3.3.2. Неприводимые многочлены в кольцах $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$

Обобщая понятие неприводимого над данным полем многочлена, будем говорить, что многочлен $f(x) \in K[x]$ *неприводим над областью целостности K*, если его степень ≥ 1 и он непредставим в виде произведения многочленов из $K[x]$ степени ≥ 1. Многочлен $f(x) \in K[x]$ будем называть *приводимым над областью целостности K*, если его можно представить в виде произведения многочленов из $K[x]$ степени ≥ 1.

Определение 3.2. Многочлен с целыми коэффициентами $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ называется *примитивным*, если НОД$(a_n, a_{n-1}, \ldots, a_1, a_0) = 1$.

Если $f(x) = a_n x^n$ — одночлен и $a_n \neq 0$, то формально считаем, что НОД(a_n) = НОД$(a_n, a_n) = a_n$.

Пример 3.7

Примитивными являются многочлены $1, -1, x, -x, x + 2, 4x^2 + 2x - 3, x^2 + 2x + 1$. Заметим, что примитивный многочлен может быть как неприводимым над кольцом целых чисел $\mathbb{Z}$ (над полем $\mathbb{Q}$), так и приводимым над $\mathbb{Z}$ (над $\mathbb{Q}$). Не являются примитивными многочлены $-3x$, $3x^2 + 6x + 3$, многочлен нулевой степени 23.

***Лемма 3.2* (*первая лемма Гаусса*).** *Произведение двух примитивных многочленов есть примитивный многочлен.*

Доказательство. Пусть даны два примитивных многочлена $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$ и пусть

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

Предположим, что НОД(c_{m+n}, c_{m+n-1}, ..., c_1, c_0) = $d \neq 1$ и p — простой делитель числа d. Поскольку данные многочлены примитивные, то все их коэффициенты не могут делиться на p. Следовательно, существуют наименьшие номера i и j, такие что a_i и b_j не делятся на p. Обозначим $k = i + j$ и рассмотрим коэффициент $c_k = a_0 b_k + \ldots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j-1} + \ldots + a_k b_0$. По предположению $c_k \vdots d \vdots p$. Все слагаемые, стоящие перед $a_i b_j$, делятся на p в силу минимальности номера i, а все слагаемые, стоящие после $a_i b_j$, делятся на p благодаря минимальности номера j. Следовательно, произведение $a_i b_j$ должно делиться на простое число p. Отсюда $a_i \vdots p$ или $b_j \vdots p$ — пришли к противоречию. Таким образом, $d = 1$, а значит, многочлен $h(x)$ примитивный.

***Лемма 3.3* (*вторая лемма Гаусса*).** *Если многочлен с целыми коэффициентами $f(x)$ приводим в $\mathbb{Q}[x]$, то он приводим и в $\mathbb{Z}[x]$.*

Доказательство. Пусть $f(x) \in \mathbb{Z}[x]$ и $f(x) = g(x) \cdot h(x)$, где $g(x)$, $h(x) \in \mathbb{Q}[x]$ и степени сомножителей ≥ 1. Если b и d — наименьшие общие кратные знаменателей всех коэффициентов соответственно многочленов $g(x)$ и $h(x)$, то $g(x) = \frac{1}{b} g_1(x)$, $h(x) = \frac{1}{d} h_1(x)$, где $g_1(x)$, $h_1(x) \in \mathbb{Z}[x]$. Пусть a и c — наибольшие общие делители всех коэффициентов соответственно многочленов $g_1(x)$ и $h_1(x)$, тогда $g_1(x) = a g_2(x)$, $h_1(x) = c h_2(x)$, где многочлены с целыми коэффициентами $g_2(x)$ и $h_2(x)$ примитивные. Их произведение $g_2(x) \cdot h_2(x) = f_1(x)$ по первой лемме Гаусса является примитивным многочленом. Таким образом,

$$f(x) = g(x) \cdot h(x) = \frac{1}{b} g_1(x) \frac{1}{d} h_1(x) =$$

$$= \frac{a}{b} g_2(x) \cdot \frac{c}{d} h_2(x) = \frac{r}{s} f_1(x),$$

где $\frac{a}{b} \cdot \frac{c}{d} = \frac{r}{s}$ и можно считать, что НОД(r, s) = 1. Пусть t_i — произвольный коэффициент многочлена $f_1(x)$. Поскольку $f(x)$ —

многочлен с целыми коэффициентами, то число $\frac{r}{s}t_i$ целое, а так как НОД$(r, s) = 1$, то $t_i \vdots s$. Итак, s является общим делителем всех коэффициентов многочлена $f_1(x)$, а так как этот многочлен примитивный, то $s = \pm 1$. Таким образом, $f(x) = \pm r \cdot g_2(x) \cdot h_2(x)$, т.е. $f(x)$ приводим в $\mathbb{Z}[x]$.

Теорема 3.8 (признак Эйзенштейна). *Пусть дан многочлен с целыми коэффициентами* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. *Если существует простое число* p, *такое что* a_n *не делится на* p, *а все остальные коэффициенты делятся на* p *и* a_0 *не делится на* p^2, *то многочлен* $f(x)$ *неприводим над* $\mathbb{Q}$.

Доказательство. Предположим противное, пусть многочлен $f(x)$ приводим над $\mathbb{Q}$. Тогда по второй лемме Гаусса $f(x)$ приводим над $\mathbb{Z}$. Пусть $f(x) = g(x) \cdot h(x)$, где $g(x)$, $h(x) \in \mathbb{Z}[x]$ и степени сомножителей ≥ 1. Пусть $g(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$, $h(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$. Тогда $b_0 c_0 = a_0 \vdots p$, откуда $b_0 \vdots p$ или $c_0 \vdots p$.

Одновременно b_0 и c_0 не могут делиться на p, так как, по условию, a_0 не делится на p^2. Пусть $b_0 \vdots p$, тогда c_0 не делится на p. Все коэффициенты многочлена $g(x)$ не могут делиться на p, так как, по условию, $a_n = b_k c_m$ не делится на p. Следовательно, существует наименьший номер $t < k$, такой что b_t не делится на p. Рассмотрим коэффициент $a_t = b_0 c_t + b_1 c_{t-1} + \ldots + b_{t-1}c_1 + b_t c_0$. По условию, $a_t \vdots p$ и в силу выбора номера t все слагаемые, кроме последнего, делятся на p. Но тогда и последнее слагаемое $b_t c_0$ также должно делиться на простое число p, откуда $b_t \vdots p$ или $c_0 \vdots p$ — пришли к противоречию. Полученное противоречие заставляет нас принять, что многочлен $f(x)$ неприводим над $\mathbb{Q}$.

Пример 3.8

Многочлен $x^n - 2$ неприводим над полем $\mathbb{Q}$ по признаку Эйзенштейна при $p = 2$. Это показывает, что существуют неприводимые над $\mathbb{Q}$ многочлены любой наперед заданной степени (в отличие от ситуаций в кольцах $\mathbb{R}[x]$ и $\mathbb{C}[x]$).

Иногда данный многочлен $f(x)$ с целыми коэффициентами не удовлетворяет условиям признака Эйзенштейна, но удается найти такое целое число c, что при замене переменной x по формуле $x = y - c$ получаем многочлен $h(y)$, удовлетворяющий условиям признака Эйзенштейна, а значит, неприводимый над $\mathbb{Z}$. В этом случае и исходный многочлен $f(x)$ также неприводим над $\mathbb{Z}$.

Пример 3.9

Для многочлена $x^4 + 2x^3 + 2x^2 - 3$ признак Эйзенштейна неприменим. Если же выполнить подстановку $x = y - 1$, то получим многочлен относительно переменой y, который неприводим по признаку Эйзенштейна при $p = 2$ (проверьте!). Отсюда делаем вывод, что и данный многочлен неприводим над полем $\mathbb{Q}$.

Пример 3.10

Для многочлена $x^4 - 3x^2 + 1$ признак Эйзенштейна неприменим. Попытка воспользоваться подстановкой $x = y - c$ при подходящем c также не приводит к успеху. Закрадывается подозрение, что данный многочлен приводим. С другой стороны, он не имеет рациональных корней, а значит, и линейных множителей. Остается предположить, что $x^4 - 3x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ при некоторых рациональных a, b, c, d. Раскрывая скобки и приравнивая коэффициенты, получаем

$$\begin{cases} a + c = 0, \\ b + ac + d = -3, \\ dc + ad = 0, \\ bd = 1. \end{cases}$$

Предполагая b и d целыми, обнаруживаем решение $b = d = -1$, $a = 1$, $c = -1$. Таким образом, $x^4 - 3x^2 + 1 = (x^2 + x - 1)(x^2 - x - 1)$.

3.3.3. Разложение на множители в кольце $\mathbb{Z}[x]$

Установим вид разложения на неприводимые множители многочлена над кольцом целых чисел. Предварительно докажем вспомогательное утверждение.

Лемма 3.4. *Если $p(x)$ и $q(x)$ — примитивные многочлены и для некоторых целых чисел a и b имеет место равенство $a \cdot p(x) = b \cdot q(x)$, то $a = \pm b$.*

Доказательство. Пусть даны примитивные многочлены

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0,$$

$$q(x) = d_n x^n + d_{n-1} x^{n-1} + \ldots + d_1 x + d_0,$$

т.е. НОД$(c_n, c_{n-1}, \ldots, c_1, c_0) = 1$ и НОД$(d_n, d_{n-1}, \ldots, d_1, d_0) = 1$. Из равенства $a \cdot px = b \cdot qx$ вытекает, что $ac_i = bd_i$ для $i = 0, 1, \ldots, n$. Тогда

$$a = a \cdot \text{НОД}(c_n, c_{n-1}, \ldots, c_1, c_0) = \text{НОД}(ac_n, ac_{n-1}, \ldots, ac_1, ac_0) =$$

$$= \text{НОД}(bd_n, bd_{n-1}, \ldots, bd_1, bd_0) = b \cdot \text{НОД}(d_n, d_{n-1}, \ldots, d_1, d_0) = \pm b.$$

Теорема 3.9 (о факторизации в кольце $\mathbb{Z}[x]$). *Всякий ненулевой многочлен с целыми коэффициентами, отличный от* ± 1, *представим в виде произведения некоторых простых чисел и неприводимых над* $\mathbb{Z}$ *примитивных многочленов. Такое разложение однозначно с точностью до порядка следования сомножителей и их знаков.*

Доказательство. Пусть дан ненулевой многочлен $f(x) \in \mathbb{Z}[x]$, отличный от ± 1. Если его степень равна нулю, т.е. $f(x) = a \in \mathbb{Z}$, то утверждение вытекает из основной теоремы арифметики. Пусть степень данного многочлена ≥ 1. Сначала докажем существование разложения данного многочлена в произведение неприводимых над кольцом $\mathbb{Z}$ множителей.

Если $f(x)$ неприводим над $\mathbb{Z}$, то доказывать нечего. Пусть $f(x)$ приводим и $f(x) = g(x) \cdot h(x)$, где $g(x), h(x) \in \mathbb{Z}[x]$, причем степени сомножителей меньше степени многочлена $f(x)$. Если многочлены $g(x)$ и $h(x)$ неприводимы над $\mathbb{Z}$, то утверждение доказано. Если же хотя бы один из сомножителей приводим, то повторим для него рассуждения. Поскольку степени сомножителей при этом разложении убывают, а бесконечно они убывать не могут, то на конечном шаге мы получим разложение многочлена $f(x)$ в произведение неприводимых в $\mathbb{Z}[x]$ множителей.

Из каждого сомножителя вынесем за скобки наибольший общий делитель всех его коэффициентов. Тогда в скобках окажутся неприводимые над $\mathbb{Z}$ примитивные многочлены. Разлагая вынесенные за скобки числовые множители в произведение простых чисел, получаем искомое представление данного многочлена.

Докажем единственность такого разложения. Пусть даны два таких разложения данного многочлена: $f(x) = a_1 a_2 \cdots a_k \times \times p_1(x) p_2(x) \cdots p_r(x)$ и $f(x) = b_1 b_2 \cdots b_m \cdot q_1(x) q_2(x) \cdots q_s(x)$, где сначала идут простые числа, а затем неприводимые над $\mathbb{Z}$ примитивные многочлены. Обозначим $a_1 a_2 \cdots a_k = a$, $b_1 b_2 \cdots b_m = b$, $p_1(x) p_2(x) \cdots p_r(x) = p(x)$, $q_1(x) q_2(x) \cdots q_s(x) = q(x)$. Тогда $a \cdot p(x) = b \cdot q(x)$. По первой лемме Гаусса многочлены $p(x)$ и $q(x)$ примитивные и по лемме 3.4 $a = \pm b$, т.е. $a_1 a_2 \cdots a_k = \pm b_1 b_2 \cdots b_m$. Вспомнив, что сомножители здесь являются простыми числами, по основной теореме арифметики заключаем, что $k = m$ и простые множители можно так упорядочить, что $a_i = \pm b_i$ для $i = 0, 1, \ldots, k$. Таким образом, $\pm b \cdot px = b \cdot qx$, откуда $\pm px = qx$, т.е. $\pm p_1(x) p_2(x) \cdots p_r(x) = q_1(x) q_2(x) \cdots q_s(x)$. Сомножители здесь являются неприводимыми в $\mathbb{Z}[x]$ многочленами, и по второй лемме Гаусса они неприводимы в $\mathbb{Q}[x]$.

Пользуясь теоремой о факторизации для кольца многочленов $\mathbb{Q}[x]$ над полем $\mathbb{Q}$ (см. теорему 2.6), отсюда заключаем, что $r = s$ и можно считать, что $p_j(x) = \varepsilon_j q_j(x)$, где $j = 1, 2, \ldots, r$ и ε_j есть некоторое рациональное число, отличное от нуля. Пусть $\varepsilon_j = \frac{m_j}{n_j}$, $m_j, n_j \in \mathbb{Z}$. Тогда $n_j p_j(x) = m_j q_j(x)$, а так как $p_j(x)$ и $q_j(x)$ примитивные, то по лемме 3.4 $m_j = \pm n_j$. Отсюда $p_j(x) = \pm q_j(x)$ и единственность указанного разложения $f(x)$ доказана. Вместе с тем теорема доказана.

Обобщим понятие простого натурального числа. В произвольной области целостности K элемент $p \in K$ будем называть *простым*, если он отличен от нуля, делителей единицы и не представим в виде произведения элементов, отличных от делителей единицы. Ненулевой элемент $a \in K$ будем называть *составным*, если его можно представить в виде произведения элементов, отличных от делителей единицы.

Понятно, что простыми элементами в $\mathbb{Z}[x]$ являются простые числа и неприводимые примитивные многочлены, а простые элементы в кольце многочленов $P[x]$ над полем P есть неприводимые над P многочлены и только они.

Факториальным кольцом называется область целостности, в которой имеет место аналог основной теоремы арифметики: *всякий ненулевой необратимый элемент области целостности представим в виде произведения простых элементов, причем однозначно с точностью до порядка следования сомножителей и делителей единицы* (*обратимых элементов*).

Используя это понятие, почти дословным повторением доказательства теоремы 3.9 можно получить более общее утверждение: *кольцо многочленов $K[x]$ над факториальным кольцом K факториально*.

Доказанные выше аналоги основной теоремы арифметики для колец многочленов над числовыми кольцами теперь можно сформулировать так: *кольца многочленов $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ факториальны*. Вообще, *всякое кольцо многочленов $P[x]$ над полем P факториально*. Отсюда последовательно получаем факториальность колец многочленов от нескольких переменных: $K[x, y] = (K[x])[y]$, $K[x, y, z] = (K[x, y])[z]$ и т.д. В частности, кольца многочленов $\mathbb{Z}[x_1 x \ldots x_n]$, $\mathbb{Q}[x_1, x_2, \ldots, x_n]$, $\mathbb{R}[x_1 x_2 \ldots x_n]$, $\mathbb{C}[x_1 x_2 \ldots x_n]$ факториальны. Кольца многочленов от нескольких переменных подробно будут рассмотрены ниже. Обобщение теории делимости на области целостности рассматривается в работе [8].

Контрольные вопросы

1. Как за конечное число шагов найти все рациональные корни многочлена с рациональными коэффициентами либо убедиться, что их нет?
2. При каком условии на коэффициенты всякий рациональный корень многочлена с целыми коэффициентами будет целым?
3. Пусть старший коэффициент многочлена с целыми коэффициентами есть простое число, а его свободный член равен единице. Каково максимально возможное число рациональных корней этого многочлена?
4. В чем состоит признак Эйзенштейна?
5. Является ли признак Эзенштейна необходимым, достаточным или необходимым и достаточным условием неприводимости многочлена с целыми коэффициентами над полем рациональных чисел?

Задачи

1. Найдите рациональные корни многочленов:
а) $x^4 + x^3 - 11x^2 - 5x + 30$;
б) $x^4 + 3x^2 + 2$;
в) $x^5 + 6x^4 + x^3 + 12x^2 + 40x + 24$;
г) $3x^4 + \frac{1}{2}x^3 + x^2 - 2x + \frac{1}{2}$.

2. Придумайте многочлены с целыми коэффициентами степени 6, имеющие заданные рациональные корни в количестве < 6 и затем найдите рациональные корни придуманных многочленов.

3. Пользуясь признаком Эйзенштейна, докажите неприводимость над полем $\mathbb{Q}$ многочленов:
а) $2x^5 + 21x^4 - 15x^3 + 24$;
б) $4x^7 - 14x^5 - 21x^3 + 28x^2 - 49x + 35$;
в) $3x^{100} - 13x + 52$;
г) $x^4 - 2x + 3$;
д) $2x^4 + 9x^3 + 20x^2 + 15x + 32$;
е) $3x^4 - 22x^3 + 60x^2 - 76x + 38$.

4. Придумайте многочлены с целыми коэффициентами, неприводимость которых над полем $\mathbb{Q}$ можно установить с помощью признака Эйзенштейна.

5. Разложите в произведение простых чисел и неприводимых над $\mathbb{Z}$ примитивных многочленов:
а) $90x^4 + 126x^3 - 108x^2 + 54x + 108$;
б) $189x^4 + 504x^3 + 252x^2 + 126x + 252$;
в) $630x^5 + 2142x^4 + 2016x^3 + 756x + 504$;
г) $54x^6 + 72x^5 - 162x^4 - 360x^3 - 144x^2 + 108x + 72$;
д) $24x^5 + 48x^4 - 36x^3 - 72x^2 - 36x - 72$;
е) $252x^5 + 252x^4 - 336x^3 - 504x + 336$.

6. Разложите на множители или докажите неприводимость многочленов:

а) $x^4 - 4x^3 + 3x^2 + 2x - 1$;

б) $x^4 + x^3 - 12x^2 + 12x - 1$;

в) $x^4 + 3x^3 - 3x + 1$;

г) $x^4 - x^3 - 5x^2 + 7x - 1$.

7. Докажите, что многочлен с целыми коэффициентами степени 2 приводим над полем $\mathbb{Q}$ тогда и только тогда, когда он имеет рациональный корень. Верно ли то же самое для многочленов степени 3? А степени 4?

8. Докажите, что многочлен $f(x)$ с целыми коэффициентами не имеет целых корней, если числа $f(0)$ и $f(1)$ нечетные.

3.4. Общие приемы решения уравнений 3-й и 4-й степеней

Речь пойдет об уравнениях вида $f(x) = 0$, где $f(x)$ — многочлен, вообще говоря, с комплексными коэффициентами степени 3 или 4. Перейдем на терминологию уравнений и корни многочлена $f(x)$ будем называть корнями уравнения $f(x) = 0$, а переменную x — неизвестной.

3.4.1. Преобразования общего уравнения третьей степени

Рассмотрим в общем виде кубическое уравнение относительно неизвестной z

$$a_3z^3 + a_2z^2 + a_1z + a_0 = 0.$$

Разделив его на старший коэффициент, получим *приведенное* кубическое уравнение вида

$$z^3 + az^2 + bz + c = 0.$$

Освободиться от квадрата неизвестной в этом уравнении можно с помощью стандартной подстановки $z = x - \frac{a}{3}$:

$$\left(x - \frac{a}{3}\right)^3 + a\left(x - \frac{a}{3}\right)^2 + b\left(x - \frac{a}{3}\right) + c =$$

$$= x^3 - 3x^2\frac{a}{3} + 3x\frac{a^2}{9} - \frac{a^3}{27} + ax^2 - 2ax\frac{a}{3} + \frac{a^3}{9} + bx - b\frac{a}{3} + c =$$

$$= x^3 + \left(b - \frac{a^2}{3}\right)x + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0.$$

Обозначив $p = b - \frac{a^2}{3}$, $q = \frac{2a^3}{27} - \frac{ab}{3} + c$, приходим к уравнению

$$x^3 + px + q = 0. \tag{3.1}$$

Далее рассмотрим частные случаи уравнения (3.1).

3.4.2. Корни уравнения $x^3 - 1 = 0$

Корни данного уравнения — это в точности корни 3-й степени из единицы: $\varepsilon_0 = 1$, $\varepsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\varepsilon_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Если обозначить $\varepsilon = \varepsilon_1$, то корни данного уравнения можно записать в виде $\varepsilon^0 = 1$, ε, ε^2. Именно в таком виде мы будем использовать их ниже. Геометрически на комплексной плоскости эти корни третьей степени из единицы изображаются точками единичной окружности, которые делят ее на три равные части.

3.4.3. Корни уравнения $x^3 - a = 0$

Если x_0 — один из корней данного уравнения, то остальные два находятся по формулам

$$x_1 = x_0 \cdot \varepsilon = x_0\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right), x_2 = x_0 \cdot \varepsilon^2 = x_0\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right).$$

В этом можно убедиться подстановкой в данное уравнение.

Пример 3.11

Решим уравнение $x^3 - 8 = 0$.

Решение. Очевидно, одним из корней является $x_0 = 2$. Остальные два корня $x_1 = 2 \cdot \varepsilon = -1 + i\sqrt{3}$, $x_2 = 2 \cdot \varepsilon^2 = -1 - i\sqrt{3}$.

3.4.4. Корни уравнения $x^3 + px + q = 0$

Корень данного уравнения будем искать в виде $x = u + v$, т.е. вместо одного неизвестного x будем искать два неизвестных u и v. Таким образом, имеем

$$(u + v)^3 + p(u + v) + q = 0.$$

Раскрывая скобки, получаем

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q =$$

$$= (u^3 + v^3 + q) + 3uv(u+v) + p(u+v) =$$

$$= (u^3 + v^3 + q) + (3uv + p)(u+v) = 0.$$

Будем искать u и v такими, чтобы $3uv + p = 0$, т.е. $3uv = -p$. Тогда $u^3 + v^3 + q = 0$. Возводя равенство $3uv = -p$ в куб, приходим к системе

$$\begin{cases} u^3 + v^3 = -q, \\ u^3 \cdot v^3 = -\dfrac{p^3}{27}. \end{cases}$$

Используя формулы Виета, заключаем, что u^3 и v^3 являются корнями так называемого *разрешающего уравнения* $z^2 + qz - \dfrac{p^3}{27} = 0$. Рассмотрим дискриминант разрешающего уравнения $D = \dfrac{q^2}{4} + \dfrac{p^3}{27} = \dfrac{4p^3 + 27q^2}{108}$.

Если $D = 0$, то $x^3 + px + q = \left(x - \dfrac{3q}{p}\right)\left(x + \dfrac{3q}{2p}\right)^2$ (проверьте!). Корнями данного уравнения будут $x_0 = \dfrac{3q}{p}$, $x_1 = x_2 = -\dfrac{3q}{2p}$.

Предположим теперь, что $D \neq 0$. Тогда находим один из корней разрешающего уравнения z_0 и решаем уравнение $u^3 = z_0$. Пусть u_0 — один из корней этого уравнения. Тогда из соотношения $u_0 v_0 = -\dfrac{p}{3}$ находим $v_0 = -\dfrac{p}{3u_0}$. Корнями данного кубического уравнения будут $x_0 = u_0 + v_0$, $x_1 = u_0\varepsilon + v_0\varepsilon^2$, $x_2 = u_0\varepsilon^2 + v_0\varepsilon$, что легко проверяется подстановкой в данное уравнение.

Докажем, что все три корня различны. Предположим сначала, что $x_0 = x_1$. Тогда $u_0 + v_0 = u_0\varepsilon + v_0\varepsilon^2$, $u_0(1 - \varepsilon) = v_0(\varepsilon^2 - 1)$. Возводя последнее равенство в куб, приходим к равенству $u_0^3 = v_0^3$. Вспомним, что $u_0^3 + v_0^3 = -q$, $u_0^3 \cdot v_0^3 = -\dfrac{p^3}{27}$, откуда $q^2 = 4u_0^6$, $p^3 = -27u_0^6$. Но тогда $108D = 4p^3 + 27q^2 = 4(-27)u_0^6 + 27 \cdot 4u_0^6 = 0$, что противоречит условию. Аналогично приходим к противоречию, предположив, что $x_0 = x_2$.

Наконец, предположим, что $x_1 = x_2$. Тогда получаем $u_0\varepsilon + v_0\varepsilon^2 = u_0\varepsilon^2 + v_0\varepsilon$, откуда $u_0 + v_0\varepsilon = u_0\varepsilon + v_0$, $u_0(1 - \varepsilon) = v_0(1 - \varepsilon)$, $u_0 = v_0$, что снова ведет к противоречию.

В заключение выделим *основные этапы решения уравнения* $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$.

1. Делим обе части уравнения на старший коэффициент a_3 и получаем уравнение вида $x^3 + ax^2 + bx + c = 0$.

2. Освобождаемся от квадрата неизвестной с помощью подстановки $x = y - \frac{a}{3}$ и получаем уравнение вида (3.1) $y^3 + py + q = 0$.

2.1. Если $p = 0$, то получаем уравнение $y^3 = -q$. Если y_0 — один из его корней, то два других есть $y_1 = y_0\varepsilon$, $y_2 = y_0\varepsilon^2$, где $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\varepsilon^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

2.2. Пусть $p \neq 0$. Составляем разрешающее уравнение $z^2 + qz - \frac{p^3}{27} = 0$ и вычисляем его дискриминант D.

2.2.1. Если $D = 0$, то корни уравнения (3.1) есть $y_0 = \frac{3q}{p}$, $y_1 = y_2 = -\frac{3q}{2p}$.

2.2.2. Если $D \neq 0$, то корни уравнения (3.1) различны и для их вычисления находим корень разрешающего уравнения $z^2 + qz - \frac{p^3}{27} = 0$. Пусть это будет z_0. Решаем уравнение $u^3 = z_0$ и отыскиваем один из его корней u_0. Из соотношения $u_0v_0 = -\frac{p}{3}$ находим $v_0 = -\frac{p}{3u_0}$. Находим корни уравнения (3.1): $y_0 = u_0 + v_0$, $y_1 = u_0\varepsilon + v_0\varepsilon^2$, $y_2 = u_0\varepsilon^2 + v_0\varepsilon$.

3. Пользуясь формулой $x = y - \frac{a}{3}$, находим корни данного уравнения.

3.4.5. Корни уравнения $x^3 + px + q = 0$ с действительными коэффициентами

Для данного кубического уравнения с действительными коэффициентами рассмотрим разрешающее уравнение.

Предположим, что дискриминант разрешающего уравнения $D > 0$. Тогда оно имеет действительный корень z_0. Но тогда

уравнение $u^3 = z_0$ имеет действительный корень u_0. В этом случае число $v_0 = -\frac{p}{3u_0}$ также действительное. В результате для данного кубического уравнения получаем один действительный корень $x_0 = u_0 + v_0$ и два мнимых сопряженных корня: $x_1 = u_0\varepsilon + v_0\varepsilon^2$ и $x_2 = u_0\varepsilon^2 + v_0\varepsilon = u_0\overline{\varepsilon} + v_0\overline{\varepsilon^2} = \overline{u_0\varepsilon + v_0\varepsilon^2} = \overline{x_1}$.

Случай $D = 0$ рассмотрен выше в подпараграфе 3.4.5 (п. 2.2.1).

Наконец, предположим, что дискриминант разрешающего уравнения $D < 0$. Тогда разрешающее уравнение имеет два мнимых сопряженных корня z_0 и $\overline{z_0}$. Но тогда уравнение $u^3 = z_0$ имеет три мнимых корня. Пусть u_0 — один из них. Поскольку v_0 находится из условия $3u_0v_0 = -p$ и p — действительное число, то $v_0 = \overline{u_0}$. Но тогда данное кубическое уравнение имеет три действительных корня:

$$x_0 = u_0 + v_0 = u_0 + \overline{u_0},\ x_1 = u_0\varepsilon + v_0\varepsilon^2 = u_0\varepsilon + \overline{u_0}\cdot\overline{\varepsilon} = u_0\varepsilon + \overline{u_0\varepsilon},$$

$$x_2 = u_0\varepsilon^2 + v_0\varepsilon = u_0\varepsilon^2 + \overline{u_0}\cdot\overline{\varepsilon^2} = u_0\varepsilon^2 + \overline{u_0\varepsilon^2}.$$

Подведем итог.

Теорема 3.10. *Пусть дано уравнение с действительными коэффициентами* $x^3 + px + q = 0$ *и* $D = \frac{q^2}{4} + \frac{p^3}{27} = \frac{4p^3 + 27q^2}{108}$. *При* $D = 0$ *уравнение имеет два действительных корня, из которых один двукратный, при* $D > 0$ *уравнение имеет один действительный и два мнимых сопряженных корня, а при* $D < 0$ *уравнение имеет три действительных корня.*

Пример 3.12

Решим уравнение $x^3 - 6x - 9 = 0$.

Решение. Составляем разрешающее уравнение $z^2 + qz - \frac{p^3}{27} = 0$. В нашем случае $p = -6$, $q = -9$, $u \cdot v = 2$ и разрешающее уравнение $z^2 - 9z + 8 = 0$. Дискриминант этого уравнения положителен, следовательно, данное кубическое уравнение имеет один действительный и два мнимых сопряженных корня. Корнями разрешающего уравнения будут $z_1 = 1$, $z_2 = 8$. Выбираем z_1 и решаем уравнение $u^3 = 1$. Выбираем действительный корень этого уравнения $u_0 = 1$, тогда $v_0 = -\frac{p}{3u_0} = 2$. Корнями данного кубического уравнения будут

$$x_0 = u_0 + v_0 = 1 + 2 = 3,$$

$$x_1 = u_0\varepsilon + v_0\varepsilon^2 = 1\cdot\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)+2\cdot\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)=-\frac{3}{2}-i\frac{\sqrt{3}}{2},$$

$$x_2 = u_0\varepsilon^2 + v_0\varepsilon = 1\cdot\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)+2\cdot\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=-\frac{3}{2}+i\frac{\sqrt{3}}{2}.$$

Ответ: $x_0 = 3$, $x_1 = -\frac{3}{2}-i\frac{\sqrt{3}}{2}$, $x_2 = -\frac{3}{2}+i\frac{\sqrt{3}}{2}$.

Рассмотрим уравнение $x^3 + px + q = 0$ и его разрешающее уравнение $z^2+qz-\frac{p^3}{27}=0$. Корнями последнего будут $z_1 = -\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, $z_2 = -\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$. Вспоминая, что $x = u + v$ и $u^3 = z_1$, $v^3 = z_2$, получаем $x=\sqrt[3]{z_1}+\sqrt[3]{z_2}$. Отсюда выводим *формулу Кардано*:

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

В этой формуле значения корней третьей степени нужно сочетать так, чтобы их утроенное произведение равнялось $-p$.

В приведенном выше примере 3.12 корнем уравнения является число 3. Следовательно, по формуле Кардано при $p = -6$, $q = -9$ получаем

$$3=\sqrt[3]{\frac{9}{2}+\sqrt{\frac{81}{4}-\frac{216}{27}}}+\sqrt[3]{\frac{9}{2}-\sqrt{\frac{81}{4}-\frac{216}{27}}},$$

во что даже трудно поверить. При попытке доказать это равенство возведением обеих частей в куб появляются неистребимые кубические корни.

Для доказательства данного равенства нужно обозначить

$$\alpha=\sqrt[3]{\frac{9}{2}+\sqrt{\frac{81}{4}-\frac{216}{27}}}+\sqrt[3]{\frac{9}{2}-\sqrt{\frac{81}{4}-\frac{216}{27}}}$$

и возведением обеих частей равенства в куб показать, что $\alpha^3 = 6\alpha + 9$, откуда $\alpha^3 - 6\alpha - 9 = 0$. Отсюда заключаем, что α является корнем уравнения $x^3 - 6x - 9 = 0$. Вместе с тем $x^3 - 6x - 9 = (x - 3)(x^2 + 3x + 3)$. Следовательно, число 3 является единственным действительным корнем данного уравнения. Отсюда и вытекает наше равенство.

Пример 3.13

Решим уравнение $x^3 + 6x^2 + 6x - 13 = 0$.

Решение. Здесь $a = 6$. Используя стандартную подстановку $x = y - \frac{a}{3} = y - 2$, приходим к уравнению $y^3 - 6y - 9 = 0$, которое решено в примере 3.12: $y_0 = 3$, $y_1 = -1\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $y_2 = -1\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Отсюда получаем корни исходного уравнения: $x_0 = y_0 - 2 = 1$, $x_1 = y_1 - 2 = -3\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $x_2 = y_2 - 2 = -3\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

3.4.6. Решение уравнений четвертой степени методом Феррари

Начнем с типичного примера.

Пример 3.14

Решим уравнение $x^4 + 2x^3 + 2x^2 - x - 1{,}25 = 0$.

Решение. Оставим в левой части равенства лишь члены, содержащие x^4 и x^3, остальное перенесем в правую часть: $x^4 + 2x^3 = -2x^2 + x + 1{,}25$. Дополним левую часть до полного квадрата: $(x^2)^2 + 2x^2 \cdot x + x^2 = x^2 - 2x^2 + x + 1{,}25$, $(x^2 + x)^2 = -x^2 + x + 1{,}25$.

Вводим новую переменную y так, чтобы в левой части равенства получился полный квадрат:

$$(x^2 + x)^2 + 2(x^2 + x) \cdot \frac{y}{2} + \frac{y^2}{4} = (x^2 + x) \cdot y + \frac{y^2}{4} - x^2 + x + 1{,}25,$$

$$\left(x^2 + x + \frac{y}{2}\right)^2 = (y - 1)x^2 + (y + 1)x + \frac{y^2}{4} + 1{,}25.$$

Подбираем y так, чтобы в правой части равенства оказался квадрат двучлена. Для этого потребуем, чтобы дискриминант квадратного трехчлена правой части равенства равнялся нулю, т.е. $D = (y + 1)^2 - 4(y - 1)\left(\frac{y^2}{4} + 1{,}25\right) = 0$. Отсюда $y^3 - 2y^2 - 3y + 6 = 0$. Возьмем корень $y_0 = 2$. При этом значении y получаем $(x^2 + x + 1)^2 = x^2 + 3x + 2{,}25$, или $(x^2 + x + 1)^2 = (x + 1{,}5)^2$. Рассмотрим два возможных случая.

1. $x^2 + x + 1 = x + 1{,}5$, $x^2 = 0{,}5$, $x_{1,2} = \pm\sqrt{0{,}5}$.
2. $x^2 + x + 1 = -x - 1{,}5$, $x^2 + 2x + 2{,}5 = 0$, $x_{3,4} = -1 \pm \sqrt{-1{,}5} = -1 \pm i\sqrt{1{,}5}$.

Ответ: $x_{1,2} = \pm\sqrt{0{,}5}$, $x_{3,4} = -1 \pm i\sqrt{1{,}5}$.

Теперь рассмотрим общий случай. Разделив общее уравнение четвертой степени на старший коэффициент, получим уравнение вида $x^4 + ax^3 + bx^2 + cx + d = 0$. Дальнейшие шаги такие же, как в рассмотренном примере: $x^4 + ax^3 = -bx^2 - cx - d$, дополняем левую часть до полного квадрата:

$$(x^2)^2 + 2 \cdot x^2 \cdot \frac{ax}{2} + \frac{a^2x^2}{4} = \frac{a^2x^2}{4} - bx^2 - cx - d,$$

$$\left(x^2 + \frac{ax}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d.$$

Дополняем левую часть равенства до полного квадрата, вводя новую переменную:

$$\left(x^2 + \frac{ax}{2}\right)^2 + 2\left(x^2 + \frac{ax}{2}\right)\frac{y}{2} + \frac{y^2}{4} =$$

$$= \left(\frac{a^2}{4} - b\right)x^2 - cx - d + \left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4},$$

$$\left(x^2 + \frac{ax}{2} + \frac{y}{2}\right)^2 = \left(\frac{a^2}{4} - b + y\right)x^2 + \left(\frac{ay}{2} - c\right)x + \frac{y^2}{4} - d. \quad (3.2)$$

Подберем y так, чтобы в правой части равенства оказался полный квадрат. Для этого нужно потребовать, чтобы дискриминант квадратного трехчлена, стоящего в правой части равенства, равнялся нулю: $\left(\frac{ay}{2} - c\right)^2 - 4\left(\frac{a^2}{4} - b + y\right)\left(\frac{y^2}{4} - d\right) = 0$, откуда

$$\frac{a^2y^2}{4} - ayc + c^2 - \frac{a^2y^2}{4} + by^2 - y^3 + a^2d - 4bd + 4dy = 0,$$

$$y^3 - by^2 + (ac - 4d)y - [c^2 + d(a^2 - 4b)] = 0.$$

Решая это уравнение, найдем такое $y = y_0$, при котором правая часть уравнения (3.2) будет квадратом: $\left(x^2 + \frac{ax}{2} + \frac{y_0}{2}\right)^2 = (mx + n)^2$. Отсюда $x^2 + \frac{ax}{2} + \frac{y_0}{2} = mx + n$ или $x^2 + \frac{ax}{2} + \frac{y_0}{2} = -mx - n$. Таким образом, остается решить два квадратных уравнения, что дает четыре корня данного уравнения. Данный метод носит

название *метода Феррари* в честь предложившего его итальянского математика XVI в. Лодовико Феррари.

Контрольные вопросы

1. Каким геометрическим преобразованием из графика многочлена $y = a_3z^3 + a_2z^2 + a_1z + a_0$ можно получить график многочлена вида $y = x^3 + px + q$?
2. Как геометрически изображаются корни уравнения $x^3 - a = 0$? Как их найти, исходя из этого изображения?
3. Как записывается разрешающее уравнение для уравнения $x^3 + px + q = 0$?
4. Как выглядит формула Кардано и в чем ее коварство?
5. В чем смысл метода Феррари?

Задачи

1. Решите уравнения третьей степени:

а) $x^3 - 27 = 0$;
б) $x^3 + 8 = 0$;
в) $x^3 - i = 0$;
г) $x^3 - 6x + 4 = 0$;
д) $x^3 + 3x^2 + 9x + 9 = 0$;
е) $x^3 - 3x^2 - 3x + 9 = 0$;
ж) $x^3 - 6x^2 + 3x - 18 = 0$;
з) $x^3 - (1 - i)x^2 - (1 + 2i)x + i = 0$;
и) $x^3 + 3x^2 + (3 - 6i)x + 5 - 10i = 0$.

2. Определите количество действительных корней уравнения:

а) $x^3 - 6x^2 + 11x - 11 = 0$;
б) $x^3 - 3x^2 - 2x + 7 = 0$;
в) $x^3 + 3x^2 - 2x - 1 = 0$;
г) $x^3 - 6x^2 + 9x + 104 = 0$;
д) $x^3 - 3x^2 - 6x + 20 = 0$;
е) $x^3 - 6x^2 + 6x + 10 = 0$.

3. Решите методом Феррари:

а) $x^4 + 2x^3 + 2x^2 + 6x - 3 = 0$;
б) $x^4 - 5x^3 + 6x^2 - 1 = 0$;
в) $x^4 - 2x^3 - 2x^2 + 12x - 24 = 0$;
г) $x^4 + 3x^3 + 2x^2 + x - 1 = 0$;
д) $x^4 - 3x^2 + 1 = 0$;
е) $x^4 + 2x^3 - 2x^2 - 2x + 1 = 0$;
ж) $x^4 - 5x^3 + 5x^2 + 5x - 5 = 0$.

4. Составьте уравнение третьей (четвертой) степени с придуманным набором корней и решите его.

5. Можно ли составить уравнение третьей степени с действительными коэффициентами, имеющее три мнимых корня? А четвертой?

6. Используя геометрическое изображение комплексных корней данной степени из данного действительного числа, решите уравнения:

а) $x^2 - 2 = 0$;

б) $x^3 - 2 = 0$;

в) $x^4 - 2 = 0$;

г) $x^6 - 2 = 0$;

д) $x^8 - 2 = 0$.

7. Докажите, что сумма корней уравнения $x^n - 1 = 0$ равна нулю.

Глава 4
МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

4.1. Основные понятия

4.1.1. Построение кольца многочленов от нескольких переменных

Пусть дана область целостности K. Ранее было доказано, что кольцо многочленов $K[x_1]$ от переменной x_1 само является областью целостности. Обозначим $K_1 = K[x_1]$ и построим кольцо многочленов $K_1[x_2]$ от переменной x_2. Обозначим $K_2 = K_1[x_2]$ и построим кольцо многочленов $K_3 = K_2[x_3]$ и т.д. На n-м шаге получим кольцо многочленов, которое будем обозначать $K[x_1, x_2, \ldots, x_n]$, а всякий его элемент будем называть *многочленом от n переменных* и обозначать $f(x_1, x_2, \ldots x_n)$.

Пример 4.1

Рассмотрим кольцо многочленов от двух переменных $K[x_1, x_2] = (K[x_1])[x_2]$. Пусть $f(x_2) = a_2x_2^2 + a_1x_2 + a_0$, где $a_2, a_1, a_0 \in K[x_1]$ и $a_2 = 2x_1 - 3$, $a_1 = 5$, $a_0 = x_1^3 - x_1 + 7$. Тогда подстановкой получаем многочлен от двух переменных

$$h(x_1, x_2) = (2x_1 - 3)x_2^2 + 5x_2 + x_1^3 - x_1 + 7 = 2x_1x_2^2 - 3x_2^2 + 5x_2 + x_1^3 - x_1 + 7.$$

Индукцией по n легко доказать, что всякий многочлен $f(x_1, x_2, \ldots, x_n)$ есть сумма *одночленов* вида $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$, где $a \in K$. Элемент a называется *коэффициентом одночлена*. Показатель α_i, $i = 1, 2, \ldots, n$, есть целое неотрицательное число. По определению считаем, что *всякая переменная в нулевой степени равна единице*. Если $a \neq 0$, то одночлен называется *ненулевым* и его *степенью* называется сумма показателей $\alpha_1 + \alpha_2 + \ldots + \alpha_n$. Если коэффициент $a = 0$, то одночлен называется *нулевым*. Многочлен от n переменных называется *нулевым*, если все его одночлены нулевые.

Одночлены $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ и $bx_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ называются *подобными*, если $\alpha_i = \beta_i$ для всякого $i = 1, 2, \ldots, n$, и данные одночлены называются *равными*, если они подобны и $a = b$. Всякий многочлен можно представить в виде суммы неподобных одночленов. При этом одночлен наибольшей степени называется *старшим членом многочлена*, а его степень называется *степенью* данного многочлена. *Стандартной записью многочлена* называется запись его в виде суммы неподобных одночленов, расположенных по убыванию их степеней. Два многочлена от n переменных, представленные своими стандартными записями, называются *равными*, если равны их соответствующие одночлены.

4.1.2. Лексикографическое упорядочение многочленов

Система расположения слов в словарях является примером лексикографического упорядочения. В словаре слово «муха» располагается выше слова «слон», а слово «слон» — выше слова «сосна» (таким образом, «муха» выше «слона», а «слон» выше «сосны»). Подобно этому упорядочению введем понятие «выше» сначала для переменных (букв алфавита), затем — для одночленов (слов), что позволит располагать члены многочлена в порядке убывания по высоте. Для обозначения отношения «выше» выберем знак $\succ$.

1. Считаем, что переменная x_i *выше* переменной x_j, если номер i меньше номера j. Таким образом, $x_1 \succ x_2 \succ x_3 \succ \ldots$.

2. Считаем, что подобные одночлены имеют *одинаковую высоту*. Пусть даны два неподобных одночлена $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ и $bx_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$. Будем считать, что первый одночлен выше второго, если существует номер k, такой что $\alpha_k > \beta_k$, а для всех номеров $i < k$ (если таковые существуют) имеем $\alpha_i = \beta_i$.

3. Если многочлен $f(x_1, x_2, \ldots, x_n)$ представлен в виде суммы неподобных одночленов, то *высшим членом* данного многочлена называется тот одночлен, который выше остальных одночленов этого многочлена. *Лексикографической записью многочлена* называется запись его в виде суммы неподобных одночленов, убывающих по высоте.

Например, $x_1 \succ x_2 \succ 33x_3$, $x_1x_2 \succ x_2^5$, $x_1^3x_2x_3 \succ x_1x_2^3x_3 \succ x_1x_2x_3^3$. Лексикографическими записями многочленов $f(x_1, x_2) = 73x_1x_2^3 - 4x_1^3x_2$ и $h(x_1, x_2) = 3x_1x_2^5 - 24x_1^2x_2 - 273x_1x_2^3 + 4x_1^3x_2$ будут соответственно $f(x_1, x_2) = -4x_1^3x_2 + 73x_1x_2^3$ и $h(x_1, x_2) = 4x_1^3x_2 - 24x_1^2x_2 + 3x_1x_2^5 - 273x_1x_2^3$. Заметим, что высший член многочлена может не совпадать с его старшим членом. Например,

в приведенном выше многочлене $h(x_1, x_2)$ высшим членом является $-4x_1^3x_2$, а старшим — $3x_1x_2^5$.

Лемма 4.1. *Если в цепочке одночленов каждый одночлен выше следующего:* $A_1 \succ A_2 \succ \ldots$, *то такая цепочка одночленов конечна.*

Доказательство. Индукцией по числу переменных n докажем конечность цепочки одночленов $A_1 \succ A_2 \succ \ldots$, где $A_1 = a_1x_1^{\alpha_{11}}x_2^{\alpha_{12}}\cdots x_n^{\alpha_{1n}}$, $A_2 = a_2x_1^{\alpha_{21}}x_2^{\alpha_{22}}\cdots x_n^{\alpha_{2n}}$, ...

При $n = 1$ получаем одночлены $A_1 = a_1x_1^{\alpha_{11}}$, $A_2 = a_2x_1^{\alpha_{21}}$, ..., причем $\alpha_{11} > \alpha_{21} > \ldots$. Поскольку показатели степеней — целые неотрицательные числа, а значит, бесконечно убывать не могут, то цепочка данных одночленов конечна.

Пусть уже доказана конечность цепочки строго убывающих по высоте одночленов от n переменных и дана цепочка строго убывающих по высоте одночленов от $n + 1$ переменных

$$B_1 = b_1x_0^{\alpha_{10}}x_1^{\alpha_{11}}x_2^{\alpha_{12}}\cdots x_n^{\alpha_{1n}},$$
$$B_2 = b_2x_0^{\alpha_{20}}x_1^{\alpha_{21}}x_2^{\alpha_{22}}\cdots x_n^{\alpha_{2n}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Тогда $\alpha_{10} \geq \alpha_{20} \geq \ldots$, а так как целые неотрицательные числа бесконечно убывать не могут, то эта последовательность показателей стабилизируется на некотором номере k. Пусть $\alpha = \alpha_{k0} = \alpha_{k+10} = \ldots$. Рассмотрим последовательность одночленов, начинающуюся с номера k:

$$B_k = b_kx_0^{\alpha}x_1^{\alpha_{k1}}x_2^{\alpha_{k2}}\cdots x_n^{\alpha_{kn}},$$
$$B_{k+1} = b_{k+1}x_0^{\alpha}x_1^{\alpha_{k+11}}x_2^{\alpha_{k+12}}\cdots x_n^{\alpha_{k+1n}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

При $x_0 = 1$ эта последовательность превращается в последовательность одночленов от n переменных, строго убывающих по высоте. По индуктивному предположению она конечна. Следовательно, конечна и последовательность $B_1 \succ B_2 \succ \ldots \succ B_k \succ \succ B_{k+1} \succ \ldots$. Лемма доказана.

Лемма 4.2 (о высшем члене произведения многочленов). *Высший член произведения двух многочленов равен произведению высших членов перемножаемых многочленов.*

Доказательство. Пусть даны многочлены $f(x_1, x_2, \ldots, x_n)$ и $h(x_1, x_2, \ldots, x_n)$ своими лексикографическими записями. Пусть $A = ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ и $B = bx_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ — высшие члены этих многочленов, а $A' = a'x_1^{\alpha'_1}x_2^{\alpha'_2}\cdots x_n^{\alpha'_n}$ и $B' = b'x_1^{\beta'_1}x_2^{\beta'_2}\cdots x_n^{\beta'_n}$ — одночлены этих многочленов, которые не являются высшими. Таким обра-

зом, $f(x_1, x_2, \ldots, x_n) = A + \ldots + A' + \ldots$, $h(x_1, x_2, \ldots, x_n) = B + \ldots + B' + \ldots$ и $f(x_1, x_2, \ldots, x_n) \cdot h(x_1, x_2, \ldots, x_n) = (A + \ldots + A' + \ldots) \cdot (B + \ldots + B' + \ldots) = AB + AB' + A'B + A'B' + \ldots$.

Докажем, что $A \cdot B$ выше произведений $A' \cdot B$, $A \cdot B'$, $A' \cdot B'$. Покажем, например, что $A \cdot B \succ A' \cdot B'$ (остальные соотношения доказываются аналогично). Имеем:

$$A \cdot B = abx_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \cdots x_n^{\alpha_n+\beta_n},$$

$$A' \cdot B' = a'b'x_1^{\alpha'_1+\beta'_1} x_2^{\alpha'_2+\beta'_2} \cdots x_n^{\alpha'_n+\beta'_n}.$$

Сравним показатели при x_1. По условию, $A \succ A'$, $B \succ B'$, откуда $\alpha_1 \geq \alpha'_1$, $\beta_1 \geq \beta'_1$ и $\alpha_1 + \beta_1 \geq \alpha'_1 + \beta'_1$. Если $\alpha_1 + \beta_1 > \alpha'_1 + \beta'_1$, то $A \cdot B \succ A' \cdot B'$, что и требовалось доказать.

Предположим, что $\alpha_1 + \beta_1 = \alpha'_1 + \beta'_1$. Если предположить, что $\alpha_1 \neq \alpha'_1$, то $\alpha_1 > \alpha'_1$, и из равенства вытекает, что $\beta_1 < \beta'_1$ — пришли к противоречию. Следовательно, $\alpha_1 = \alpha'_1$, откуда $\beta_1 = \beta'_1$. В этом случае переходим к сравнению показателей при x_2. Таким образом, либо на некотором шаге мы придем к выводу о том, что $A \cdot B \succ A' \cdot B'$, что и требуется доказать, либо установим, что $\alpha_1 = \alpha'_1$, $\alpha_2 = \alpha'_2$, ..., $\alpha_n = \alpha'_n$, а значит, одночлены A и A' подобны. Но это противоречит условию. Вместе с тем лемма доказана.

Контрольные вопросы

1. Как определяется лексикографическое упорядочение членов многочлена от нескольких переменных?
2. Однозначна ли лексикографическая запись многочлена?
3. Как определяются понятия старшего члена и высшего члена данного многочлена от нескольких переменных? Могут ли они совпадать? Не совпадать?
4. Можно ли построить бесконечную цепочку одночленов убывающих по высоте?
5. Как формулируется основное свойство высшего члена произведения двух многочленов?

Задачи

1. Пусть $K_1 = \mathbb{Z}[x_1]$, $K_2 = \mathbb{Z}[x_2]$. Запишите данный многочлен в виде многочлена кольца $K_2[x_1]$ и в виде многочлена кольца $K_1[x_2]$:

а) $7x_1x_2^3 - 4x_1^3x_2 + 3x_1x_2^2 + 2x_1 - x_2 + 1$;

б) $7x_1^2 - 4x_2^2 + 3x_1x_2 - 2x_1 + x_2 + 11$;

в) $(x_1 + x_2 + 1)^2$.

2. Запишите многочлены лексикографически и укажите их старшие члены:

а) $273x_1x_2^3 - 4x_1^3x_2$;

б) $x_1x_3 + x_2x_3 - x_1x_2 - x_1^2$;

в) $x_1x_3 + x_1x_2x_3 - x_1x_2x_3^2 - x_1x_2$;

г) $x_1 + x_2 - x_1x_2$;

д) $37x_1 + 8x_2 - x_1x_2$;

е) $3x_1 + 8x_2$.

3. Для данного одночлена выпишите все одночлены той же степени от трех переменных с коэффициентом 1, которые ниже его:

а) x_1x_2; б) $x_1^2x_2$; в) $x_1^2x_2x_3$;

г) $x_1x_2^2x_3$; д) $x_1^3x_2x_3$.

4. Расположите данные многочлены в виде последовательности многочленов, строго убывающих по высоте: $x_1x_3 + x_2x_3 - x_1x_2 - x_1^2$, $x_1^3x_2x_3 + x_1x_2x_3$, x_1x_2.

5. Укажите высший член произведения данных многочленов:

а) $x_1x_3 + x_2x_3 - x_1x_2 - x_1^2$ и $3x_1x_3 + 2x_2x_3 - 5x_1^2x_2 - x_1^2$;

б) $x_1 + x_2 - x_1x_3$ и $x_1x_3 + x_2x_3 + x_1x_2$;

в) $x_1^2x_3 + x_2x_3 - x_1x_2 - x_1^2$ и $3x_1x_3 + 2x_2^2x_3 - 5x_1^2x_2 - x_1^2$.

6. Сколько существует одночленов от трех переменных той же степени с коэффициентом 1, выше которых данный одночлен:

а) $x_1^3x_2x_3$;

б) $x_1^4x_2^3x_3^2$;

в) $x_1^nx_2x_3$?

7. Пусть два многочлена даны своими лексикографическими записями. Верно ли, что низший член произведения равен произведению низших членов сомножителей?

8. Приведите пример трехчлена, у которого высший член является первым, а старший член — последним.

9. Приведите примеры многочленов от трех переменных, у которых каждый член имеет одну и ту же степень, и запишите их лексикографически.

10. Выпишите все одночлены от трех переменных четвертой степени с коэффициентом 1 и составьте из них лексикографическую запись многочлена.

4.2. Симметрические многочлены

4.2.1. Элементарные симметрические многочлены

Рассмотрим многочлен $f(x_1, x_2, x_3) = x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3$. Выполним перестановку переменных: $x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_1$. Получим многочлен $x_2^3x_3x_1 + x_2x_3^3x_1 + x_2x_3x_1^3$, равный данному. Легко видеть, что это будет так при любой перестановке переменных. В силу этого данный многочлен называется симметрическим. Дадим общее определение.

Определение 4.1. Многочлен $f(x_1, x_2, ..., x_n)$ называется *симметрическим*, если при любой перестановке переменных получаем многочлен, равный данному.

Понятно, что сумма и произведение двух симметрических многочленов будут симметрическими многочленами, так что множество всех симметрических многочленов над областью целостности K образует кольцо, которое является подкольцом кольца всех многочленов $K[x_1, x_2, ..., x_n]$.

Выделим в кольце симметрических многочленов так называемые элементарные симметрические многочлены.

Определение 4.2. *Элементарными симметрическими многочленами* от n переменных называются многочлены

$$\sigma_1(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n,$$

$$\sigma_2(x_1, x_2, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n,$$

.....

$$\sigma_n(x_1, x_2, ..., x_n) = x_1x_2\cdots x_n.$$

Например, элементарными симметрическими многочленами от двух переменных будут $\sigma_1(x_1, x_2) = x_1 + x_2$ и $\sigma_2(x_1, x_2) = x_1x_2$; от трех переменных — $\sigma_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$, $\sigma_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3(x_1, x_2, x_3) = x_1x_2x_3$. Если ясно, о каких переменных идет речь, то для краткости элементарные симметрические многочлены будем обозначать одной буквой, опуская переменные: $\sigma_1, \sigma_2, ..., \sigma_n$.

4.2.2. Леммы о симметрических многочленах

Наша задача — доказать, что всякий симметрический многочлен $f(x_1, x_2, ..., x_n)$ можно представить в виде суммы комбинаций элементарных симметрических многочленов вида $a\sigma_1^{\gamma_1}\sigma_2^{\gamma_2}\cdots_n^{\gamma_n}$, т.е. в виде некоторого многочлена от элементарных симметрических многочленов: $f(x_1, x_2, ..., x_n) = h(\sigma_1, \sigma_2, ..., \sigma_n)$.

Рассмотрим симметрический многочлен

$$f(x_1, x_2, x_3) = x_1x_2^3x_3^3 + x_1^3x_2x_3^3 + x_1^3x_2^3x_3 + x_1^3 + x_2^3 + x_3^3 + 5x_1x_2x_3.$$

Он распадается на сумму двух симметрических многочленов:

$$g(x_1, x_2, x_3) = x_1x_2^3x_3^3 + x_1^3x_2x_3^3 + x_1^3x_2^3x_3,$$

$$h(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + 5x_1x_2x_3.$$

Замечаем, что все члены первого многочлена имеют одну и ту же степень 7, а все члены второго многочлена — степень 3. Обобщим этот типичный пример, введя соответствующее понятие.

Определение 4.3. Многочлен от n переменных называется *однородным*, если каждый его член имеет одну и ту же степень.

Понятно, что всякий симметрический многочлен равен сумме своих однородных симметрических компонент, так что поставленную выше задачу достаточно решить для однородных симметрических многочленов.

Лемма 4.3. 1. *Сумма двух однородных симметрических многочленов одной и той же степени есть либо нулевой многочлен, либо однородный симметрический многочлен той же степени.*

2. *Произведение двух однородных симметрических многочленов степеней соответственно k и m есть однородный симметрический многочлен степени $k + m$.*

Доказательство. 1. Сложение двух однородных симметрических многочленов одной и той же степени k сводится к приписыванию к первому многочлену второго с последующим приведением подобных. В итоге получим либо нулевой многочлен, либо однородный симметрический многочлен той же степени.

2. Пусть даны однородные симметрические многочлены $f(x_1, x_2, \ldots, x_n)$ и $h(x_1, x_2, \ldots, x_n)$ степеней соответственно k и m, и пусть $A = ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ и $B = bx_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ — их произвольные одночлены. Тогда $\alpha_1 + \alpha_2 + \ldots + \alpha_n = k$, $\beta_1 + \beta_2 + \ldots + \beta_n = m$ и произвольный член произведения данных многочленов имеет вид

$$AB = abx_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \cdots x_n^{\alpha_n+\beta_n},$$

причем $(\alpha_1 + \beta_1) + (\alpha_2 + \beta_2) + \ldots + (\alpha_n + \beta_n) = k + m$. Следовательно, произведение $f(x_1, x_2, \ldots, x_n) \cdot h(x_1, x_2, \ldots, x_n)$ есть однородный симметрический многочлен степени $k + m$.

Следствие. Комбинация элементарных симметрических многочленов $a\sigma_1^{\gamma_1}\sigma_2^{\gamma_2} \cdots \sigma_n^{\gamma_n}$ есть однородный симметрический многочлен.

Лемма 4.4. *Если $A = ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ — высший член симметрического многочлена $f(x_1, x_2, \ldots, x_n)$, данного своей лексикографической записью, то $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$.*

Доказательство. Докажем, что $\alpha_1 \geq \alpha_2$. Для этого в многочлене $f(x_1, x_2, \ldots, x_n)$ поменяем местами переменные x_1 и x_2. При этом многочлен $f(x_1, x_2, \ldots, x_n)$ не изменится, а его высший член $A = ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ преобразуется в одночлен

$A' = ax_2^{\alpha_1} x_1^{\alpha_2} x_3^{\alpha_3} \cdots x_n^{\alpha_n} = ax_1^{\alpha_2} x_2^{\alpha_1} x_3^{\alpha_3} \cdots x_n^{\alpha_n}$, который уже не является высшим. Следовательно, $A \succ A'$, откуда $\alpha_1 \geq \alpha_2$.

При перемене мест переменных x_2 и x_3 получим одночлен $A'' = ax_1^{\alpha_1} x_2^{\alpha_3} x_3^{\alpha_2} \cdots x_n^{\alpha_n}$ данного симметрического многочлена, который также не является высшим. Сравнивая по высоте одночлены A и A'', заключаем, что $\alpha_2 \geq \alpha_3$. И т.д. Лемма доказана.

Лемма 4.5. *Высший член комбинации элементарных симметрических многочленов* $a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$ *равен* $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_{n-1}^{\alpha_{n-1}}x_n^{\alpha_n}$.

Доказательство. Высшие члены элементарных симметрических многочленов σ_1, σ_2, ..., σ_n равны соответственно x_1, x_1x_2, ..., $x_1x_2\cdots x_n$. Вспомним, что высший член произведения симметрических многочленов равен произведению высших членов этих многочленов. Поэтому высший член симметрического многочлена $a\sigma_1^{\alpha_1-\alpha_2}\sigma_1^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$ равен $ax_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3}\cdots(x_1x_2\cdots x_{n-1})^{\alpha_{n-1}-\alpha_n}(x_1x_2\cdots x_{n-1}x_n)^{\alpha_n}$. Показатель степени при переменной x_1 равен $(\alpha_1 - \alpha_2) + (\alpha_2 - \alpha_3) + \ldots + (\alpha_{n-1} - \alpha_n) + \alpha_n = \alpha_1$. Аналогично устанавливаем, что показатели степеней при переменных x_2, ..., x_n равны соответственно α_2, ..., α_n. Лемма доказана.

Следствие 1. Если $A = ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ — высший член симметрического многочлена $f(x_1, x_2, \ldots, x_n)$, данного лексикографической записью, то A выше высшего члена многочлена $f_1(x_1, x_1, \ldots, x_n) = f - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$.

Доказательство. Достаточно заметить, что по лемме 4.5 высшие члены многочленов $f(x_1, x_2, \ldots, x_n)$ и $a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$ одинаковы.

Следствие 2. Высший член комбинации элементарных симметрических многочленов $a\sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_{n-1}^{\beta_{n-1}}\sigma_n^{\beta_n}$ равен $ax_1^{\beta_1+\beta_2+\ldots+\beta_n}x_2^{\beta_2+\beta_3+\ldots+\beta_n}\cdots x_{n-1}^{\beta_{n-1}+\beta_n}x_n^{\beta_n}$.

Доказательство. Положим $\alpha_n = \beta_n$, $\alpha_{n-1} = \alpha_n + \beta_{n-1}$, ..., $\alpha_2 = \alpha_3 + \beta_2$, $\alpha_1 = \alpha_2 + \beta_1$. Тогда $\beta_1 = \alpha_1 - \alpha_2$, $\beta_2 = \alpha_2 - \alpha_3$, ..., $\beta_{n-1} = \alpha_{n-1} - \alpha_n$, $\beta_n = \alpha_n$, откуда $\beta_1 + \beta_2 + \ldots + \beta_{n-1} + \beta_n = \alpha_1$, $\beta_2 + \beta_3 + \ldots + \beta_{n-1} + \beta_n = \alpha_2$, ..., $\beta_{n-1} + \beta_n = \alpha_{n-1}$, $\beta_n = \alpha_n$.

Поскольку $a\sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_{n-1}^{\beta_{n-1}}\sigma_n^{\beta_n} = a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_1-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{n}$, то по лемме 4.5 высший член комбинации многочленов $a\sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_{n-1}^{\beta_{n-1}}\sigma_n^{\beta_n}$ равен

$$ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_{n-1}^{\alpha_{n-1}}x_n^{\alpha_n} = ax_1^{\beta_1+\beta_2+\ldots+\beta_n}x_2^{\beta_2+\beta_3+\ldots+\beta_n}\cdots x_{n-1}^{\beta_{n-1}+\beta_n}x_n^{\beta_n}.$$

4.2.3. Основная теорема о симметрических многочленах

Теперь мы можем достичь цели, поставленной в подпараграфе 4.2.2: основываясь на доказанных выше леммах об элементарных симметрических многочленах, докажем теорему, которую принято называть основной для симметрических многочленов. Она устанавливает существование представления всякого симметрического многочлена в виде многочлена от элементарных симметрических многочленов. Доказательство существования носит конструктивный характер и может быть использовано для практического нахождения такого представления.

Теорема 4.1. *Всякий симметрический многочлен однозначно представим в виде многочлена от элементарных симметрических многочленов. Точнее, для любого симметрического многочлена* $f(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ *существует и притом только один многочлен* $h(y_1, y_2, \ldots, y_n) \in K[y_1, y_2, \ldots, y_n]$, *такой что* $f(x_1, x_2, \ldots, x_n) = h(\sigma_1, \sigma_2, \ldots, \sigma_n)$..

Доказательство. *Существование*. Как уже было сказано выше, теорему достаточно доказать для однородных симметрических многочленов. Для однородного симметрического многочлена нулевой степени $f(x_1, x_2, \ldots, x_n) = a \in K$ имеем $f(x_1, x_2, \ldots, x_n) = a\sigma_1^0\sigma_2^0 \cdots \sigma_n^0$ и утверждение доказано.

Пусть дан однородный симметрический многочлен $f(x_1, x_2, \ldots, x_n)$ и $A = ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ — его высший член ненулевой степени. Тогда, по следствию 1 из леммы 4.5 A выше высшего члена многочлена $f_1 = f - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$. По лемме 4.3 $f(x_1, x_2, \ldots, x_n)$ есть либо нулевой, либо однородный симметрический многочлен. В первом случае получаем $f = a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$ и утверждение доказано. Рассмотрим второй случай. Пусть $bx_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ — высший член симметрического многочлена $f_1(x_1, x_2, \ldots, x_n)$. Тогда по следствию 1 из леммы 4.5 высший член многочлена f_1 выше высшего члена симметрического многочлена $f_2 = f_1 - b\sigma_1^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}\cdots\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n}$ и т.д. Поскольку последовательность высших членов симметрических многочленов $f, f_1, f_2, \ldots$ строго убывает по высоте, то по лемме 4.1 эта последовательность симметрических многочленов конечна. Но процесс образования многочленов последовательности может закончиться только на нулевом многочлене. В итоге на некотором номере k получаем равенства

$$f_1 = f - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n},$$

$$f_2 = f_1 - b\sigma_1^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}\cdots\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n},$$

.....

$$0 = f_k = f_{k-1} - c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3}\cdots\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}.$$

Складывая их, получаем

$$0 = f - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n} -$$
$$- b\sigma_1^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}\cdots\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n} - \ldots - c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3}\cdots\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}.$$

Отсюда вытекает искомое равенство:

$$f = a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\cdots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n} + b\sigma_1^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}\cdots\sigma_{n-1}^{\beta_{n-1}-\beta_n}\sigma_n^{\beta_n} +$$
$$+ \ldots + c\sigma_1^{\gamma_1-\gamma_2}\sigma_2^{\gamma_2-\gamma_3}\cdots\sigma_{n-1}^{\gamma_{n-1}-\gamma_n}\sigma_n^{\gamma_n}.$$

Существование представления доказано.

Единственность. Пусть имеем два представления ненулевого симметрического многочлена $f(x_1, x_2, \ldots, x_n)$ в виде многочленов от элементарных симметрических многочленов: $f = g_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ и $f = g_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$, где $g_1(y_1, y_2, \ldots, y_n) \neq g_2(y_1, y_2, \ldots, y_n)$. Тогда многочлен $h(y_1, y_2, \ldots, y_n) = g_1(y_1, y_2, \ldots, y_n) - g_2(y_1, y_2, \ldots, y_n)$ ненулевой.

Рассмотрим два его неподобных одночлена:

$$A(y_1, y_2, \ldots, y_n) = ay_1^{\alpha_1}y_2^{\alpha_2}\cdots y_n^{\alpha_n},\ B(y_1, y_2, \ldots, y_n) = by_1^{\beta_1}y_2^{\beta_2}\cdots y_n^{\beta_n}.$$

Имеем

$$A(\sigma_1, \sigma_2, \ldots, \sigma_n) = a\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdots\sigma_n^{\alpha_n},\ B(\sigma_1, \sigma_2, \ldots, \sigma_n) = b\sigma_1^{\beta_1}\sigma_2^{\beta_2}\cdots\sigma_n^{\beta_n}.$$

По следствию 2 из леммы 4.5 высшими членами этих многочленов являются соответственно $ax_1^{\alpha_1+\alpha_2+\ldots+\alpha_n}x_2^{\alpha_2+\ldots+\alpha_n}\cdots x_n^{\alpha_n}$ и $bx_1^{\beta_1+\beta_2+\ldots+\beta_n}x_2^{\beta_2+\ldots+\beta_n}\cdots x_n^{\beta_n}$. Если предположить, что эти одночлены подобны, то получаем равенства $\alpha_1 + \alpha_2 + \ldots + \alpha_n = \beta_1 + \beta_2 + \ldots + \beta_n$, $\alpha_2 + \ldots + \alpha_n = \beta_2 + \ldots + \beta_n$, $\ldots$, $\alpha_n = \beta_n$, из которых следует, что $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, $\ldots$, $\alpha_n = \beta_n$. Таким образом, одночлены $A(y_1, y_2, \ldots, y_n) = ay_1^{\alpha_1}y_2^{\alpha_2}\cdots y_n^{\alpha_n}$ и $B(y_1, y_2, \ldots, y_n) = by_1^{\beta_1}y_2^{\beta_2}\cdots y_n^{\beta_n}$ оказываются подобными вопреки нашему предположению.

Следовательно, высшие члены многочленов $A(\sigma_1, \sigma_2, \ldots, \sigma_n)$ и $B(\sigma_1, \sigma_2, \ldots, \sigma_n)$ не подобны. Отсюда заключаем, что многочлен $h(\sigma_1, \sigma_2, \ldots, \sigma_n)$ имеет ненулевой высший член. С другой

стороны, $h(\sigma_1, \sigma_2, ..., \sigma_n) = g_1(\sigma_1, \sigma_2, ..., \sigma_n) - g_1(\sigma_1, \sigma_2, ..., \sigma_n) = f - f = 0$, т.е. $h(\sigma_1, \sigma_2, ..., \sigma_n)$ как многочлен от переменных x_1, x_2, ..., x_n является нулевым. Пришли к противоречию. Вместе с тем единственность доказана.

Пример 4.2

Рассмотрим упоминавшийся в начале подпараграфа 4.2.2 симметрический многочлен

$$f(x_1, x_2, x_3) = x_1x_2^3x_3^3 + x_1^3x_2x_3^3 + x_1^3x_2^3x_3 + x_1^3 + x_2^3 + x_3^3 + 5x_1x_2x_3$$

и представим его в виде многочлена от элементарных симметрических многочленов.

Решение. Сначала займемся первой однородной компонентой данного многочлена и запишем ее лексикографически, т.е. расположим одночлены по убыванию их высот:

$$g(x_1, x_2, x_3) = x_1^3x_2^3x_3 + x_1^3x_2x_3^3 + x_1x_2^3x_3^3.$$

Согласно основной теореме о симметрических многочленах ответ следует искать в виде $g = a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\sigma_3^{\alpha_3} + b\sigma_1^{\beta_1-\beta_2}\sigma_2^{\beta_2-\beta_3}\sigma_3^{\beta_3} + ...$, где слагаемые строго убывают по высоте (как многочлены от x_1, x_2, x_3). Высшие члены этих слагаемых равны соответственно $ax_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$, $bx_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$, ... Поскольку высший член данного многочлена равен $x_1^3x_2^3x_3$, то $a = 1$, $\alpha_1 = 3$, $\alpha_2 = 3$, $\alpha_3 = 1$. Так как многочлен $g(x_1, x_2, x_3)$ — однородный степени 7, то степень одночлена $bx_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$ также должна быть равна 7. Кроме того, одночлен $x_1^3x_2^3x_3$ выше одночлена $bx_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$. Следовательно, система показателей этого одночлена может быть только (3, 2, 2), т.е. $\beta_1 = 3$, $\beta_2 = 2$, $\beta_3 = 2$, и данный одночлен имеет вид $bx_1^3x_2^2x_3^2$. Поскольку невозможно придумать систему показателей, чтобы соответствующий одночлен был ниже найденного, то получаем $g = \sigma_1^{3-3}\sigma_2^{3-1}\sigma_3^1 + b\sigma_1^{3-2}\sigma_2^{2-2}\sigma_3^2 = \sigma_2^2\sigma_3 + b\sigma_1\sigma_3^2$. Все эти вычисления удобно заносить в таблицу.

Система показателей	Высшие члены	Комбинации элементарных симметрических многочленов
(3, 3, 1)	$x_1^3x_2^3x_3$	$\sigma_1^{3-3}\sigma_2^{3-1}\sigma_3^1 = \sigma_2^2\sigma_3$
(3, 2, 2)	$bx_1^3x_2^2x_3^2$	$b\sigma_1^{3-2}\sigma_2^{2-2}\sigma_3^2 = b\sigma_2^2\sigma_3 = b\sigma_1\sigma_3^2$

Таким образом, $g = \sigma_2^2\sigma_3 + b\sigma_1\sigma_3^2$. Для нахождения коэффициента b берем, например, $x_1 = x_2 = x_3 = 1$. Тогда $g(1, 1, 1) = 3$, $\sigma_1(1, 1, 1) = 3$, $\sigma_2(1, 1, 1) = 3$, $\sigma_3(1, 1, 1) = 1$ и получаем $3 = 3^2 \cdot 1 + b \cdot 3 \cdot 1^2$, откуда $b = -2$ и $g = \sigma_2^2\sigma_3 - 2\sigma_1\sigma_3^2$.

Теперь займемся второй однородной компонентой данного симметрического многочлена $h(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + 5x_1x_2x_3$. Составим таблицу.

Система показателей	Высшие члены	Комбинации элементарных симметрических многочленов
(3, 0, 0)	x_1^3	$\sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0 = \sigma_1^3$
(2, 1, 0)	$ax_1^2x_2$	$a\sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 = a\sigma_1\sigma_2$
(1, 1, 1)	$bx_1x_2x_3$	$b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1 = b\sigma_3$

Таким образом, $h = \sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3$. Сначала полагаем $x_1 = x_2 = 1$, $x_3 = 0$, тогда $h(1, 1, 0) = 2$, $\sigma_1(1, 1, 0) = 2$, $\sigma_2(1, 1, 0) = 1$, $\sigma_3(1, 1, 0) = 0$. Получаем $2 = 2^3 + a \cdot 2 + 0$, $a = -3$. Следовательно, $h = \sigma_1^3 - 3\sigma_1\sigma_2 + b\sigma_3$. Затем полагаем $x_1 = x_2 = x_3 = 1$ и получаем $h(1, 1, 1) = 8$, $\sigma_1(1, 1, 1) = 3$, $\sigma_2(1, 1, 1) = 3$, $\sigma_3(1, 1, 1) = 1$, откуда $8 = 3^3 - 3 \cdot 3 \cdot 3 + b$, $b = 8$ и $h = \sigma_1^3 - 3\sigma_1\sigma_2 + 8\sigma_3$.

Ответ: $f = g + h = \sigma_2^2\sigma_3 - 2\sigma_1\sigma_3^2 + \sigma_1^3 - 3\sigma_1\sigma_2 + 8\sigma_3$.

Контрольные вопросы

1. Каково определяющее свойство симметрического многочлена?
2. Сколько существует элементарных симметрических многочленов от четырех переменных и каковы их степени?
3. Каковы высшие члены элементарных симметрических многочленов от четырех (пяти) переменных?
4. Каковы свойства элементарных симметрических многочленов, на базе которых доказывается основная теорема о симметрических многочленах?
5. Как формулируется основная теорема о симметрических многочленах?
6. В формулировке основной теоремы о симметрических многочленах $f(x_1, x_2, \ldots, x_n) = h(\sigma_1, \sigma_2, \ldots, \sigma_n)$ как связаны степень многочлена f и степени многочлена h относительно $\sigma_1, \sigma_2, \ldots, \sigma_n$ и относительно переменных $x_1, x_2, \ldots, x_n$?

Задачи

1. Составьте симметрический многочлен от трех переменных наименьшей степени, содержащий данное слагаемое, и представьте его лексикографической записью:

а) $3x_1x_2^3x_3^2$;
б) $x_1x_3^2$;
в) $x_1x_2x_3$;
г) x_3^3;
д) $x_1x_2^2x_3$;

е) x_1;
ж) $(x_1 + x_2)(x_1 + x_3)$.

2. Составьте цепочку одночленов от трех переменных строго убывающих по высоте, начинающуюся с данного одночлена:
а) x_1^3;
б) $x_1^5 x_2$;
в) $x_1 x_2^6 x_3$;
г) x_2^4;
д) $x_1^3 x_2^3 x_3^3$.

3. Расположите в порядке убывания по высоте все элементарные симметрические многочлены от четырех переменных.

4. Представьте в виде многочлена от элементарных симметрических многочленов данные симметрические многочлены от трех переменных:
а) $x_1^3 + x_2^3 + x_3^3 + 2x_1x_2x_3$;
б) $x_1^3x_2 + x_1^3x_3 + x_2^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2x_3^3$;
в) $x_1^4 + x_2^4 + x_3^4 + 3x_1^2x_2 + 3x_1^2x_3 + 3x_2^2x_3 + 3x_1x_2^2 + 3x_1x_3^2 + 3x_2x_3^2$;
г) $x_1^3x_2^2 + \ldots$;
д) $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$.

4.3. Некоторые приложения теории симметрических многочленов

4.3.1. Симметрические многочлены и формулы Виета

Рассмотрим пример.

Пример 4.3

Найдем сумму кубов корней многочлена $f(x) = x^3 + 2x^2 + x + 5$.

Решение. Пусть c_1, c_2, c_3 — корни данного многочлена. Нам нужно найти $c_1^3 + c_2^3 + c_3^3$, т.е. значение симметрического многочлена $h(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$ от корней данного многочлена. Сначала представляем многочлен $h(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$ в виде многочлена от элементарных симметрических многочленов. Для этого, как и в предыдущем примере, составляем соответствующую таблицу и получаем $h = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$ (проверьте!). По формулам Виета имеем $\sigma_1(c_1, c_2, c_3) = c_1 + c_2 + c_3 = -2$, $\sigma_2(c_1, c_2, c_3) = c_1c_2 + c_1c_3 + c_2c_3 = 1$, $\sigma_3(c_1, c_2, c_3) = c_1c_2c_3 = -5$. Следовательно,

$$c_1^3 + c_2^3 + c_3^3 = h(c_1, c_2, c_3) =$$
$$= (\sigma_1(c_1, c_2, c_3))^3 - 3\sigma_1(c_1, c_2, c_3) \cdot \sigma_2(c_1, c_2, c_3) + 3\sigma_3(c_1, c_2, c_3) =$$
$$= (-2)^3 - 3(-2) + 3(-5) = -17.$$

Обобщая ситуацию рассмотренного примера, получаем следующее утверждение.

***Следствие* (*из основной теоремы о симметрических многочленах*).** Пусть дан многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ над полем P. Пусть поле P_1 содержит поле P и все корни данного многочлена $c_1, c_2, \ldots, c_n$. Тогда для любого симметрического многочлена $h(x_1, x_2, \ldots, x_n) \in P[x_1, x_2, \ldots, x_n]$ значение этого многочлена от корней данного многочлена в поле P_1 принадлежит полю P, т.е. $h(c_1, c_2, \ldots, c_n) \in P$.

Доказательство. По основной теореме о симметрических многочленах для симметрического многочлена $h(x_1, x_2, \ldots, x_n)$ существует многочлен $g(y_1, y_2, \ldots, y_n) \in P[y_1, y_2, \ldots, y_n]$, такой что $h = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$. В то же время по формулам Виета получаем

$$\sigma_1(c_1, c_2, \ldots, c_n) = c_1 + c_2 + \ldots + c_n = -\frac{a_{n-1}}{a_n} \in P,$$

$$\sigma_2(c_1, c_2, \ldots, c_n) = c_1c_2 + c_1c_3 + \ldots + c_{n-1}c_n = \frac{a_{n-2}}{a_n} \in P,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n(c_1, c_2, \ldots, c_n) = c_1c_2\cdots c_n = (-1)^n \frac{a_0}{a_n} \in P.$$

Следовательно, $h(c_1, c_2, \ldots, c_n) = g(\sigma_1(c_1, \ldots, c_n), \ldots, \sigma_n(c_1, \ldots, c_n)) \in P$.

4.3.2. Степенные суммы и формулы Ньютона

Определение 4.4. *Степенными суммами* от n переменных называются многочлены $s_k = x_1^k + x_2^k + \ldots + x_n^k$ для $k = 0, 1, \ldots$.

Выведем формулы Ньютона, связывающие степенные суммы и элементарные симметрические многочлены. Рассмотрим многочлен $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$. Его можно представить в виде $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots + (-1)^n\sigma_n$, где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — элементарные симметрические многочлены от переменных $x_1, x_2, \ldots, x_n$. Отсюда

$$f'(x) = nx^{n-1} - \sigma_1(n-1)x^{n-2} + \sigma_2(n-2)x^{n-3} - \ldots + (-1)^{n-1}\sigma_{n-1}.$$

С другой стороны, индукцией по n легко доказать, что

$$f'(x) = (x - x_2)(x - x_3)\cdots(x - x_n) + (x - x_1)(x - x_3)\cdots(x - x_n) + \ldots +$$
$$+ (x - x_1)(x - x_2)\cdots(x - x_{n-1}) = \frac{f(x)}{x - x_1} + \frac{f(x)}{x - x_2} + \ldots + \frac{f(x)}{x - x_n}.$$

По схеме Горнера разделим $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots + (-1)^n \sigma_n$ на $x - x_i$ для $i = 1, 2, \ldots, n$.

	1	$-\sigma_1$	σ_2	...	$(-1)^{n-1}\sigma_{n-1}$
x_i	1	$x_i - \sigma_1$	$x_i^2 - \sigma_1 x_i + \sigma_2$	...	$x_i^{n-1} - \sigma_1 x_i^{n-2} + \ldots + (-1)^{n-2}\sigma_{n-2} x_i + (-1)^{n-1}\sigma_{n-1}$

Таким образом,

$$\frac{f(x)}{x - x_i} = x^{n-1} + (x_i - \sigma_1)x^{n-2} + (x_i^2 - \sigma_1 x_i + \sigma_2)x^{n-3} + \ldots + x_i^{n-1} - \sigma_1 x_i^{n-2} + \ldots + (-1)^{n-2}\sigma_{n-2} x_i + (-1)^{n-1}\sigma_{n-1}.$$

Суммируя равенства по i от 1 до n, находим

$$f'(x) = nx^{n-1} + (s_1 - n\sigma_1)x^{n-2} + (s_2 - \sigma_1 s_1 + n\sigma_2)x^{n-3} + \ldots + s_{n-1} - \sigma_1 s_{n-2} + \ldots + (-1)^{n-2}\sigma_{n-2} s_1 + (-1)^{n-1} n\sigma_{n-1}.$$

Приравнивая соответствующие коэффициенты, получаем формулы Ньютона:

$$s_1 - n\sigma_1 = -\sigma_1(n-1) \Rightarrow s_1 - \sigma_1 = 0,$$

$$s_2 - \sigma_1 s_1 + n\sigma_2 = \sigma_2(n-2) \Rightarrow s_2 - \sigma_1 s_1 + 2\sigma_2 = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{n-1} - \sigma_1 s_{n-2} + \ldots + (-1)^{n-2}\sigma_{n-2} s_1 + (-1)^{n-1} n\sigma_{n-1} = (-1)^{n-1}\sigma_{n-1} \Rightarrow$$

$$\Rightarrow s_{n-1} - \sigma_1 s_{n-2} + \ldots + (-1)^{n-2}\sigma_{n-2} s_1 + (-1)^{n-1}(n-1)\sigma_{n-1} = 0.$$

Теперь выведем аналогичные формулы для степенных сумм s_k при $k \geq n$. Для любого $i = 1, 2, \ldots, n$ имеем равенство

$$f(x) = x_i^n - \sigma_1 x_i^{n-1} + \sigma_2 x_i^{n-2} - \ldots + (-1)^n \sigma_n = f(x_i) = 0.$$

Умножив на x_i^{k-n}, получим

$$x_i^k - \sigma_1 x_i^{k-1} + \sigma_2 x_i^{k-2} - \ldots + (-1)^n \sigma_n x_i^{k-n} = 0.$$

Просуммировав по i, будем иметь

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} - \ldots + (-1)^n \sigma_n s_{k-n} = 0. \qquad (4.1)$$

Пользуясь полученными соотношениями, можно последовательно выражать степенные суммы через элементарные симме-

трические многочлены. Например, при $n = 2$ получаем $s_1 = \sigma_1$, теперь по формуле (4.1) при $k = 2$ имеем $s_2 - \sigma_1 s_1 + \sigma_2 s_0 = 0$, откуда $s_2 = \sigma_1 s_1 - \sigma_2 s_0 = \sigma_1^2 - 2\sigma_2$, снова по той же формуле при $k = 3$ получаем $s_3 - \sigma_1 s_2 + \sigma_2 s_1 = 0$, откуда $s_3 = \sigma_1 s_2 - \sigma_2 s_1 = \sigma_1(\sigma_1^2 - 2\sigma_2) - \sigma_2\sigma_1 = \sigma_1^3 - 3\sigma_1\sigma_2$.

Упражнение 4.1. Продолжите приведенные вычисления до $k = 7$. Выпишите аналогичные формулы при $n = 3$ до $k = 5$.

4.3.3. Решение систем двух симметрических уравнений с двумя неизвестными

Иногда систему двух симметрических уравнений с двумя неизвестными удается решить, выражая соответствующие многочлены через элементарные симметрические многочлены $\sigma_1(x_1, x_2)$, $\sigma_2(x_1, x_2)$ и решая сначала полученную систему относительно σ_1 и σ_2, а затем находя x_1 и x_2 как корни квадратного уравнения, составленного по найденным σ_1 и σ_2. Рассмотрим соответствующий пример.

Пример 4.4

Решим систему уравнений

$$\begin{cases} x_1^4 + x_2^4 = 17, \\ x_1 + x_2 = 3. \end{cases}$$

Решение. Представим симметрический многочлен $x_1^4 + x_2^4$ в виде многочлена от элементарных симметрических многочленов:

$$x_1^4 + x_2^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$$

проверьте!). Приходим к системе

$$\begin{cases} \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 = 17, \\ \sigma_1 = 3. \end{cases}$$

Отсюда подстановкой получаем уравнение $\sigma_2^2 - 18\sigma_2 + 32 = 0$. Решая его, находим корни: $\sigma_2 = 16$ или $\sigma_2 = 2$. Получаем две системы:

$$\begin{cases} \sigma_1 = 3, \\ \sigma_2 = 16; \end{cases} \quad \begin{cases} \sigma_1 = 3, \\ \sigma_2 = 2. \end{cases}$$

Рассмотрим первую систему. Поскольку $x_1 + x_2 = 3$, $x_1 \cdot x_2 = 16$, то x_1 и x_2 являются корнями квадратного уравнения $x^2 - 3x + 16 = 0$. Решая это уравнение, обнаруживаем, что оно не имеет действительных корней. Рассматривая аналогично вторую систему, получаем $x_1 = 1, x_2 = 2$ или $x_1 = 2, x_2 = 1$.

Придумаем новую систему уравнений, аналогичную предыдущей. Положим $x_1 = 5$, $x_2 = -3$. Тогда

$$\begin{cases} x_1^4 + x_2^4 = 706, \\ x_1 + x_2 = 2. \end{cases}$$

Упражнение 4.2. Решите полученную систему уравнений относительно неизвестных x_1 и x_2. Исчерпываются ли решения системы исходными значениями неизвестных?

4.3.4. Решение некоторых иррациональных уравнений

Иногда решение иррационального уравнения удается свести к решению системы двух симметрических уравнений с двумя переменными.

Пример 4.5

Решим иррациональное уравнение $\sqrt[4]{x+8} + \sqrt[4]{9-x} = 3$.

Решение. Напрашиваются обозначения: $x_1 = \sqrt[4]{x+8}$, $x_2 = \sqrt[4]{9-x}$. В этих обозначениях получаем систему двух симметрических уравнений

$$\begin{cases} x_1^4 + x_2^4 = 17, \\ x_1 + x_2 = 3. \end{cases}$$

Эта система решена в примере 4.4: $x_1 = 1, x_2 = 2$ или $x_1 = 2, x_2 = 1$. В первом случае получаем $x_1 = \sqrt[4]{x+8} = 1$, откуда $x + 8 = 1$, $x = -7$. Значение $x_2 = 2$ приводит к тому же результату. При $x_1 = 2$ получаем $\sqrt[4]{x+8} = 2$, откуда $x + 8 = 16$ и $x = 8$. Случай $x_2 = 1$ приводит к этому же результату.

Ответ: $x = -7$ или $x = 8$.

Пример 4.6

Решим иррациональное уравнение

$$\sqrt{x^2 - 3x + 2}(4 + 3x - x^2) + \sqrt{4 + 3x - x^2}(x^2 - 3x + 2) = \frac{9}{2}.$$

Решение. Напрашиваются обозначения $x_1 = \sqrt{x^2 - 3x + 2}$, $x_2 = \sqrt{4 + 3x - x^2}$. В этих обозначениях получаем систему двух симметрических уравнений

$$\begin{cases} x_1 x_2^2 + x_1^2 x_2 = \frac{9}{2}, \\ x_1^2 + x_2^2 = 6. \end{cases}$$

Как и в предыдущем примере, выразив каждый симметрический многочлен через элементарные симметрические многочлены, получим

$$\begin{cases}\sigma_1\sigma_2 = \dfrac{9}{2},\\ \sigma_1^2 - 2\sigma_2 = 6.\end{cases}$$

Из второго уравнения находим $\sigma_2 = \dfrac{\sigma_1^2 - 6}{2}$ и, подставляя в первое уравнение, получаем $\sigma_1^3 - 6\sigma_1 - 9 = 0$. Единственным действительным корнем этого уравнения будет $\sigma_1 = 3$. Тогда $\sigma_2 = \dfrac{3}{2}$. Отсюда следует, что x_1 и x_2 являются корнями квадратного уравнения $y^2 - 3y + \dfrac{3}{2} = 0$. Решая его, находим корни $y_1 = \dfrac{3}{2} + \dfrac{\sqrt{3}}{2}$, $y_2 = \dfrac{3}{2} - \dfrac{\sqrt{3}}{2}$. Замечаем, что $\dfrac{3}{2} \pm \dfrac{\sqrt{3}}{2} > 0$. Следовательно,

$$\begin{cases}x_1 = \dfrac{3}{2} + \dfrac{\sqrt{3}}{2},\\ x_2 = \dfrac{3}{2} - \dfrac{\sqrt{3}}{2}\end{cases} \text{ либо } \begin{cases}x_1 = \dfrac{3}{2} - \dfrac{\sqrt{3}}{2},\\ x_2 = \dfrac{3}{2} + \dfrac{\sqrt{3}}{2}.\end{cases}$$

В первом случае имеем $x_1 = \sqrt{x^2 - 3x + 2} = \dfrac{3}{2} + \dfrac{\sqrt{3}}{2}$, откуда $x^2 - 3x + 2 = \dfrac{9}{4} + \dfrac{3\sqrt{3}}{2} + \dfrac{3}{4}$. Получаем уравнение $x^2 - 3x - 1 - \dfrac{3\sqrt{3}}{2} = 0$. Второе уравнение первой системы приводит к тому же. Решая уравнение, находим $x = \dfrac{3}{2} \pm \sqrt{\dfrac{9}{4} + 1 + \dfrac{3\sqrt{3}}{2}} = \dfrac{3 \pm \sqrt{13 + 6\sqrt{3}}}{2}$. Вторая система приводит к уравнению $x^2 - 3x - 1 + \dfrac{3\sqrt{3}}{2} = 0$, что дает

$$x = \frac{3}{2} \pm \sqrt{\frac{9}{4} + 1 - \frac{3\sqrt{3}}{2}} = \frac{3 \pm \sqrt{13 - 6\sqrt{3}}}{2}.$$

Ответ: $x = \dfrac{3 + \sqrt{13 + 6\sqrt{3}}}{2}$, или $x = \dfrac{3 - \sqrt{13 + 6\sqrt{3}}}{2}$, или $x = \dfrac{3 + \sqrt{13 - 6\sqrt{3}}}{2}$, или $x = \dfrac{3 - \sqrt{13 - 6\sqrt{3}}}{2}$.

Контрольные вопросы

1. Верно ли, что значение элементарного симметрического многочлена от корней данного многочлена принадлежит полю, над которым рассматривается данный многочлен?

2. Какое применение в школьной математике находит теория симметрических многочленов?

3. Как школьными методами вывести последовательно формулы для степенных сумм от двух переменных?

4. Какова связь между элементарными симметрическими многочленами и формулами Виета?

5. Всякую ли систему двух симметрических уравнений с двумя переменными можно решить, используя теорию симметрических многочленов?

Задачи

1. Выразите через элементарные симметрические многочлены степенные суммы:

а) $x_1^2 + x_2^2 + x_3^2$;

б) $x_1^3 + x_2^3 + x_3^3$;

в) $x_1^4 + x_2^4 + x_3^4$;

г) $x_1^5 + x_2^5 + x_3^5$.

2. Найдите значение данного симметрического многочлена от корней многочлена $h(x)$:

а) $x_1x_2^3 + x_1x_3^3 + x_2x_3^3 + x_1^3x_2 + x_1^3x_3 + x_2^3x_3$, $h(x) = 3x^3 - 6x^2 + 3x + 6$;

б) $(3x_1 - x_2 - x_3)(3x_2 - x_1 - x_3)(3x_3 - x_1 - x_2)$, $h(x) = x^3 + 2x^2 + 3x + 3$;

в) $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$, $h(x) = 2x^3 - 4x^2 + 3x - 2$.

3. Найдите значения элементарных симметрических многочленов от комплексных корней n-й степени из единицы.

4. Решите системы симметрических уравнений:

а) $\begin{cases} x + y = \dfrac{5}{6}, \\ \dfrac{1}{x^2y} + \dfrac{1}{xy^2} = 30; \end{cases}$

б) $\begin{cases} \dfrac{x}{y^2} + \dfrac{y}{x^2} = 18, \\ \dfrac{1}{x} + \dfrac{1}{y} = 12; \end{cases}$

в) $\begin{cases} \dfrac{1}{x^4} + \dfrac{1}{x^2} + \dfrac{1}{y^4} + \dfrac{1}{y^2} = 92, \\ xy = \dfrac{1}{3}; \end{cases}$

г) $\begin{cases} \dfrac{x}{x^3} + \dfrac{1}{x^3y^3} + \dfrac{1}{y^3} = 17, \\ \dfrac{1}{x} + \dfrac{1}{xy} + \dfrac{1}{y} = 0. \end{cases}$

5. Решите иррациональные уравнения:

а) $x+\sqrt{25-x^2}+x\sqrt{25-x^2}=19$;

б) $12(\sqrt{1-x^2}+x)-35x\sqrt{1-x^2}=0$;

в) $(x^2-2x+4)\sqrt{9+2x-x^2}+(9+2x-x^2)\sqrt{x^2-2x+4}=30$.

6. Составьте квадратное уравнение, корнями которого являются (квадраты) кубы корней данного многочлена:

а) $x^2 - 3x + 5$;

б) $x^3 + 2x - 1$.

7. Найдите сумму пятых степеней корней многочлена $x^6 + 2x^5 - 5x^4 - 17x^3 - 20x^2 - 12x - 2$.

4.4. Основная теорема алгебры

4.4.1. Краткая историческая справка

Напомним происхождение самого слова «алгебра». В IX в. в г. Хивы, входившем в Хорезмское ханство, жил выдающийся узбекский ученый ал-Хорезми Абу Абдулла Мухаммед ибн Мусса аль Маджуси. В историю математики он вошел под именем аль-Хорезми. Он написал много книг по математике и астрономии. Латинизированное имя этого математика — Algoritmus — является истоком термина «алгоритм». Его книга по решению линейных и квадратных уравнений называлась «Хисаб аль-джебр ва аль-мукабала», что в переводе означает «исчисление восполнения и противопоставления». В ней он вводит правила переноса слагаемых из одной части уравнения в другую с изменением знака. Эта книга в Европе стала известна в латинском переводе, а от слова «аль-джебр» и произошло слово «алгебра» — так стали называть науку об уравнениях.

В связи с решением кубических уравнений появились комплексные числа. Когда уже научились решать уравнения не только третьей, но и четвертой степени и искали общие приемы решения уравнений более высоких степеней, появилась настоятельная потребность установить: а имеет ли хоть какое-то необязательно формульное решение произвольное уравнение с комплексными коэффициентами? Или комплексные числа придется снова расширять, присоединяя, быть может, корни какого-нибудь уравнения, не имеющего корней среди комплексных чисел? Конечно же, теорему, которая решала этот вопрос, сразу назвали «основной теоремой алгебры». Теперь ее чаще всего называют более скромно: «основ-

ной теоремой алгебры комплексных чисел», или «теоремой об алгебраической замкнутости поля комплексных чисел».

Несмотря на столь громкое название, основная теорема алгебры не имеет чисто алгебраического доказательства, поскольку использует свойства непрерывности, которые изучает математический анализ.

Впервые высказанная А. Жираром в 1629 г., первое строгое доказательство она получила в 1799 г. в Гельмштадской диссертации К. Ф. Гаусса (1777—1855). Во всех предыдущих доказательствах предполагалось заранее, что какие-то «идеальные» корни многочлена существуют, а затем доказывалось, что по крайней мере один из них является комплексным числом. К. Гаусс первый дал доказательство без предположения, что корни существуют. Его доказательство, по существу, содержало построение поля разложения многочлена. Ниже мы приведем «самое алгебраическое» доказательство основной теоремы алгебры, четко выделяя момент использования непрерывности.

4.4.2. Доказательство основной теоремы алгебры

Сначала докажем теорему для многочленов с действительными коэффициентами.

Теорема 4.2. *Всякий многочлен с действительными коэффициентами* $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ *степени* $n \geq 1$ *имеет по крайней мере один комплексный корень.*

Доказательство. Пусть $n = 2^m n_0$, где n_0 нечетно. Докажем теорему индукцией по m.

1. Начало индукции. Пусть $m = 0$. Тогда $n = n_0$, т.е. степень данного многочлена $f(x)$ нечетна. Лемма о модуле старшего члена многочлена гласит, что при достаточно больших $|x|$ модуль старшего члена многочлена $|x^n|$ во сколько угодно раз больше модуля суммы остальных членов этого многочлена. Следовательно, для достаточно больших $|x|$ знак многочлена совпадает со знаком его старшего члена. Поскольку степень нашего многочлена нечетна, то для отрицательных достаточно больших по модулю значений x значение многочлена отрицательно, а для положительных достаточно больших по модулю значений x значение многочлена положительно. При вычерчивании графика непрерывной функции $f(x)$, переходя из нижней полуплоскости в верхнюю полуплоскость, мы обязательно пересечем ось абсцисс. Другими словами, найдется такое значение переменной $x = x_0$, что $f(x_0) = 0$. Так что в этом случае мы находим даже действительный корень многочлена.

Строго говоря, здесь мы опираемся на теорему Больцано — Коши[1]: *пусть функция $f(x)$ определена и непрерывна в замкнутом промежутке $[a; b]$ и на концах этого промежутка принимает значения разных знаков. Тогда между a и b найдется точка c, в которой $f(c) = 0$.*

2. Шаг индукции. Пусть теорема верна для всех многочленов с действительными коэффициентами, чья степень равна $2^{m-1}n_0'$, где n_0' нечетно. Докажем, что теорема верна для многочлена $f(x)$ степени $n = 2^m n_0$, где n_0 нечетно. Обозначим через F поле, содержащее поле комплексных чисел и все корни данного многочлена. Над этим полем данный многочлен $f(x)$ можно разложить на линейные множители: $f(x) = (x - u_1)(x - u_2)\cdots(x - u_n)$, $u_1, u_2, \ldots, u_n \in F$. Зафиксируем некоторое действительное число a и образуем элементы

$$v_{12} = u_1u_2 + a(u_1 + u_2),$$

$$v_{13} = u_1u_3 + a(u_1 + u_3),$$

$$\ldots\ldots\ldots\ldots$$

$$v_{n-1\,n} = u_{n-1}u_n + a(u_{n-1} + u_n).$$

Общий вид таких элементов $v_{ij} = u_iu_j + a(u_i + u_j)$, $1 \le i < j \le n$. Количество этих элементов обозначим через k. Очевидно,

$$k = C_n^2 = \frac{n(n-1)}{2} = \frac{2^m n_0(2^m n_0 - 1)}{2} = 2^{m-1}k_0',$$

где $k_0' = n_0(2^m n_0 - 1)$ — нечетное натуральное число.

Образуем многочлен $f_a(z) = (z - v_{12})(z - v_{13})\cdots(z - v_{n-1\,n}) \in F[z]$. Раскрывая скобки и приводя подобные, получаем $f_a(z) = z^k + b_{k-1}z^{k-1} + \ldots + b_1z + b_0$, где по формулам Виета

$$b_{k-1} = -\sigma_1(v_{12}, v_{13}, \ldots, v_{n-1\,n}),$$

$$b_{k-2} = \sigma_2(v_{12}, v_{13}, \ldots, v_{n-1\,n}),$$

$$\ldots\ldots\ldots\ldots$$

$$b_1 = (-1)^{k-1}\sigma_{k-1}(v_{12}, v_{13}, \ldots, v_{n-1\,n}),$$

$$b_0 = (-1)^k\sigma_k(v_{12}, v_{13}, \ldots, v_{n-1\,n}).$$

---

[1] См.: *Фихтенгольц Г. М.* Основы математического анализа. Т. 1. М. : Наука, 1968. С. 128.

Другими словами, коэффициенты b_{k-1}, b_{k-2}, ..., b_1, b_0 с точностью до знака совпадают со значениями элементарных симметрических многочленов σ_1, σ_2, ..., σ_k от v_{12}, v_{13}, ..., $v_{n-1\,n}$. Подставляя в формулы для коэффициентов выражения v_{ij} через u_i, u_j, получаем $b_{k-t} = h_t(u_1, u_2, ..., u_n)$, $t = 1, 2, ..., k$.

Считая u_1, u_2, ..., u_n переменными, докажем, что для любого $t = 1, 2, ..., k$ многочлен $h_t(u_1, u_2, ..., u_n)$ является симметрическим. Возьмем произвольную подстановку индексов $s = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ и посмотрим, как преобразуется v_{ij} при перестановке переменных u_1, u_2, ..., u_n согласно этой подстановке. Не нарушая общности, можно выбрать v_{12}. Итак, имеем

$$v_{12} = u_1u_2 + a(u_1 + u_2) \xrightarrow{s} u_{i_1}u_{i_2} + a(u_{i_1} + u_{i_2}) = v_{i_1i_2}.$$

Таким образом, при любой перестановке переменных u_1, u_2, ..., u_n переменные v_{12}, v_{13}, ..., $v_{n-1\,n}$ переходят друг в друга. Но, как отмечалось выше, многочлен $h_t(u_1, u_2, ..., u_n) = b_{k-t}$ с точностью до знака совпадает с элементарным симметрическим многочленом от переменных v_{12}, v_{13}, ..., $v_{n-1\,n}$. Отсюда следует, что $h_t(u_1, u_2, ..., u_n)$ является симметрическим многочленом от переменных u_1, u_2, ..., u_n.

Вспомним теперь, что u_1, u_2, ..., u_n есть корни многочлена $f(x) \in \mathbb{R}[x]$, а по следствию из основной теоремы о симметрических многочленах значение симметрического многочлена от корней данного многочлена принадлежит полю коэффициентов данного многочлена, т.е. полю $\mathbb{R}$. Следовательно, коэффициент $b_{k-t} = h_t(u_1, u_2, ..., u_n)$ является действительным числом и многочлен $f_a(z) = z^k + b_{k-1}z^{k-1} + ... + b_1z + b_0$ является многочленом с действительными коэффициентами. Степень этого многочлена равна $k = 2^{m-1}k_0$, и по индуктивному предположению многочлен $f_a(z)$ имеет по крайней мере один комплексный корень. Другими словами, среди элементов v_{12}, v_{13}, ..., $v_{n-1\,n}$ есть хотя бы одно комплексное число. Вспомним, что $v_{ij} = u_iu_j + a(u_i + u_j)$, и при каждом значении параметра $a \in \mathbb{R}$ среди элементов системы v_{12}, v_{13}, ..., $v_{n-1\,n}$ есть хотя бы одно комплексное число. Поскольку пар индексов (i, j), где $1 \le i < j \le n$, конечное число, а множество значений параметра a бесконечно, то найдутся два различных значения этого параметра a_1 и a_2 и пара индексов (i, j), такие что

$$c_1 = u_iu_j + a_1(u_i + u_j),\ c_2 = u_iu_j + a_2(u_i + u_j) \qquad (4.2)$$

являются комплексными числами. Вычитая из первого равенства второе, получаем $c_1 - c_2 = (a_1 - a_2)(u_i + u_j)$, откуда $u_i + u_j = \frac{c_1 - c_2}{a_1 - a_2} \in \mathbb{C}$. Далее найдем из равенств (4.2) произведение $u_1 u_2$. Для этого первое равенство умножим на a_2, а второе — на a_1. Получим $c_1 a_2 = a_2 u_i u_j + a_1 a_2 (u_i + u_j)$, $a_1 c_2 = a_1 u_i u_j + a_1 a_2 (u_i + u_j)$. Вычитая из первого равенства второе, будем иметь $c_1 a_2 - a_1 c_2 = (a_2 - a_1) u_i u_j$, откуда $u_i u_j = \frac{c_1 a_2 - a_1 c_2}{a_2 - a_1} \in \mathbb{C}$. Таким образом, элементы u_i и u_j являются корнями квадратного уравнения с комплексными коэффициентами

$$z^2 - (u_i + u_j) z + u_i u_j = 0$$

и находятся по формуле

$$u_{i,j} = \frac{u_i + u_j}{2} \pm \sqrt{\frac{(u_i + u_j)^2}{4} - u_i u_j}.$$

Отсюда делаем вывод, что числа u_i и u_j являются комплексными. Тем самым мы нашли два комплексных корня данного многочлена $f(x)$. Теорема доказана.

Теорема 4.3 (основная теорема алгебры). *Всякий многочлен $f(z)$ с комплексными коэффициентами степени $n \geq 1$ имеет хотя бы один комплексный корень.*

Доказательство. Пусть $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$, где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{C}$. Рассмотрим многочлен, коэффициенты которого сопряжены с соответствующими коэффициентами данного многочлена: $f_1(z) = \overline{a}_n z^n + \overline{a}_{n-1} z^{n-1} + \ldots + \overline{a}_1 z + \overline{a}_0$, и найдем произведение этих многочленов. Это будет многочлен степени $2n$ вида

$$g(z) = f(z) \cdot f_1(z) = d_{2n} z^{2n} + d_{2n-1} z^{2n-1} + \ldots + d_1 z + d_0,$$

где $d_k = a_k \overline{a}_0 + a_{k-1} \overline{a}_1 + \ldots + a_1 \overline{a}_{k-1} + a_0 \overline{a}_k$, $k = 0, 1, \ldots, 2n$. Легко видеть, что $\overline{d}_k = d_k$, следовательно, d_k является действительным числом. Итак, $g(z)$ является многочленом с действительными коэффициентами и по теореме 4.2 имеет некоторый комплексный корень z_0. Но тогда $0 = g(z_0) = f(z_0) \cdot f_1(z_0)$, откуда $f(z_0) = 0$ или $f_1(z_0) = 0$. В первом случае z_0 — искомый комплексный корень данного многочлена $f(z)$. Во втором случае, как легко видеть, $\overline{z}_0$ является комплексным корнем многочлена $f(z)$. Теорема доказана.

4.4.3*. Существование поля разложения данного многочлена

Устраним пробел в доказательстве основной теоремы алгебры и докажем существование поля, содержащего все корни данного многочлена[1].

Напомним, что если поле P является подполем поля F, то поле F называется *расширением* поля P.

Теорема 4.4. *Пусть многочлен $\varphi(x)$ неприводим над полем P. Существует расширение F поля P, содержащее хотя бы один корень многочлена $\varphi(x)$.*

Доказательство. Рассмотрим множество всех многочленов кольца $P[x]$, кратных многочлену $\varphi(x)$: $\{f(x)\cdot\varphi(x) \mid f(x)\in P[x]\}$.

Это множество многочленов называется *идеалом, порожденным многочленом* $\varphi(x)$, и обозначается $\langle\varphi(x)\rangle$. Легко доказать, что это множество многочленов замкнуто относительно сложения и умножения на любой многочлен кольца $P[x]$.

Будем говорить, что многочлены $g(x)$ и $h(x)$ *сравнимы по идеалу* $\langle\varphi(x)\rangle$, если их разность $g(x)-h(x)\in\langle\varphi(x)\rangle$. Легко проверяется, что отношение сравнимости по идеалу рефлексивно, симметрично и транзитивно, т.е. является отношением эквивалентности. По этому отношению множество всех многочленов кольца $P[x]$ разбивается на непересекающиеся классы, которые называются *смежными классами по идеалу* $\langle\varphi(x)\rangle$. Класс эквивалентных элементов, содержащий многочлен $h(x)\in P[x]$, имеет вид $h(x)+\langle\varphi(x)\rangle=\{h(x)+f(x)\cdot\varphi(x) \mid f(x)\in P[x]\}$. Для удобства введем обозначение $\overline{h(x)}=h(x)+\langle\varphi(x)\rangle$ для любого $h(x)\in P[x]$. Множество всех смежных классов обозначим через F. Таким образом, $F=\{\overline{h(x)} \mid h(x)\in P[x]\}$.

Определим сложение и умножение элементов множества F, положив

$$\overline{f(x)}+\overline{g(x)}=\overline{f(x)+g(x)},\ \overline{f(x)}\cdot\overline{g(x)}=\overline{f(x)\cdot g(x)}$$

для любых $\overline{f(x)},\overline{g(x)}\in F$. Можно доказать, что сумма и произведение смежных классов не зависят от выбора представителей этих классов. Легко видеть, что F является кольцом с нулем $\overline{0}=0+\langle\varphi(x)\rangle=\langle\varphi(x)\rangle$ и единицей $\overline{1}=1+\langle\varphi(x)\rangle$.

---

[1] Обычно этот материал рассматривается в следующем, заключительном семестре курса алгебры, в теме «Расширения полей» (см. работу [8]). Мы приводим его здесь для «алгебраической замкнутости» изложения. Поэтому доказательства будут даны несколько конспективно и восстановление опущенных деталей можно рассматривать как упражнения.

Докажем, что F является полем. Пусть $\overline{g(x)} \neq \overline{0}$. Другими словами, $g(x) + \langle\varphi(x)\rangle \neq \langle\varphi(x)\rangle$. Это означает, что $g(x) \notin \langle\varphi(x)\rangle$, что в свою очередь означает, что $g(x)$ не делится на $\varphi(x)$. По свойству неприводимого многочлена отсюда следует, что НОД$(g(x), \varphi(x)) = 1$. Но тогда существуют многочлены $u(x), v(x) \in P[x]$, такие что $g(x)u(x) + \varphi(x)v(x) = 1$. Отсюда $g(x)u(x) = 1 - \varphi(x)v(x)$, а значит, $(g(x) + \langle\varphi(x)\rangle) \cdot (u(x) + \langle\varphi(x)\rangle) = 1 + \langle\varphi(x)\rangle$. Используя обозначения, получаем $\overline{g(x)} \cdot \overline{u(x)} = \overline{1}$. Это означает, что элемент $\overline{g(x)}$ обратим. Следовательно, кольцо F является полем.

Пусть $\varphi(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, где $b_n, b_{n-1}, \ldots, b_1, b_0 \in P$ и $\overline{\varphi}(x) = \overline{b_n}x^n + \overline{b_{n-1}}x^{n-1} + \ldots + \overline{b_1}x + \overline{b_0}$. Непосредственной проверкой убеждаемся, что корнем этого многочлена в поле F будет элемент $\overline{x} = x + \langle\varphi(x)\rangle$. Таким образом, поле F является расширением поля $\overline{P} = \{\overline{a} \mid a \in \overline{P}\}$ и содержит корень $\overline{x}$ многочлена $\overline{\varphi}(x)$. Поскольку произвольным элементам $a, b \in P$ соответствуют элементы $\overline{a}, \overline{b} \in \overline{P}$, так что сумме $a + b$ соответствует сумма $\overline{a} + \overline{b}$ и произведению $a \cdot b$ соответствует произведение $\overline{a} \cdot \overline{b}$ в поле $\overline{P}$, то поле P можно отождествить с полем $\overline{P}$, а многочлен $\varphi(x)$ — с многочленом $\overline{\varphi}(x)$. С точностью до таких обозначений можно считать, что поле F содержит поле P и корень многочлена $\varphi(x) \in P[x]$. Теорема доказана.

Теорема 4.5. *Для всякого многочлена $f(x)$ степени $n \geq 1$ над полем P существует расширение этого поля F, содержащее все корни данного многочлена* (поле разложения многочлена $f(x)$).

Доказательство. Данный многочлен $f(x)$ степени $n \geq 1$ над полем P можно представить в виде произведения неприводимых над P множителей. Пусть $f(x) = \varphi(x)h(x)$, где многочлен $\varphi(x)$ неприводим над P. По теореме 4.4 существует расширение F_1 поля P, содержащее некоторый корень c_1 многочлена $\varphi(x)$. Тогда над полем F_1 имеем разложение $\varphi(x) = (x - c_1)g(x)$, где $g(x) \in F_1[x]$. Отсюда $f(x) = (x - c_1)g(x)h(x) = (x - c_1)f_1(x)$, где $f_1(x) \in F_1[x]$. Если многочлен $f_1(x)$ имеет степень 0, то $f_1(x) = a \in F_1$ и $f(x) = a(x - c_1)$ — искомое разложение многочлена $f(x)$ на линейные множители, а F_1 — искомое поле разложения данного многочлена. Если же многочлен $f_1(x)$ имеет степень ≥ 1, то повторим для него рассуждения и получим поле F_2, являющееся расширением поля F_1, такое что $f_1(x) = (x - c_2)f_2(x)$ для некоторого $c_2 \in F_2$ и $f_2(x) \in F_2[x]$. Отсюда $f(x) = (x - c_1)(x - c_2)f_2(x)$. Через конечное число шагов получим искомое поле разложения данного многочлена.

Контрольные вопросы

1. Как наглядно-геометрически сформулировать свойство непрерывности, которое используется в приведенном выше доказательстве основной теоремы алгебры?
2. Какое утверждение для многочленов с действительными коэффициентами лежит в основе приведенного выше доказательства основной теоремы алгебры?
3. Какие свойства симметрических многочленов используются в приведенном выше доказательстве основной теоремы алгебры?
4. Каковы неприводимые многочлены над полем комплексных чисел и как выглядит над этим полем разложение всякого многочлена в произведение неприводимых множителей?
5. Как можно трактовать значение основной теоремы алгебры в связи с решением уравнений?

Задачи

В задачах заполняются пробелы в доказательстве теоремы 4.4.

1. Зафиксируем многочлен $\varphi(x)$ над полем P и рассмотрим множество многочленов $\langle\varphi(x)\rangle = \{f(x)\cdot\varphi(x) \mid f(x)\in P[x]\}$, называемое идеалом, порожденным многочленом $\varphi(x)$, и обозначаемое $\langle\varphi(x)\rangle$. Докажите, что множество многочленов $\langle\varphi(x)\rangle$ замкнуто относительно сложения многочленов и умножения на любой многочлен кольца $P[x]$, т.е. для любых многочленов $g(x)$, $h(x)\in\langle\varphi(x)\rangle$ $g(x)+h(x)\in\langle\varphi(x)\rangle$ и для любого многочлена $f(x)\in P[x]$ $f(x)\cdot g(x)\in\langle\varphi(x)\rangle$.

2. Для любых многочленов $f(x), g(x)\in P[x]$ определим $f(x)\sim g(x)\Leftrightarrow$ $\Leftrightarrow f(x)-g(x)\in\langle\varphi(x)\rangle$. Докажите, что отношение $\sim$ является отношением эквивалентности и множество $P[x]$ распадается на непересекающиеся классы эквивалентных элементов. Докажите, что для любого $h(x)\in P[x]$ класс эквивалентных элементов, содержащий $h(x)$, представляет собой множество $h(x)+\langle\varphi(x)\rangle=\{h(x)+f(x)\cdot\varphi(x) \mid f(x)\in P[x]\}$, которое обозначим $\overline{h(x)}$ (смежный класс по идеалу, порожденному многочленом $\varphi(x)$).

3. Пусть $\overline{h}(x)=h(x)+\langle\phi(x)\rangle$ и $F=\{\overline{f(x)} \mid f(x)\in P[x]\}$. Определим $\overline{f(x)}+\overline{g(x)}=\overline{f(x)+g(x)}$, $\overline{f(x)}\cdot\overline{g(x)}=\overline{f(x)\cdot g(x)}$ для любых $\overline{f(x)}, \overline{g(x)}\in F$. Докажите, что так определенные сложение и умножение смежных классов не зависят от выбора представителей классов. Докажите, что система $\langle F, +, \cdot\rangle$ является кольцом, а если многочлен $\varphi(x)$ неприводим над полем P, то является полем.

4. Докажите, что если $\varphi(x)=b_nx^n+b_{n-1}x^{n-1}+\ldots+b_1x+b_0$, то элемент $\overline{x}=x+\langle\varphi(x)\rangle\in F$ является корнем многочлена $\overline{\varphi}(x)=\overline{b_n}x^n+\overline{b_{n-1}}x^{n-1}+\ldots+$ $+\overline{b_1}x+\overline{b_0}$.

5. Докажите, что отображение ψ, сопоставляющее всякому элементу $a\in P$ элемент $\overline{a}\in F$, является взаимно однозначным и удовлетворяет условиям $\psi(a+b)=\psi(a)+\psi(b)$ и $\psi(a\cdot b)=\psi(a)\cdot\psi(b)$, т.е. является изоморфизмом (изоморфное вложение поля P в поле F).

4.5. Результант и дискриминант

4.5.1. Результант двух многочленов

Начнем с примера.

Пример 4.7

Пусть даны многочлены $f(x) = 2x^2 - 3x - 2$ и $g(x) = 3x^3 - x^2 - 3x + 1$. Запишем определитель матрицы:

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

Сначала выписываются коэффициенты первого многочлена три раза со сдвигом каждый раз на одно место вправо, а затем выписываются коэффициенты второго многочлена два раза также со сдвигом вправо. На остальных местах ставим нули. Таким образом, порядок определителя равен 2 + 3 = 5, где 2 — степень первого многочлена, а 3 — второго. Вычисляя определитель матрицы, получим $R(f, g) = 225$ (проверьте!).

Найденное число $R(f, g)$ является результантом многочленов $f(x)$ и $g(x)$. Дадим общее определение.

Определение 4.5. Пусть даны многочлены над числовым полем P : $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, причем $a_m \neq 0$ или $b_n \neq 0$. *Результантом* данных многочленов $f(x)$ и $g(x)$ называется определитель матрицы

$$M = \begin{pmatrix} a_m & a_{m-1} & \ldots & a_1 & a_0 & & \\ & a_m & a_{m-1} & \ldots & a_1 & a_0 & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ & & a_m & a_{m-1} & \ldots & a_1 & a_0 \\ b_n & b_{n-1} & \ldots & b_1 & b_0 & & \\ & b_n & b_{n-1} & \ldots & b_1 & b_0 & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ & & b_n & b_{n-1} & \ldots & b_1 & b_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \end{matrix},$$

где на остальных местах в матрице стоят нули. Обозначается $R(f, g) = |M|$.

Теорема 4.6. *Если многочлены $f(x)$ и $g(x)$ имеют общий корень, то $R(f, g) = 0$.*

Доказательство. Пусть α — общий корень данных многочленов $f(x)$ и $g(x)$. Рассмотрим однородную систему линейных уравнений с матрицей M. Эта система имеет своим ненулевым решением вектор $(\alpha^{m+n-1}, \alpha^{m+n-2}, \ldots, \alpha, 1)$. В самом деле, например, подстановка в первое уравнение соответствующей однородной системы дает

$$a_m\alpha^{m+n-1} + a_{m-1}\alpha^{m+n-2} + \ldots + a_1\alpha^n + a_0\alpha^{n-1} + 0\alpha^{n-2} + \ldots +$$

$$+ 0\alpha + 0 \cdot 1 = \alpha^{n-1}(a_m\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0) = 0.$$

Подставляя в уравнение с номером n, получаем

$$0\alpha^{m+n-1} + 0\alpha^{m+n-2} + \ldots + 0\alpha^{m+1} + a_m\alpha^m + a_{m-1}\alpha^{m-1} + \ldots +$$

$$+ a_1\alpha + a_0 \cdot 1 = 0.$$

Упражнение 4.3. Рассмотрите подстановку данного набора значений переменных в уравнение с номером $n + 1$ и в последнее уравнение системы.

Итак, однородная система линейных уравнений с матрицей M имеет ненулевое решение. Следовательно, определитель матрицы системы равен нулю, а значит, $R(f, g) = |M| = 0$.

Теорема 4.7. *Если $R(f, g) = 0$ и по крайней мере один из коэффициентов a_m, b_n отличен от нуля, то многочлены $f(x)$ и $g(x)$ имеют общий корень (быть может комплексный).*

Доказательство. Рассмотрим однородную систему линейных уравнений, матрица которой есть транспонированная матрица M^T (столбцы матрицы M становятся строками матрицы M^T). Переменные этой системы обозначим $X_{n-1}, \ldots, X_0, Y_{m-1}, \ldots, Y_0$. Поскольку определитель матрицы этой системы $|M^T| = |M| = R(f, g) = 0$, то однородная система линейных уравнений с матрицей M^T имеет ненулевое решение. Пусть ее ненулевым решением является следующий набор значений переменных: $X_{n-1} = c_{n-1}, X_{n-2} = c_{n-2}, \ldots, X_1 = c_1, X_0 = c_0$; $Y_{m-1} = d_{m-1}, Y_{m-2} = d_{m-2}, \ldots, Y_1 = d_1, Y_0 = d_0$. Тогда будем иметь равенства

$$a_m c_{n-1} + b_n d_{m-1} = 0,$$

$$a_{m-1}c_{n-1} + a_m c_{n-2} + b_{n-1}d_{m-1} + b_n d_{m-2} = 0,$$

.....

$$a_0c_1 + a_1c_0 + b_0d_1 + b_1d_0 = 0,$$

$$a_0c_0 + b_0d_0 = 0.$$

Эти равенства говорят о том, что

$$(a_mx^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0)(c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots +$$

$$+ c_1x + c_0) + (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0)(d_{m-1}x^{m-1} +$$

$$+ d_{m-2}x^{m-2} + \ldots + d_1x + d_0) = 0.$$

Запишем это в краткой форме: $f(x) \cdot u(x) + g(x) \cdot v(x) = 0$. Отсюда $f(x) \cdot u(x) = -g(x) \cdot v(x)$. Вспомним, что, по условию, $a_m \neq 0$ или $b_n \neq 0$. Предположим, что $a_m \neq 0$. Если предположить, что $u(x) = 0$, то $c_i = 0$ для всех $i = 0, 1, \ldots, n - 1$, а так как рассматриваемый набор значений переменных является ненулевым решением, то среди чисел d_j, $j = 0, 1, \ldots, m - 1$, есть отличные от нуля. Следовательно, $v(x) \neq 0$ и $g(x) \cdot v(x) = 0$, откуда $g(x) = 0$. Но тогда многочлены $f(x)$ и $g(x)$ имеют общий корень, что и требовалось доказать. Пусть $u(x)$ — ненулевой многочлен. Из равенства $f(x) \cdot u(x) = -g(x) \cdot v(x)$ вытекает, что $f(x) \cdot u(x) \vdots g(x)$. Если предположить, что НОД$(f(x), g(x)) = 1$, то $u(x) \vdots g(x)$, что невозможно, поскольку степень многочлена $u(x)$ меньше степени многочлена $g(x)$. Следовательно, НОД$(f(x), g(x)) = d(x)$, где степень $d(x)$ больше нуля. Таким образом, многочлены $f(x)$ и $g(x)$ имеют общий множитель $d(x)$ степени ≥ 1. Но тогда многочлены $f(x)$ и $g(x)$ имеют и общий корень. Теорема доказана.

4.5.2. Исключение неизвестного из системы двух уравнений с двумя неизвестными при помощи результанта

Рассмотрим систему двух уравнений с двумя неизвестными

$$\begin{cases} f(x,y) = 0, \\ g(x,y) = 0, \end{cases} \tag{4.3}$$

где $f(x, y)$, $g(x, y) \in P[x, y]$ и P является числовым полем. Расположим многочлены по убывающим степеням переменной x:

$$\begin{cases} f(x,y) = a_m(y)x^m + a_{m-1}(y)x^{m-1} + \ldots + a_1(y)x + a_0(y), \\ g(x,y) = b_n(y)x^n + b_{n-1}(y)x^{n-1} + \ldots + b_1(y)x + b_0(y), \end{cases}$$

где $a_i(y)$, $b_j(y) \in P[y]$ для $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$. Найдем результант этих многочленов, рассматривая их как многочлены от переменной x:

$$R_x(f,g) = \begin{vmatrix} a_m(y) & a_{m-1}(y) & \ldots & a_1(y) & a_0(y) & & \\ & a_m(y) & a_{m-1}(y) & \ldots & a_1(y) & a_0(y) & \\ & & \ldots\ldots\ldots\ldots & & & & \\ & & & a_m(y) & a_{m-1}(y) & \ldots & a_1(y)\ a_0(y) \\ b_n(y) & b_{n-1}(y) & \ldots & b_1(y) & b_0(y) & & \\ & b_n(y) & b_{n-1}(y) & \ldots & b_1(y) & b_0(y) & \\ & \ldots\ldots\ldots\ldots & & & & & \\ & & & b_n(y) & b_{n-1}(y) & \ldots & b_1(y)\ b_0(y) \end{vmatrix}.$$

Таким образом, $R_x(f, g) = S(y) \in P[y]$.

Теорема 4.8. 1. *Если упорядоченная пара чисел* (α, β) *является решением системы* (4.3), *то* β *есть решение уравнения* $S(y) = 0$.

2. *Пусть число* β *является решением уравнения* $S(y) = 0$.

2.1. *Если* $a_m(\beta) \neq 0$ *или* $b_n(\beta) \neq 0$, *то система* (4.3) *имеет решение* (α, β) *при некотором* α.

2.2. *Если* $a_m(\beta) = 0$ *и* $b_n(\beta) = 0$, *то может существовать число* α, *такое что* (α, β) *является решением системы* (4.3), *а может такого* α *и не существовать*.

Доказательство. 1. Пусть упорядоченная пара (α, β) является решением системы (4.3). При $y = \beta$ многочлены $f(x, \beta)$ и $g(x, \beta)$ имеют общий корень $x = \alpha$ и по теореме 4.6 их результант $S(\beta) = 0$. Это означает, что β есть решение уравнения $S(y) = 0$.

2. Пусть $\beta \in P$ является решением уравнения $S(y) = 0$.

2.1. Предположим, что $a_m(\beta) \neq 0$ или $b_n(\beta) \neq 0$. Поскольку результант многочленов $f(x, \beta)$ и $g(x, \beta)$ равен $S(\beta) = 0$ то, по теореме 4.7, эти многочлены имеют некоторый общий корень α, т.е. $f(\alpha, \beta) = 0$ и $g(\alpha, \beta) = 0$. Но это и означает, что (α, β) есть решение системы (4.3).

2.2. Следующие примеры подтверждают сказанное:

$$\begin{cases} yx^2 + x - 1 = 0, \\ 2yx^2 + x - 1 = 0; \end{cases} \quad \begin{cases} yx^2 + x - 1 = 0, \\ 2yx - 1 = 0. \end{cases}$$

Теорема доказана.

Упражнение 4.4. Проверьте, что примеры, приведенные в доказательство п. 2.2 теоремы 4.8, действительно ее подтверждают.

Теорема 4.8 подсказывает следующую стратегию решения системы двух уравнений с двумя переменными (4.3). Сначала записываем многочлены системы по убывающим степеням одной переменной и, рассматривая вторую переменную как параметр, находим результант $R_x(f, g) = S(y)$. Решая уравнение $S(y) = 0$, находим все его корни β_i. Затем для каждого β_i рассматриваем систему с одной переменной

$$\begin{cases} f(x,\beta_i)=0, \\ g(x,\beta_i)=0. \end{cases}$$

Таким образом, из системы удается исключить одну переменную.

Пример 4.8

Решим систему

$$\begin{cases} x^2y+5xy+2y-4=0, \\ 3xy+2x+y-2=0. \end{cases}$$

Решение. Расположим данные многочлены по убывающим степеням переменной x:

$$\begin{cases} y\cdot x^2+5y\cdot x+(2y-4)=0, \\ (3y+2)x+(y-2)=0. \end{cases}$$

Используя обозначения, принятые выше, имеем $a_2(y) = y$, $a_1(y) = 5y$, $a_0(y) = 2y - 4$, $b_1(y) = 3y + 2$, $b_0(y) = y - 2$. Найдем результант данных многочленов и приравняем его к нулю:

$$S(y)=\begin{vmatrix} y & 5y & 2y-4 \\ 3y+2 & y-2 & 0 \\ 0 & 3y+2 & y-2 \end{vmatrix}=$$

$$=y(y-2)^2+(3y+2)^2(2y-4)-5y(3y+2)(y-2)=$$

$$=(y-2)[y(y-2)+2(3y+2)^2-5y(3y+2)]=$$

$$=(y-2)(y^2-2y+18y^2+24y+8-15y^2-10y)=$$

$$=(y-2)(4y^2+12y+8)=4(y-2)(y^2+3y+2)=$$

$$=4(y-2)(y+1)(y+2)=0.$$

Пользуясь обозначениями, принятыми в теореме 4.8, получаем решения $\beta_1 = 2$, $\beta_2 = -1$, $\beta_3 = -2$.

1. $y = \beta_1 = 2$. Тогда $a_2(\beta_1) = \beta_1 = 2$, $b_1(\beta_1) = 3\beta_1 + 2 = 8$. Поскольку $a_2(\beta_1) \neq 0$ и $b_1(\beta_1) \neq 0$, то данная система имеет решение при $y = \beta_1 = 2$. Система приобретает вид

$$\begin{cases} 2x^2 + 10x = 0, \\ 8x = 0. \end{cases}$$

Следовательно, пара (0, 2) является решением данной системы.

Аналогично рассматриваются остальные случаи. В итоге получаем три решения данной системы: (0, 2), (–3, –1) и (–1, –2).

4.5.3. Дискриминант многочлена

Ранее было доказано, что многочлен $f(x)$ над числовым полем не имеет кратных множителей тогда и только тогда, когда он взаимно прост со своей производной $f'(x)$ (см. следствие 2 из теоремы 2.8). Следовательно, многочлен $f(x)$ имеет кратные множители, в частности кратные корни, тогда и только тогда, когда $f(x)$ и $f'(x)$ имеют общие корни, а это в соответствии с теоремами 4.6 и 4.7 равносильно тому, что результант $R(f, f') = 0$. В связи с этим введем новое понятие.

Определение 4.6. *Дискриминантом* многочлена $f(x)$ со старшим коэффициентом a_n называется $D(f) = \dfrac{1}{a_n}(-1)^{\frac{n(n-1)}{2}} R(f, f')$.

Из проведенных выше рассуждений вытекает следующая теорема.

Теорема 4.9. *Ненулевой многочлен $f(x)$ над числовым полем имеет кратные корни тогда и только тогда, когда его дискриминант равен нулю.*

Найдем дискриминант квадратного трехчлена $f(x) = a_2x^2 + a_1x + a_0$. Имеем $f'(x) = 2a_2x + a_1$ и

$$R(f, f') = \begin{vmatrix} a_2 & a_1 & a_0 \\ 2a_2 & a_1 & 0 \\ 0 & 2a_2 & a_1 \end{vmatrix} = a_2a_1^2 + 4a_2^2a_0 - 2a_2a_1^2 = a_2(4a_2a_0 - a_1^2).$$

Отсюда $D(f) = \dfrac{1}{a_2}(-1)^{\frac{2(2-1)}{2}} R(f, f') = a_1^2 - 4a_2a_0$.

Упражнение 4.5. Убедитесь, что дискриминант кубического трехчлена $f(x) = x^3 + px + q$ равен $D(f) = -(4p^3 + 27q^2)$.

Напомним, что для уравнения $x^3 + px + q = 0$ разрешающим уравнением является $z^2 + qz - \frac{p^3}{27} = 0$. Его дискриминант равен $D = \frac{q^2}{4} + \frac{p^3}{27} = \frac{4p^3 + 27q^2}{108}$. Таким образом, дискриминант $D(f)$ данного кубического многочлена и дискриминант D его разрешающего уравнения связаны соотношением $D(f) = -108D$.

Контрольные вопросы

1. Какова цель введения результанта?
2. Каков принцип написания результанта двух данных многочленов?
3. Что такое определитель матрицы и как он вычисляется?
4. Какова стратегия решения системы двух уравнений с двумя переменными?
5. На какой вопрос отвечает дискриминант многочлена?

Задачи

1. Найдите результант данных многочленов:

а) $3x^3 - 2x^2 + x + 2$, $x^2 - 2x + 3$;

б) $x^4 - x^2 + x + 1$, $x^2 + x + 1$;

в) $x^4 - x^2 + x + 1$, $x^3 + x + 1$.

2. При каком λ многочлены $f(x) = 4x^3 - \lambda x + 1$ и $g(x) = 2x^2 - \lambda x + 1$ имеют общий корень?

3. Исключите x из системы уравнений:

а) $\begin{cases} x^2 + xy + y^2 = 3, \\ x^2y - xy^2 = -6; \end{cases}$

б) $\begin{cases} x^3 + xy + y^3 - y = 0, \\ x^2 + xy - y^2 - 1 = 0; \end{cases}$

в) $\begin{cases} x^3 + 2x^2 - 6x - 8 + y = 0, \\ x^3 + 8x^2 + 5x - 2 + y = 0. \end{cases}$

4. Решите системы уравнений:

а) $\begin{cases} 4x^2 - 13x + y^2 + 7xy - 2y = 3, \\ 9x^2 - 28x + y^2 + 14xy - 4y = 5; \end{cases}$

б) $\begin{cases} 4x^2 - 7xy + y^2 - 2x + 7y - 6 = 0, \\ 9x^2 - 14xy + y^2 - 4x + 12y - 13 = 0; \end{cases}$

в) $\begin{cases} x^3 + x^2 - 5x - y^3 + 5y^2 + (x - 7)y + 3 = 0, \\ x^2 + 2x + y^2 - (x + 4)y + 3 = 0. \end{cases}$

5. Найдите дискриминант многочлена:

а) $x^3 + 2x^2 - x - 1$;

б) $x^3 - x^2 + 3x - 2$;

в) $x^4 - x^3 - x + 1$;

г) $x^4 + 3x^3 - 4x - 1$;

д) $ax^3 + bx^3 + (3a - b)x + a$.

6. Найдите значения λ, при которых данный многочлен имеет кратные корни:

а) $x^3 + \lambda x - 2$;

б) $y^4 - (\lambda + 3)y^2 - 2\lambda y - \lambda$;

в) $x^3 - 5x^2 - \lambda x + \lambda$;

г) $x^4 + 4x + \lambda$.

7. Найдите дискриминант многочлена $x^n + a$.

Список литературы

Учебники, учебные пособия, монографии

1. *Ван дер Варден, Б. Л.* Алгебра / Б. Л. Ван дер Варден. — М. : Наука, 1976.
2. *Винберг, Э. Б.* Алгебра многочленов : учеб. пособие для студентов-заочников / Э. Б. Винберг. — М. : Изд-во МГЗПИ, 1980.
3. *Винберг, Э. Б.* Курс алгебры / Э. Б. Винберг. — М. : Факториал Пресс, 2002.
4. *Кострикин, А. И.* Основы алгебры / А. И. Кострикин. — М. : Физматлит, 2000.
5. *Куликов, Л. Я.* Алгебра и теория чисел / Л. Я. Куликов. — М. : Высшая школа, 1979.
6. *Курант, Р.* Что такое математика? / Р. Курант, Г. Роббинс. — М. : Изд-во МЦНМО, 2000.
7. *Курош, А. Г.* Курс высшей алгебры / А. Г. Курош. — М. : Высшая школа, 1979.
8. *Ларин,* С. В. Алгебра и теория чисел. Группы, кольца и поля / С. В. Ларин — М. : Издательство Юрайт, 2017.
9. *Окунев, Л. Я.* Высшая алгебра / Л. Я. Окунев. — М. : Государственное издательство технико-теоретической литературы, 1949.
10. *Понтрягин, Л. С.* Знакомство с высшей математикой. Алгебра / Л. С. Понтрягин. — М. : Наука, 1987.
11. *Прасолов, В. В.* Многочлены / В. В. Прасолов. — М. : Изд-во МЦНМО, 2003.
12. *Сушкевич, А. К.* Основы высшей алгебры. — М. : Вузовская книга, 2017.
13. *Фаддеев, Д. К.* Лекции по алгебре / Д. К. Фаддеев. — М. : Наука, 1984.

Задачники

14. *Куликов, Л. Я.* Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. — М. : Просвещение, 1993.

15. *Солодовников, А. С.* Задачник-практикум по алгебре / А. С. Солодовников, М. А. Родина. — М. : Просвещение, 1985.
16. *Фаддеев, Д. К.* Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. — М. : Наука, 1977.

Новые издания по дисциплине «Высшая математика» и смежным дисциплинам

1. *Баврин, И. И.* Высшая математика для химиков, биологов и медиков : учебник и практикум для прикладного бакалавриата / И. И. Баврин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.
2. *Бекман, И. Н.* Высшая математика: математический аппарат диффузии : учебник для бакалавриата и магистратуры / И. Н. Бекман. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.
3. *Богомолов, Н. В.* Математика. Задачи с решениями : в 2 ч. : учеб. пособие для прикладного бакалавриата / Н. В. Богомолов. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2016.
4. *Бугров, Я. С.* Высшая математика : в 3 т. Т. 1. Дифференциальное и интегральное исчисление : в 2 кн. : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2017.
5. *Бугров, Я. С.* Высшая математика : в 3 т. Т. 2. Элементы линейной алгебры и аналитической геометрии : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2017.
6. *Бугров, Я. С.* Высшая математика : в 3 т. Т. 3 : в 2 кн. Кн. 1. Дифференциальные уравнения. Кратные интегралы : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2016.
7. *Бугров, Я. С.* Высшая математика : в 3 т. Т. 3 : в 2 кн. Кн. 2. Ряды. Функции комплексного переменного : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2016.
8. *Бугров, Я. С.* Высшая математика. Задачник : учеб. пособие для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — М. : Издательство Юрайт, 2017.

9. Высшая математика : учебник и практикум для академического бакалавриата / М. Б. Хрипунова [и др.] ; под общ. ред. М. Б. Хрипуновой, И. И. Цыганок. — М. : Издательство Юрайт, 2017.

10. Высшая математика для экономического бакалавриата : в 3 ч. : учебник и практикум для академического бакалавриата / под ред. Н. Ш. Кремера. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

11. *Гисин, В. Б.* Математика. Практикум : учеб. пособие для бакалавриата и магистратуры / В. Б. Гисин, Н. Ш. Кремер. — М. : Издательство Юрайт, 2017.

12. *Далингер, В. А.* Информатика и математика. Решение уравнений и оптимизация в mathcad и maple : учебник и практикум для прикладного бакалавриата / В. А. Далингер, С. Д. Симонженков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

13. *Дорофеева, А. В.* Высшая математика : учебник для академического бакалавриата / А. В. Дорофеева. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

14. *Дорофеева, А. В.* Высшая математика. Сборник задач : учеб.-практ. пособие для академического бакалавриата / А. В. Дорофеева. — 2-е изд. — М. : Издательство Юрайт, 2017.

15. *Кремер, Н. Ш.* Высшая математика для экономического бакалавриата : учебник и практикум / Н. Ш. Кремер ; отв. ред. Н. Ш. Кремер. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

16. *Ларин, С. В.* Числовые системы : учеб. пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

17. *Мачулис, В. В.* Высшая математика : учеб. пособие для вузов / В. В. Мачулис. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2016.

18. *Павлюченко, Ю. В.* Высшая математика для гуманитарных направлений : учебник и практикум для прикладного бакалавриата / Ю. В. Павлюченко, Н. Ш. Хассан ; под общ. ред. Ю. В. Павлюченко. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

19. *Попов, А. М.* Высшая математика для экономистов : учебник для бакалавров / А. М. Попов, В. Н. Сотников. — М. : Издательство Юрайт, 2017.

20. *Поспелов, А. С.* Сборник задач по высшей математике : в 4 ч. : учеб. пособие для прикладного бакалавриата / А. С. По-

спелов ; под ред. А. С. Поспелова. — М. : Издательство Юрайт, 2016.

21. Сборник задач по высшей математике. Ч. 1 : учеб. пособие для прикладного бакалавриата / А. С. Поспелов [и др.] ; под ред. А. С. Поспелова. — М. : Издательство Юрайт, 2017.

22. *Сухотин, А. М.* Высшая математика. Альтернативная методология преподавания : учеб. пособие для прикладного бакалавриата / А. М. Сухотин, Т. В. Тарбокова. — М. : Издательство Юрайт, 2016.

23. *Фоменко, Т. Н.* Высшая математика. Общая алгебра. Элементы тензорной алгебры : учебник и практикум для академического бакалавриата / Т. Н. Фоменко. — М. : Издательство Юрайт, 2017.

24. *Шипачев, В. С.* Высшая математика : учебник и практикум / В. С. Шипачев. — 8-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

25. *Шипачев, В. С.* Высшая математика. Полный курс : в 2 т. : учебник для академического бакалавриата / В. С. Шипачев ; под ред. А. Н. Тихонова. — 4-е изд., испр. и доп. — М. : Издательство Юрайт, 2016.

Предметный указатель