МИНИСТЕРСТВО НАРОДНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ
БЕЛАРУСЬ

ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Ф.СКОРИНЫ

Кафедра алгебры и геометрии

В.С.Монахов

ЧИСЛА И МНОГОЧЛЕНЫ

Тексты лекций по курсу "Алгебра и теория чисел"

Гомель 1992

УДК 512

Рецензенты: В.И.Гойко, кандидат физико-математических наук, Гомельский политехнический институт; Л.Н.Закревская, кандидат физико-математических наук, Белорусский институт инженеров железнодорожного транспорта.

Рекомендовано к печати ученым советом Гомельского государственного университета им. Ф.Скорины.

Монахов В.С. Числа и многочлены: Тексты лекций по курсу "Алгебра и теория чисел". – Гомель: ГГУ им. Ф.Скорины, 1992. – 80 с.

Изложены тексты лекций по курсу "Алгебра и теория чисел", касающиеся следующих разделов: целые числа и сравнения, кольцо классов вычетов, поле комплексных чисел, кольцо многочленов.

Рекомендовано студентам специальности 01.01 – "Математика", а также может быть полезно студентам других специальностей вузов, интересующихся началами высшей алгебры.

СОДЕРЖАНИЕ

ЛИТЕРАТУРА

1. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981.
2. Кострикин А.И. Введение в алгебру. – М.: Наука, 1977.
3. Куликов Л.Я. Алгебра и теория чисел. – М.: Высшая школа, 1977.
4. Милованов М.В., Тышкевич Р.И., Феденко А.С. Алгебра и аналитическая геометрия. – Мн.: Вышэйшая школа, 1984.
5. Фаддеев Д.К. Лекции по алгебре. – М.: Наука, 1984.

ВВЕДЕНИЕ

Настоящие тексты лекций отражают содержание тех разделов курса "Алгебра и теория чисел", которые изучаются на математическом факультете в первом семестре и касаются чисел и многочленов. Первые четыре параграфа посвящены целым числам и сравнениям. Здесь, кроме традиционного материала, предложен бинарный алгоритм нахождения наибольшего общего делителя целых чисел, который удобен в компьютерных вычислениях. В § 5 строится кольцо целых чисел, и указывается когда оно будет полем. В следующих двух параграфах рассматриваются комплексные числа, а в §§ 8–13 изучаются многочлены над произвольным полем. Последний параграф посвящен рациональным дробям. Приведены 45 примеров, иллюстрирующих основные методы решения ключевых задач.

§ 1. КОЛЬЦО ЦЕЛЫХ ЧИСЕЛ

Натуральные числа – это числа, возникшие в процессе счета, т.е. 1, 2, 3, ... Множество натуральных чисел обозначим через $\mathbb{N}$. Итак, $\mathbb{N} = \{1, 2, 3, \ldots\}$. Множество $\mathbb{Z}$ целых чисел состоит из множества натуральных чисел, числа ноль 0 и отрицательных чисел –1, –2, –3, ...

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\} = \{0, \pm 1, \pm 2, \ldots\}.$$

Сумма $a + b$, разность $a - b$ и произведение ab целых чисел a и b также являются целыми числами. Частное a/b от деления a на $b \neq 0$ не всегда целое число.

Во множестве натуральных чисел нет нулевого элемента, поэтому $\mathbb{N}$ не является кольцом. Множество целых чисел $\mathbb{Z}$ с операциями сложения и умножения целых чисел будет коммутативным кольцом с единицей. Обратные целым числам не принадлежат $\mathbb{Z}$, поэтому $\mathbb{Z}$ не поле.

ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ. Говорят, что целое число b *делит* целое a, если существует целое число q такое, что $a = bq$. В этом случае говорят также, что a *делится* на b. Число b называют делителем числа a, число a – кратным числу b, число q – *частным*. Запись $b \mid a$ означает, что b делит a, а запись $a \vdots b$ – число a делится на b.

Пусть $b = 0$. Если $a \neq 0$, то не существует такого числа q, что $a = bq$, поэтому ни одно число $a \neq 0$ не делится на ноль. С другой стороны, при $a = 0$ для любого $q \in \mathbb{Z}$ имеем $0 \cdot q = 0$, т.е. частное не определено однозначно. Поэтому *деление на ноль невозможно*.

Из определения легко получается следующая

Лемма 1.1. Для любых целых a, b и c справедливы следующие утверждения:

1) $a \mid a$;
2) если $a \mid b$, $b \mid c$, то $a \mid c$;
3) если $a \mid b$, то $\pm a \mid \pm b$;
4) если $a \mid b$ и $a \mid c$, то $a \mid bu + cv$, для любых целых u и v;

5) если $a \mid b$, то $a \mid bc$;

6) любое целое делит ноль;

7) единица I делит любое целое;

8) если $a \mid b$ и $b \neq 0$, то $|a| \leq |b|$.

ДЕЛЕНИЕ С ОСТАТКОМ. Разделить целое число a на целое число $b \neq 0$ с о с т а т к о м - это значит найти два таких целых числа q и r, чтобы выполнялись условия: $a = bq + r$; $0 \leq r < |b|$. Число q называется н е п о л н ы м ч а с т н ы м, а r - о с т а т к о м от деления a на b. Очевидно, $r = 0$ тогда и только тогда, когда $a : b$.

Покажем, что деление с остатком всегда возможно. Пусть сначала $b > 0$. Рассмотрим числа кратные b и расположим их в порядке возрастания:

$$\ldots, -3b, -2b, -b, 0, b, 2b, 3b, \ldots$$

Выберем число q таким, что $bq \leq a < b(q+1)$. Тогда $0 \leq a - bq < b$. Положив $r = a - bq$, получим:

$$a = bq + r, \quad 0 \leq r < b.$$

Пусть теперь $b < 0$. Тогда $-b > 0$ и согласно первому случаю деление a на $-b$ с остатком возможно. Это означает, что существуют целые q и r такие, что $a = (-b)q + r$, $0 \leq r < -b$. Поэтому $a = b(-q) + r$, $0 \leq r < |b|$.

Итак, возможность деления с остатком доказана. Проверим единственность. Предположим, что $a = bq_1 + r_1 = bq_2 + r_2$, где $0 \leq r_1, r_2 < |b|$. Ясно, что $|r_2 - r_1| < |b|$ и $b(q_1 - q_2) = r_2 - r_1$. Предположим, что $r_2 \neq r_1$. Тогда из последнего равенства имеем, что $|r_2 - r_1| \geq |b|$, противоречие. Значит, допущение $r_2 \neq r_1$ неверно, и остатки r_1 и r_2 равны. Но тогда $q_1 = q_2$.

Таким образом доказана следующая

Т е о р е м а I.2. (Теорема о делении с остатком). Для любого целого числа a и любого целого $b \neq 0$ существуют и единственны такие целые числа q и r, что $a = bq + r$, где $0 \leq r < |b|$.

П р и м е р I. Разделить с остатком ± 257 на ± 23.

△ Так как

$$\begin{array}{r|l} 257 & 23 \\ \underline{23} & 11 \\ 27 & \\ \underline{23} & \\ 4 & \end{array},$$

то $257 = 23 \cdot 11 + 4$. Здесь II - неполное частное, 4 - остаток.

Разделим -257 на 23. Для этого, как в доказательстве теоремы I.2, найдем целое q такое, что $23q \leq -257 < 23(q+1)$. Так как $23 \cdot (-12) = -276 \leq -257 < 23 \cdot (-11)$, то $-257 = 23 \cdot (-12) + 19$.

Делим на (-23). Как в доказательстве теоремы I.2, берем $257 = 23 \cdot 11 + 4$ и записываем в виде $257 = (-23)(-11) + 4$. Для деления (-257) на (-23) берем $-257 = 23 \cdot (-12) + 19$ и записываем в виде $-257 = (-23) \cdot 12 + 19$.

О т в е т: $257 = 23 \cdot 11 + 4$; $257 = (-23)(-11) + 4$;
$-257 = 23 \cdot (-12) + 19$; $-257 = (-23) \cdot 12 + 19$.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. Всякое целое число, которое делит целые числа a и b, называется их о б щ и м д е л и т е л е м. Наибольшее число среди общих делителей чисел a и b называется н а и б о л ь ш и м о б щ и м д е л и т е л е м чисел a и b и обозначается через НОД(a, b).

Любое целое число, отличное от нуля является делителем 0. Поэтому общие делители для пары (0, 0) исчерпывают все множество $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ целых чисел без нуля. Наибольшего числа во множестве $\mathbb{Z}^*$ нет. Поэтому НОД(0, 0) не существует.

Если $a \neq 0$, то для любого целого b совокупность общих делителей для чисел a и b будет подмножеством множества всех делителей числа a. По лемме 1.I.8 множество всех делителей числа a конечно, и в нем можно взять наибольшее число. Поэтому, наибольший общий делитель любой пары чисел (a, b), отличной от (0, 0), существует. Ясно также, что НОД(a, b) = НОД$(\pm a, \pm b)$ = НОД$(|a|, |b|)$.

Л е м м а I.3. Если $a \mid b$, то НОД$(a, b) = |a|$.

Δ Если $d|a$, то $d|b$ по лемме I.I.2. Поэтому общие делители чисел a и b исчерпываются делителями числа a. Наибольшим будет делитель $|a|$.

Л е м м а I.4. Если $a = bq + r$, где a, b и r отличны от нуля, то НОД(a,b)=НОД(b,r).

Δ Пусть d - общий делитель чисел a и b. Тогда $d|a-bq=r$ и d делит r. Поэтому общие делители чисел a и b являются общими делителями чисел b и r. Обратно, если c делит b и r, то c делит $bq+r=a$, т.е. c. - общий делитель для a и b. Таким образом, множество общих делителей a и b и множество общих делителей b и r совпадают, и НОД(a,b)=НОД(b,r).

АЛГОРИТМ ЕВКЛИДА. Для нахождения НОД(a,b) используется алгоритм Евклида, который основан на многократном применении теоремы о делении с остатком. Пусть $a,b \in \mathbb{Z}$, $a \geq b > 0$. Если $b|a$, то НОД$(a,b)=b$. Пусть b не делит a. Тогда мы можем написать цепочку равенств

$$
\text{(I)}\quad
\begin{aligned}
a &= bq_1 + r_1, && 0 < r_1 < b;\\
b &= r_1 q_2 + r_2, && 0 < r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, && 0 < r_3 < r_2;\\
&\cdots && \cdots\\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, && 0 < r_{n-1} < r_{n-2};\\
r_{n-2} &= r_{n-1} q_n + r_n, && 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}
$$

Каждое из равенств (I) основано на теореме о делении с остатком. Поскольку остатки

$$b > r_1 > r_2 > \ldots > r_{n-1} > r_n \geq 0$$

строго убывают, то через конечное число шагов должен появиться остаток, равный нулю, т.е. на каком-то этапе деление произойдет без остатка. В (I) деление без остатка записано в последней строке.

А л г о р и т м Е в к л и д а для чисел a и b заключается в нахождении равенств (I) для этих чисел.

Т е о р е м а I.5. Пусть a и b - целые положительные числа и b не делит a. Тогда НОД(a,b) равен последнему отличному от нуля остатку в алгоритме Евклида для чисел a и b.

Δ В силу леммы I.4 получаем из (I):

$$
\begin{aligned}
&\text{НОД}(a,b) = \text{НОД}(b,r_1);\\
&\text{НОД}(b,r_1) = \text{НОД}(r_1,r_2);\\
&\text{НОД}(r_1,r_2) = \text{НОД}(r_2,r_3);\\
&\cdots\cdots\\
&\text{НОД}(r_{n-3},r_{n-2}) = \text{НОД}(r_{n-2},r_{n-1});\\
&\text{НОД}(r_{n-2},r_{n-1}) = \text{НОД}(r_{n-1},r_n);\\
&\text{НОД}(r_{n-1},r_n) = r_n.
\end{aligned}
$$

Поэтому НОД$(a,b)=r_n$.

П р и м е р 2. Найти НОД(2585, 7975).

Δ

7975 | 2585	3	7975 = 2585·3 + 220
7755		
2585 | 220	11	2585 = 220·11 + 165
2200		
385		220 = 165·1 + 55
220		
220 | 165	1	165 = 55·3
165		
165 | 55	3	
165		
0		

Слева записаны вспомогательные вычисления, справа - алгоритм Евклида для данных чисел. Последний отличный от нуля остаток равен 55, это и есть наибольший общий делитель чисел 2585 и 7975.

О т в е т: НОД(2585, 7975)=55.

Т е о р е м а I.6. Если d =НОД(a,b), то существуют целые числа u и v такие, что $d=au+bv$.

△ Доказательство проведем индукцией по числу строк в алгоритме Евклида (I) для чисел a и b. Если в (I) имеется только одна строка, то $a=bq_1$, и в этом случае b =НОД(a,b). Так как $b=a\cdot 0+b\cdot 1$, то наше утверждение справедливо.

Пусть теперь утверждение верно для всех чисел, у которых в алгоритме Евклида n строк. И пусть для чисел a и b в алгоритме Евклида $n+1$ строка, см. (I). Уберем первую строку. Тогда оставшиеся строки будут алгоритмом Евклида для чисел b и r_1. По индукции существуют такие целые числа u_1 и v_1, что $r_n=bu_1+r_1v_1$. Вместо r_1 подставим его выражение из первого равенства $a=bq_1+r_1$. Имеем $r_n=bu_1+(a-bq_1)v_1=av_1+b(u_1-q_1v_1)$.

П р и м е р 3. Найти линейное представление наибольшего общего делителя чисел 2585 и 7975.

△ Воспользуемся примером 2. $55=220-165=$

$=220-(2585-220\cdot 11)=220\cdot 12-2585=$

$=(7975-2585\cdot 3)\cdot 12-2585=2585\cdot(-37)+$

$+7975\cdot 12.$

О т в е т: $55=2585\cdot(-37)+7975\cdot 12.$

ВЗАИМНО ПРОСТЫЕ ЧИСЛА. Два числа называются в з а и м н о п р о с т ы м и, если их наибольший общий делитель равен I.

Т е о р е м а I.7. Если $a\mid bc$, причем a и b - взаимно просты, то $a\mid c$.

△ По теореме I.6. существуют числа u и v такие, что $1=au+bv$. Умножим обе части последнего равенства на число c. Получим $c=acu+bcv$. По условию теоремы bc делится на a, поэтому c делится на a по

лемме I.I.

Т е о р е м а I.8. Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что $1=au+bv$.

△ Если a и b взаимно просты, то НОД$(a,b)=1$ и по теореме I.6. существуют целые u и v такие, что $au+bv=1$. Обратно, если $au+bv=1$ и d - общий делитель чисел a и b, то $d\mid au+bv=1$ и целые числа a и b - взаимно просты.

НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ. Если число c делится на числа a и b, то c называют о б щ и м к р а т н ы м чисел a и b. Наименьшее среди положительных общих кратных чисел a и b назвают н а и м е н ь ш и м о б щ и м к р а т н ы м чисел и обозначают через НОК(a,b).

Т е о р е м а I.9. Если a и b - целые положительные числа, то $ab=$ НОК(a,b) НОД(a,b).

△ Если $d=$НОД(a,b), то $a=a_1d$, $b=b_1d$ и НОД$(a_1,b_1)=1$.

Пусть m - положительное общее кратное чисел a и b. Тогда $m=ac$ и $b=b_1d\mid a_1dc$. Отсюда с учетом теоремы I.7 получаем, что $b_1\mid c$. Теперь $c=b_1l$ и $m=ac=a_1db_1l$. Таким образом, любое положительное общее кратное чисел a и b имеет вид

$$a_1db_1l=\frac{a_1db_1dl}{d}=\frac{ab}{d}l.$$

Так как

$$\frac{ab}{d}=\frac{a_1db_1d}{d}=a_1b_1d=ab_1=a_1b,$$

то ab/d будет также общим кратным. Поэтому

$$\text{НОК}(a,b)=\frac{ab}{d}=\frac{ab}{\text{НОД}(a,b)}.$$

П р и м е р 4. Найти НОК(2585, 7975)

△ По теореме I.9 имеем НОК$(2585,7975)=$

$=2585\cdot 7975/$ НОД$(2585,7975)=$

$=2585\cdot 7975/55=374825.$

О т в е т: НОК(2585, 7975)=374825.

§ 2. БИНАРНЫЙ АЛГОРИТМ

Кроме алгоритма Евклида для нахождения НОД используется также бинарный алгоритм. Он основан на следующих трех очевидных свойствах НОД.

Л е м м а 2.1. Для любых целых чисел a и b справедливы следующие утверждения:

1. $НОД(2a, 2b) = 2\,НОД(a, b)$;
2. $НОД(2a, 2b+1) = НОД(a, 2b+1)$;
3. $НОД(a, b) = НОД(a-b, b)$.

△ Проверим, например, третье свойство. Если d – общий делитель a и b, то d – общий делитель $a-b$ и b, и наоборот. Значит, общие делители чисел a, b и $a-b$, b совпадают, значит, равны и их НОД. ▲

В соответствии с этими свойствами для нахождения $d = НОД(a, b)$ осуществляются следующие действия.

Шаг 1. Выделяют наибольшую степень двойки 2^k, на которую делятся числа a и b. Уменьшают числа a и b в 2^k раз: $a = 2^k a_1$, $b = 2^k b_1$. Одно из чисел a_1 или b_1 нечетно, пусть нечетно b_1. Теперь $d = 2^k d_1$, где $d_1 = НОД(a_1, b_1)$.

Шаг 2. Если a_1 четно, то делят его на максимальную возможную степень 2, оставив b_1 без изменения. Получают, $a_1 = 2^s a_2$, a_2 и b_1 нечетны и $d_1 = НОД(a_1, b_1) = НОД(a_2, b_1)$. Теперь надо найти НОД двух нечетных чисел a_2, b_1.

Шаг 3. Вычитают из большего числа меньшее. Если $a_2 > b_1$, то $НОД(a_2, b_1) = НОД(a_2 - b_1, b_1)$ не изменится.

Число $a_2 - b_1$ четное как разность двух нечетных чисел.

Шаг 4. Применяют к $a_2 - b_1$ действие шага 2, затем действие шага 3 и т.д.

После выполнения действий шага 2 и шага 3 НОД не меняется, а хотя бы одно из чисел пары уменьшается. Поэтому в некоторый момент оба числа станут равными друг другу и равными d_1. Искомый $НОД(a, b)$ вычисляется после этого как произведение чисел 2^k и d_1.

В приведенном бинарном алгоритме используются лишь две операции: вычитание и деление на 2. Это позволяет при "ручном" нахождении НОД избежать вычислительных ошибок, ведь необходимо только правильно вычитать и делить на 2.

Проиллюстрируем бинарный алгоритм на следующем примере.

П р и м е р 1. Найти НОД(29568, 8580).

△ Шаг 1. Выделяем наибольшую степень двойки, на которую делятся эти числа $29568 = 2^2 \cdot 7392$; $8580 = 2^2 \cdot 2145$. Запоминаем 2^2.

Шаг 2. Число 7392 четное. Делим его на максимальную возможную степень 2, оставляя второе число 2145 без изменения. $7392 = 2^5 \cdot 231$. Теперь надо искать $d = НОД(231, 2145)$.

Шаг 3. Вычитаем из большего числа 2145 меньшее 231. Имеем $2145 - 231 = 1914$, $d = НОД(231, 1914)$.

Шаг 4. Применяем к 1914 действие шага 2. Получаем $1914 = 2 \cdot 957$. Теперь $d = НОД(231, 957)$. и надо возвращаться к действиям шага 2 и шага 3, и т.д.

Все эти вычисления проводятся в двух столбиках следующим образом.

29568	2^2	8580
7392		2145
231		231
33		1914
198		957
99		231
33		726
66		365
33		231
33		134
0		33

Итак, $НОД(29568, 8580) = 2^2 \cdot 33 = 132$.

Вычислим НОД (29568, 8580) с помощью алгоритма Евклида

$$
\begin{array}{r|l}
29568 & 8580 \\
\underline{25740} & 2 \\
8580 & 3828 \\
\underline{7656} & 2 \\
3828 & 924 \\
\underline{3696} & 4 \\
924 & 132 \\
\underline{924} & 7 \\
0 &
\end{array}
$$

$$29568 = 8580 \cdot 2 + 3828$$

$$8580 = 3828 \cdot 2 + 924$$

$$3828 = 924 \cdot 4 + 132$$

$$924 = 132 \cdot 7$$

О т в е т: НОД(29568, 8580)=I32.

Можно соединить алгоритм Евклида с бинарным алгоритмом следующим образом. Если $a \geq b > 0$ нечетны, то $a = bq + r$, где $0 < |r| < b$ и r четно. Поэтому если $r \neq 0$, то

r делим на максимальную степень 2, пока r не станет нечетным. Затем пару a, b заменяем парой $b, |r|$ и повторяем этот процесс.

П р и м е р 2. Найдем опять НОД(29568, 8580)

Δ $НОД(29568, 8580) = 2^2 НОД(7392, 2145)$

$$7392 = 2145 \cdot 4 - 1188$$
$$1188 = 4 \cdot 297$$
$$2145 = 297 \cdot 7 + 66$$
$$66 = 2 \cdot 33$$
$$297 = 33 \cdot 9$$

Итак, $НОД(7392, 2145) = 33$ и

$НОД(29568, 8580) = 132$.

О т в е т: НОД(29568, 8580)=I32.

§ 3. ПРОСТЫЕ ЧИСЛА

Натуральное число p называется п р о с т ы м ч и с л о м, если оно больше I и не имеет положительных делителей, отличных от p и I. Все натуральные числа, отличные от I и простых чисел, называются с о с т а в н ы м и ч и с л а м и. Итак, множество N натуральных чисел разбивается на три подмножества: простые числа; составные числа; число I.

Л е м м а 3.I. Всякое натуральное число $n > 1$ делится хотя бы на одно простое число.

Δ Применим метод математической индукции. Для натурального числа $n = 2$ лемма справедлива. Предположим, что утверждение справедливо для всех натуральных чисел, больших I и меньше n, и докажем справедливость леммы для n.

Если n - простое число, то n делится на простое n, и лемма справедлива.

Если n - составное число, то $n = ab$, где a и b - натуральные числа > 1. Так как $1 < a < n$, то к a применима индукция. Значит, число a делится на некоторое простое p. Но тогда и n делится на p.

Теорема 3.2 (Евклида). Множество простых чисел бесконечно.

△ Проведем доказательство от противного. Предположим, что множество простых чисел конечно. Пусть это будут числа $p_1, p_2, \dots, p_k$. Составим произведение $p_1 p_2 \cdots p_k$ всех простых чисел, и рассмотрим натуральное число $q = 1 + p_1 p_2 \cdots p_k$. Так как $q > p_i$ для всех i, то q – составное число и по лемме 3.1 число q делится на некоторое простое число. Пусть q делится на p_1. Тогда $q - p_1 p_2 \cdots p_k = 1$ тоже должно делится на p_1. Но это невозможно, так как $p_1 > 1$. Поэтому допущение неверно, и множество простых чисел бесконечно.

Лемма 3.3. Если n – натуральное число, а p – простое, то либо p делит n, либо p и n – взаимно просты.

△ Пусть $d = НОД(p, n)$. Так как $d \mid p$, то либо $d = 1$, либо $d = p$. В первом случае числа n и p взаимно просты, во втором – число p делит n.

Лемма 3.4. Если произведение нескольких натуральных чисел делится на простое число p, то хотя бы один из сомножителей делится на p.

△ Пусть $a_1 a_2$ делится на p. Если a_1 делится на p, то утверждение леммы справедливо. Если a_1 не делится на p, то a_1 и p – взаимно просты по лемме 3.3, а по теореме I.7 число a_2 делится на p. Итак, для двух сомножителей лемма справедлива.

Далее индукцией по числу сомножителей. Считаем, что утверждение леммы справедливо для произведений с числом сомножителей $n-1$. Пусть $a = a_1 \dots a_n$. Представим число a в виде двух сомножителей $a = \bar{a} \cdot a_n$, где $\bar{a} = a_1 \dots a_{n-1}$. Но для двух сомножителей лемма доказана, т.е. p делит либо $\bar{a}$, либо a_n. Если p делит $a a_n$, то лемма справедлива. Если p делит $\bar{a}$, то по индукции p делит одно из чисел $a_1, \dots, a_{n-1}$.

Теорема 3.5. (Основная теорема арифметики). Всякое целое число $a > 1$ либо простое, либо может быть представлено, и притом единственным образом,

в виде произведения простых чисел.

△ Так как 2 – простое число, то для $a = 2$ утверждение доказано.

Предположим, что утверждение справедливо для всех целых чисел от 2 до $a-1$, и докажем справедливость его для a.

Если a – простое, то утверждение доказано. Если a – составное, то $a = a_1 a_2$, где $1 < a_1 < a$, $1 < a_2 < a$. По индуктивному предположению числа a_1 и a_2 разложимы в произведение простых чисел.

$$a_1 = p_1 \cdots p_t, \qquad a_2 = p_{t+1} \cdots p_s.$$

Поэтому $a = p_1 \cdots p_t p_{t+1} \cdots p_s$, и разложение числа a в произведение простых чисел доказано.

Предположим, что целое a двумя способами представлено в виде произведения простых чисел

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r.$$

Тогда p_1 делит $q_1 q_2 \cdots q_r$ и по лемме 2.4 одно из чисел, пусть q_1, делится на p_1. Так как q_1 – простое, то $q_1 = p_1$. Теперь для

$$\frac{a}{p_1} = p_2 \cdots p_s = q_2 \cdots q_r$$

по индукции считаем, что $s = r$ и при подходящей нумерации $p_2 = q_2, \dots, p_s = q_s$.

Следствие. Всякое целое число $a \neq \pm 1$ и отличное от нуля однозначно представляется в виде $a = \varepsilon p_1 \dots p_s$, где $\varepsilon = \pm 1$ и $p_1 \le p_2 \le \dots \le p_s$ – простые числа. ▲

В разложении целого a на простые сомножители некоторые из них могут повторяться. Пусть простое p_1 встречается α_1 раз, p_2 встречается α_2 раз, ..., p_k встречается α_k раз, все $p_1, p_2, \dots, p_k$ – различные простые числа. Тогда разложение числа a на простые множители можно записать следующим образом:

$$a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Это разложение называют **каноническим**.

Пример 1. $7000 = 7 \cdot 1000 = 7 \cdot 2 \cdot 500 =$

$= 7 \cdot 2 \cdot 2 \cdot 250 = 7 \cdot 2 \cdot 2 \cdot 2 \cdot 125 = 7 \cdot 2^3 \cdot 5 \cdot 25 = 2^3 \cdot 5^3 \cdot 7.$

Теорема 3.6. Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ – канонические разложения натуральных чисел a и b. Тогда

$$НОД(a,b) = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k}, \text{ где } \lambda_i = \min\{\alpha_i, \beta_i\};$$

$$НОК(a,b) = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}, \text{ где } \mu_i = \max\{\alpha_i, \beta_i\}.$$

△ Ясно, что все делители числа a имеют вид $p_1^{\delta_1} \dots p_k^{\delta_k}$, где $0 \le \delta_i \le \alpha_i$, $i = 1, 2, \dots, k$. Общими делителями чисел a и b будут числа $p_1^{\delta_1} \dots p_k^{\delta_k}$, где $0 \le \delta_i \le \alpha_i$, $0 \le \delta_i \le \beta_i$. Наибольшим общим делителем чисел a и b будет $p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k}$, где $\lambda_i = \min\{\alpha_i, \beta_i\}$.

Общие кратные чисел a и b имеют вид $p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$, где $\gamma_i \ge \alpha_i$ и $\gamma_i \ge \beta_i$. Поэтому наименьшее общее кратное получится при $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Пример 2. Так как $39000 = 13 \cdot 3000 = 13 \cdot 3 \cdot 1000 = 13 \cdot 3 \cdot 8 \cdot 125 = 2^3 \cdot 3 \cdot 5^3 \cdot 13$, то $НОД(39000, 7000) = 2^3 \cdot 5^3$, а $НОК(39000, 7000) = 2^3 \cdot 3 \cdot 5^3 \cdot 7 \cdot 13$.

Лемма 3.7. Если натуральное число a не делится ни на одно простое число $\le \sqrt{a}$, то число a простое.

△ Предположим, что a – составное число, и пусть $a = pb$, где p – наименьшее простое число, делящее число a. Тогда $p \le b$ и $a = pb \ge p^2$. Теперь, $p \le \sqrt{a}$, что противоречит условию. ▲

Эта лемма уменьшает количество проверок, которое нужно

провести, чтобы убедиться, является ли число простым или составным.

Пример 3. Являются ли числа 181 и 197 простыми?

△ 181 и 197 не делятся на простые числа 2, 5, 7, 11, 13. Так как других простых чисел не более 15 нет и $\sqrt{181} < \sqrt{197} < 15$, то числа 181 и 197 простые.

Ответ: являются.

Пример 4. Разложить 2353 на простые множители.

△ Так как $\sqrt{2353} < 49$, то надо испытать все простые числа не более 47. Числа 2, 3, 5, 7, 11 не делят 2353, а 13 делит $2353 = 13 \cdot 181$. В примере 3 мы установили, что 181 – простое число.

Ответ: $2353 = 13 \cdot 181$.

§ 4. СРАВНЕНИЯ

Пусть $a, b, m \in \mathbb{Z}$, $m > 0$. Если m делит $a - b$, то пишут $a \equiv b \pmod m$ и говорят: a сравнимо с b по модулю m. Если m не делит $a - b$, то пишут $a \not\equiv b \pmod m$.

Пример 1. $12 \equiv 3 \pmod 3$; $5 \equiv 11 \pmod 6$; $11 \equiv -4 \pmod 5$, $11 \not\equiv 3 \pmod 7$.

Теорема 4.1. Два целых a и b сравнимы по модулю m тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m.

△ Пусть $a \equiv b \pmod m$. Это означает, что $m \mid a - b$, т.е. $a - b = mt$, где t – целое. Разделим b на m: $b = mq + r$, $0 \le r < m$. Теперь $a = b + mt = mq + r + mt = m(q + t) + r$, т.е. при делении a на m получается тот же остаток, что и при

делении b на m.

Обратно, пусть остатки при делении a и b на m равны, т.е. $a=mq_1+r$, $b=mq_2+r$, где $0\le r<m$. Тогда $a-b=m(q_1-q_2)$, т.е. m делит $a-b$. Это означает, что $a\equiv b(\mathrm{mod}\,m)$. ▲

В следующей лемме приведены самые простые свойства сравнений, похожие на свойства равенства.

Лемма 4.2. 1) $a\equiv a(\mathrm{mod}\,m)$;

2) если $a\equiv b(\mathrm{mod}\,m)$, то $b\equiv a(\mathrm{mod}\,m)$;

3) если $a\equiv b(\mathrm{mod}\,m)$, $b\equiv c(\mathrm{mod}\,m)$, то $a\equiv c(\mathrm{mod}\,m)$.

△ Проверим третье свойство: $m\mid a-b$, $m\mid b-c$, поэтому m делит $a-b+b-c=a-c$, и $a\equiv c(\mathrm{mod}\,m)$.

Лемма 4.3. Сравнения по одному и тому же модулю можно почленно складывать, вычитать и перемножать.

△ Пусть $a\equiv b(\mathrm{mod}\,m)$, $c\equiv d(\mathrm{mod}\,m)$. Тогда $a-b=mq_1$, $c-d=mq_2$ и $a=b+mq_1$, $c=d+mq_2$. Поэтому $ac=bd+m(bq_2+dq_1+mq_1q_2)$, т.е. $ac\equiv bd(\mathrm{mod}\,m)$. Аналогично, $ac=(b+mq_1)(d+mq_2)=bd+m(bq_2+dq_1+mq_1q_2)$, т.е. $ac\equiv bd(\mathrm{mod}\,m)$.

Следствие. Если $a\equiv b(\mathrm{mod}\,m)$ и $n\in N$, то $a^n\equiv b^n(\mathrm{mod}\,m)$.

Лемма 4.4. К обеим частям сравнения можно прибавлять одно и то же целое число.

△ Действительно, если $a\equiv b(\mathrm{mod}\,m)$ и k – любое целое число, то $k\equiv k(\mathrm{mod}\,m)$ по лемме 4.2, и теперь $a+k\equiv b+k(\mathrm{mod}\,m)$ по лемме 4.3.

Лемма 4.5. Члены сравнения можно переносить из одной части сравнения в другую с противоположным знаком.

△ Прибавляя к сравнению $a\equiv b+c(\mathrm{mod}\,m)$ сравнение $-b\equiv -b(\mathrm{mod}\,m)$, получаем $a-b\equiv c(\mathrm{mod}\,m)$.

Лемма 4.6. Обе части сравнения можно умножать на одно и то же целое число.

△ Умножая сравнение $a\equiv b(\mathrm{mod}\,m)$ на сравнение $c\equiv c(\mathrm{mod}\,m)$, получаем $ac\equiv bc(\mathrm{mod}\,m)$.

Пример 2. Доказать, что $6^{1001}+1$ и $6^{1000}-1$ делятся на 7.

△ Так как $6\equiv -1(\mathrm{mod}\,7)$, то $6^{1000}\equiv 1(\mathrm{mod}\,7)$ и $6^{1001}\equiv -1(\mathrm{mod}\,7)$, т.е. 7 делит $6^{1000}-1$ и $6^{1001}+1$.

Пример 3. Доказать, что число n и сумма его цифр имеют одинаковые остатки от деления на 9 и 3.

△ Пусть число n имеет цифры $a_r, a_{r-1}, \dots, a_1, a_0$, т.е. $n=a_ra_{r-1}\dots a_1a_0$. Это значит, что

$$n=a_0+a_1\cdot 10+a_2\cdot 10^2+\dots+a_{r-1}\cdot 10^{r-1}+a_r\cdot 10^r.$$

Так как $10\equiv 1(\mathrm{mod}\,9)$, то $10^k\equiv 1(\mathrm{mod}\,9)$ для любого целого $k\ge 0$. По лемме 4.2 $a_k\equiv a_k(\mathrm{mod}\,9)$, а по лемме 4.3 $a_k10^k\equiv a_k(\mathrm{mod}\,9)$, для любого $k\ge 0$. Складывая почленно сравнения $a_k10^k\equiv a_k(\mathrm{mod}\,9)$ для $k=0,1,\dots,r$, получим $n\equiv a_0+a_1+\dots+a_r(\mathrm{mod}\,9)$. ▲

Из этого примера вытекает следующий признак делимости: если сумма цифр числа n делится на 3 или на 9, то и само число n делится на 3 или на 9 соответственно.

Заметим, что делить сравнения, вообще говоря, нельзя. Например, $2\equiv 12(\mathrm{mod}\,10)$, $2\equiv 2(\mathrm{mod}\,10)$, но $1\not\equiv 6(\mathrm{mod}\,10)$. Далее, может быть так, что $a\not\equiv 0(\mathrm{mod}\,m)$ $b\not\equiv 0(\mathrm{mod}\,m)$, но $ab\equiv 0(\mathrm{mod}\,m)$. Например, $2\not\equiv 0(\mathrm{mod}\,10)$, $5\not\equiv 0(\mathrm{mod}\,10)$, но $2\cdot 5\equiv 0(\mathrm{mod}\,10)$.

Перечисленные сравнения не зависели от модуля. Следующие свойства сравнения связаны с модулем.

Лемма 4.7. Обе части сравнения и модуль можно умножить на одно и то же натуральное число.

△ Пусть $a\equiv b(\mathrm{mod}\,m)$. Тогда $a-b=mt$. Если c – целое число, то $c(a-b)=cmt$ и $ca-cb=(cm)t$, т.е. $ca\equiv cb(\mathrm{mod}\,cm)$.

Лемма 4.8. Если $ak\equiv bk(\mathrm{mod}\,m)$, $d=\text{НОД}(k,m)$, то $a\equiv b\left(\mathrm{mod}\,\frac{m}{d}\right)$.

Δ Пусть $m=dm_1$, $\kappa=d\kappa_1$ и НОД$(m_1,\kappa_1)=1$. Если $a\kappa\equiv b\kappa(\mathrm{mod}\,m)$, то $dm_1 \mid a\kappa-b\kappa=ad\kappa_1-bd\kappa_1=(a\kappa_1-b\kappa_1)d$, откуда $m_1 \mid a\kappa_1-b\kappa_1=(a-b)\kappa_1$. Так как НОД$(m_1,\kappa_1)=1$, то $m_1 \mid a-b$ и $a\equiv b(\mathrm{mod}\,m_1)$. ▲

При $\kappa=d$ из леммы 4.8 получаем

Следствие 1. Обе части сравнения и модуль можно разделить на любой их общий делитель. ▲

При $d=1$ из леммы 4.8 получаем

Следствие 2. Обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.

§ 5. КОЛЬЦО КЛАССОВ ВЫЧЕТОВ

Вначале докажем следующую теорему.

Теорема 5.1. Пусть m – натуральное число. Каждое целое число a сравнимо по модулю m точно с одним из чисел $0,1,\dots,m-1$, а именно с остатком от деления a на m.

Δ Если $a=mq+r$, $0\le r\le m-1$, где r – остаток от деления a на m, то $a-r=mq$ и $a\equiv r(\mathrm{mod}\,m)$. Итак, каждое целое число сравнимо со своим остатком от деления на m.

Осталось показать, что различные остатки от деления на m не сравнимы по модулю m. Если $0\le r_1<r_2\le m-1$, то $0<r_2-r_1\le m-1$, и $r_2\not\equiv r_1(\mathrm{mod}\,m)$. ▲

Введем теперь следующие подмножества в кольце $\mathbb{Z}$:

$\overline{0}=\{0,\pm m,\pm 2m,\dots\}$ – множество всех чисел, кратных m;

$\overline{1}=\{1,\pm m+1,\pm 2m+1,\dots\}$ – множество всех чисел, которые при делении на m дают остаток 1; . . . . . .

$\overline{r}=\{r,\pm m+r,\pm 2m+r,\dots\}$ – множество всех чисел, которые при делении на m дают остаток r;

. . . . . .

$\overline{m-1}=\{m-1,\pm m+m-1,\pm 2m+m-1,\dots\}$ – множество всех чисел, которые при делении на m дают остаток $m-1$.

По теореме 5.1 каждое целое число попадает точно в одно из этих множеств. Поэтому

$$\mathbb{Z}=\overline{0}\cup\overline{1}\cup\overline{2}\cup\dots\cup\overline{m-1},$$

причем различные подмножества имеют пустое пересечение.

Подмножества $\overline{0},\overline{1},\overline{2},\dots,\overline{m-1}$ называют **классами вычетов по модулю** m. Множество классов вычетов по модулю m обозначают через $\mathbb{Z}_m$. Итак, $\mathbb{Z}_m=\{\overline{0},\overline{1},\dots,\overline{m-1}\}$.

Если a – произвольное целое число, то через $\overline{a}$ обозначим множество всех целых чисел, которые при делении на m дают тот же остаток, что и число a.

Лемма 5.2. Если r – остаток от деления a на m, то $\overline{a}=\overline{r}$.

Δ $\overline{r}\subseteq\overline{a}$ по определению множеств $\overline{r}$ и $\overline{a}$. Ясно, что $a\in\overline{r}$. Если b – произвольное число из $\overline{a}$, то при делении b на m получается в остатке r, т.е. $b\in\overline{r}$ и $\overline{a}\subseteq\overline{r}$. Теперь $\overline{a}=\overline{r}$. ▲

Итак, при любом целом a множество $\overline{a}$ также является классом вычетов по модулю m, и $\overline{a}=\overline{r}\in\mathbb{Z}_m$. Поэтому $\mathbb{Z}_m=\{\overline{a}\mid a\in\mathbb{Z}\}$.

Используя теорему 4.1, получаем

Следствие. Во множестве $\mathbb{Z}_m$ тогда и только тогда $\overline{a}=\overline{b}$, когда $a\equiv b(\mathrm{mod}\,m)$. ▲

Пример 1. $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$, где

$\overline{0}=\{0,\pm 4,\pm 8,\dots\}=\{\dots,-8,-4,0,4,8,\dots\}$;
$\overline{1}=\{1,\pm 4+1,\pm 8+1,\dots\}=\{\dots,-7,-3,1,5,9,\dots\}$;
$\overline{2}=\{2,\pm 4+2,\pm 8+2,\dots\}=\{\dots,-6,-2,2,6,10,\dots\}$;
$\overline{3}=\{3,\pm 4+3,\pm 8+3,\dots\}=\{\dots,-5,-1,3,7,11,\dots\}$.

Кроме того, $\overline{4}=\overline{0}$, $\overline{5}=\overline{1}$, $-\overline{1}=\overline{3}$, $-\overline{2}=\overline{2}$, и т.д. ▲

Для произвольных $\overline{a}$ и $\overline{b}\in\mathbb{Z}_m$ положим

(I) $\overline{a}+\overline{b}=\overline{a+b}$, $\overline{a}\cdot\overline{b}=\overline{ab}$.

Л е м м а 5.3. Равенства (I) задают алгебраические операции на множестве $\mathbb{Z}_m$.

△ В определении алгебраической операции требуется, чтобы каждой паре элементов соответствовал единственный элемент. В $\mathbb{Z}_m$ элементами являются классы вычетов, а в равенствах (I) фигурируют целые числа a и b . Поэтому нам надо показать, что если $\overline{a}=\overline{a}_1$, $\overline{b}=\overline{b}_1$, то $\overline{a+b}=\overline{a_1+b_1}$, $\overline{ab}=\overline{a_1b_1}$.

Воспользуемся свойствами сравнений. Если $\overline{a}=\overline{a}_1$, $\overline{b}=\overline{b}_1$, то $a\equiv a_1$, $b\equiv b_1(mod\,m)$. По лемме 4.3 $a+b\equiv a_1+b_1$ и $ab\equiv a_1b_1(mod\,m)$, т.е. $\overline{a+b}=\overline{a_1+b_1}$ и $\overline{ab}=\overline{a_1b_1}$.

Т е о р е м а 5.4. Множество $\mathbb{Z}_m$ классов вычетов по модулю m с операциями сложения и умножения (I) является коммутативным кольцом с единицей.

△ Легко проверить, что сложение и умножение определено на множестве $\mathbb{Z}_m$, ассоциативно, коммутативно и дистрибутивно. $\overline{0}$ и $\overline{1}$ – нулевой и единичный элементы, т.к. $\overline{a}+\overline{0}=\overline{a+0}=\overline{a}$, $\overline{a}\cdot\overline{1}=\overline{a\cdot1}=\overline{a}$. Класс $\overline{-a}$ будет противоположным элементом к $\overline{a}$: $\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}$. ▲

Кольцо $\mathbb{Z}_m$ называют к о л ь ц о м к л а с с о в в ы ч е т о в п о м о д у л ю m .

П р и м е р 2. Составим таблицы сложения и умножения для кольца $\mathbb{Z}_4$.

△ $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$

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

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

На пересечении строки $\overline{a}$ и столбца $\overline{b}$ в таблице сложения ставится сумма $\overline{a+b}$, в таблице умножения – произведение $\overline{ab}$.

Обратим внимание на то, что $\overline{2}\cdot\overline{2}=\overline{0}$, т.е. в кольце $\mathbb{Z}_4$ имеются делители нуля.

Л е м м а 5.5. Элемент $\overline{a}$ кольца $\mathbb{Z}_m$ обладает обратным тогда и только тогда, когда числа a и m взаимно просты.

△ Пусть элемент $\overline{a}$ обладает в кольце $\mathbb{Z}_m$ обратным. Это означает, что существует $\overline{b}\in\mathbb{Z}_m$ такой, что $\overline{a}\cdot\overline{b}=\overline{ab}=\overline{1}$. В этом случае $ab\equiv1(mod\,m)$, т.е. $ab-1=mc$ и $ab+m(-c)=1$. По теореме I.8 целые числа a и m – взаимно просты.

Обратно, Пусть целые a и m – взаимно просты. По теореме I.8 существуют целые u и v такие, что $au+mv=1$. Теперь $au-1=m(-v)$ и $au\equiv1(mod\,m)$. Это означает, что $\overline{au}=\overline{a}\cdot\overline{u}=\overline{1}$ и $\overline{u}$ – обратный элемент к $\overline{a}$.

Т е о р е м а 5.6. Кольцо классов вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда m – простое число.

△ Пусть $\mathbb{Z}_m$ – поле. Тогда каждый из элементов $\overline{1},\overline{2},\dots,\overline{m-1}$ обладает обратным. Если $m=st$ – составное число, $1<s<m-1$, то s и m не взаимно просты, и по лемме 5.5 элемент $\overline{s}$ не обладает обратным, противоречие. Итак, если $\mathbb{Z}_m$ – поле, то m – простое число.

Обратно, Пусть m – простое число. Тогда каждое из чисел $1,2,\dots,m-1$ взаимно просто с m , и каждый из элементов $\overline{1},\overline{2},\dots,\overline{m-1}$ обладает в $\mathbb{Z}_m$ обратным по лемме 4.5. Вместе с теоремой 5.4 это доказывает, что $\mathbb{Z}_m$ – поле.

П р и м е р 3. В кольце $\mathbb{Z}_4$ указать противоположные элементы и обратные.

△ Из таблицы сложения для $\mathbb{Z}_4$ противоположные элементы определяем следующим образом. В строке $\overline{a}$ находим нулевой элемент $\overline{0}$. Если он стоит в столбце $\overline{b}$, то $\overline{a}+\overline{b}=\overline{0}$ и $\overline{b}$ – противоположный элемент для $\overline{a}$.

Итак, $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{3}$, $-\overline{2}=\overline{2}$, $-\overline{3}=\overline{1}$.

Точно также поступаем с обратными, только в таблице умножения вместо нулевого элемента находим единичный: $\overline{1}^{-1}=\overline{1}$, $\overline{3}^{-1}=\overline{3}$. Элементы $\overline{0}$ и $\overline{2}$ обратным не обладают.

§6. ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Нам известны следующие множества чисел:

$\mathbb{N}$ – множество натуральных чисел;
$\mathbb{Z}$ – кольцо целых чисел;
$\mathbb{Q}$ – поле рациональных чисел;
$\mathbb{R}$ – поле действительных чисел.

Натуральные числа возникают при счете отдельных предметов. Кольцо целых чисел является расширением множества натуральных чисел, но целых чисел недостаточно даже для решения уравнений первой степени с одним неизвестным: $px+q=0$. Рациональные числа $\mathbb{Q}=\{p/q \mid p,q\in\mathbb{Z}, q\neq 0\}$ расширяют кольцо целых чисел, но в поле рациональных чисел невозможно извлекать квадратные корни. Например, $\sqrt{2}$ – не рациональное число. Поле $\mathbb{R}$ действительных чисел расширяет множество рациональных чисел, но в $\mathbb{R}$ простейшие квадратные уравнения не имеют решения.

Поставим следующую задачу: расширить поле действительных чисел так, чтобы в новом поле имело решение уравнение

(I) $$x^2+1=0.$$

ПОСТРОЕНИЕ ПОЛЯ КОМПЛЕКСНЫХ ЧИСЕЛ. Рассмотрим множество упорядоченных пар (a,b) действительных чисел

$$\mathbb{C}=\{(a,b) \mid a,b\in\mathbb{R}\}.$$

Две пары (a_1,b_1) и (a_2,b_2) считаются равными, если $a_1=a_2$, $b_1=b_2$.

Введем операцию сложения

(2) $$(a,b)+(c,d)=(a+c,b+d).$$

Лемма 6.1. Множество $\mathbb{C}$ с операцией сложения (2) является абелевой группой.

△ Так как $a+c$ и $b+d\in\mathbb{R}$, то сложение определено на $\mathbb{C}$. Оно коммутативно

$$(c,d)+(a,b)=(c+a,d+b)=(a+c,b+d)=(a,b)+(c,d)$$

и ассоциативно

$$((a,b)+(c,d))+(f,g)=(a+c,b+d)+(f,g)=$$
$$=(a+c+f,b+d+g)=(a,b)+(c+f,d+g)=$$
$$=(a,b)+((c,d)+(f,g))$$

Пара $(0,0)$ является нулевым элементом в $\mathbb{C}$:

$$(a,b)+(0,0)=(a+0,b+0)=(a,b),$$

а пара $(-a,-b)$ – противоположным элементом к паре (a,b):

$$(a,b)+(-a,-b)=(0,0).$$ ▲

На множестве $\mathbb{C}$ введем операцию умножения

(3) $$(a,b)(c,d)=(ac-bd,ad+bc)$$

Лемма 6.2. Множество $\mathbb{C}^*=\mathbb{C}\setminus\{0,0\}$ с операцией умножения является абелевой группой.

△ Так как $ac-bd$ и $ad+bc\in\mathbb{R}$, то умножение определено на $\mathbb{C}$. Оно коммутативно

$$(c,d)(a,b)=(ca-db,cb+da)=(ac-bd,$$
$$ad+bc)=(a,b)(c,d)$$

и ассоциативно

$$((a,b)(c,d))(f,g)=(ac-bd,ad+bc)(f,g)=$$
$$=((ac-bd)f-(ad+bc)g,(ac-bd)g+(ad+bc)f)=$$

$= (ac\xi - bd\xi - ad\eta - b c\eta, ac\eta - bd\eta + ad\xi +$

$+ bc\xi) = (a(c\xi - d\eta) - b(d\xi + c\eta), a(c\eta + d\xi) + b(c\xi -$

$- d\eta)) = (a, b)(c\xi - d\eta, d\xi + c\eta) = (a, b)((c, d)(\xi, \eta)).$

Пара $(1,0)$ – единичный элемент:

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

Пара $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ – обратный элемент к паре (a,b):

$$(a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(a\,\frac{a}{a^2+b^2} - b\,\frac{-b}{a^2+b^2},\right.$$

$$\left. a\,\frac{-b}{a^2+b^2} + b\,\frac{a}{a^2+b^2}\right) = (1,0).$$

Заметим, что $a^2 + b^2 \neq 0$ для каждой ненулевой пары (a,b). Поэтому обратные элементы существуют для всех элементов из $\mathbb{C}^*$.

Теорема 6.3. Множество $\mathbb{C}$ с операциями сложения (2) и умножения (3) являются полем.

△ В силу лемм 6.1 и 6.2 остается показать только дистрибутивность сложения относительно умножения:

$$(a,b)((c,d)+(\xi,\eta)) = (a,b)(c+\xi, d+\eta) =$$

$$= (a(c+\xi) - b(d+\eta), a(d+\eta) + b(c+\xi)) =$$

$$= (ac - bd + a\xi - b\eta, ad + bc + a\eta + b\xi) =$$

$$= (ac - bd, ad + bc) + (a\xi - b\eta, a\eta + b\xi) =$$

$$= (a,b)(c,d) + (a,b)(\xi,\eta). \quad ▲$$

Построенное поле $\mathbb{C}$ называют **полем комплексных чисел**, а элементы поля $\mathbb{C}$ – **комплексными числами**.

КОМПЛЕКСНЫЕ ЧИСЛА В АЛГЕБРАИЧЕСКОЙ ФОРМЕ. Пары $(a,0)$, $a \in \mathbb{R}$ складываются и умножаются как действительные числа:

$$(a,0) + (b,0) = (a+b,0)$$

$$(a,0)(b,0) = (ab - 0\cdot 0, a\cdot 0 + 0\cdot b) = (ab,0).$$

Это позволяет нам отождествлять пару $(a,0)$ с действительным числом a, т.е. положить $(a,0) = a$. Поле $\mathbb{R}$ действительных чисел становится подполем поля $\mathbb{C}$ комплексных чисел.

Пару $(0,1)$ обозначим через i. Так как: $bi = (b,0)(0,1) = (b\cdot 0 - 0\cdot 1, b\cdot 1 + 0\cdot 0) = (0,b)$, то $(a,b) = (a,0) + (0,b) = a + bi$. Кроме того, $i^2 = (0,1)(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 0\cdot 1) = (-1,0) = -1$, т.е. i является решением уравнения (I).

Запись $a + bi$ называется **алгебраической формой комплексного числа** (a,b), число a – его **действительной частью**, а bi – **мнимой частью**. Сложение (2) и умножение (3) в алгебраической форме записываются так:

$$(a+bi) + (c+di) = a + c + (b+d)i$$

$$(a+bi)(c+di) = ac - bd + (ad + bc)i.$$

В частности, при умножении комплексных чисел раскрываются скобки и заменяется i^2 на -1.

Итак, $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$ – поле комплексных чисел, $\mathbb{R} \subseteq \mathbb{C}$ и в $\mathbb{C}$ уравнение (I) имеет решение $x = i$. Поставленная задача решена.

СОПРЯЖЕННЫЕ КОМПЛЕКСНЫЕ ЧИСЛА. Для комплексного числа $z = a + bi$ комплексное число $a - bi$ называется сопряженным и обозначается через $\overline{z}$. Итак, у сопряженных чисел действительные части совпадают, а мнимые – взаимно противоположны.

Очевидно, что $\overline{z} = z$ тогда и только тогда, когда z – действительное число.

Лемма 6.4. Сумма и произведение двух сопряженных комплексных чисел являются действительными числами.

△ Пусть $z = a + bi$. Тогда $\overline{z} = a - bi$ и

$z + \overline{z} = (a+bi) + (a-bi) = 2a$, $z\overline{z} = (a+bi)(a-bi) = a^2 - (bi)^2 = a^2 + b^2$.

Лемма 6.5. (1) $\overline{z+w} = \overline{z} + \overline{w}$; (2) $\overline{zw} = \overline{z}\,\overline{w}$; (3) $\overline{z^k} = \overline{z}^k$ для $k \in \mathbb{N}$.

△ Пусть $z = a + bi$, $w = c + di$. Тогда $\overline{z+w} = \overline{a+bi+c+di} = \overline{a+c+(b+d)i} = a+c-(b+d)i = a-bi+c-di = \overline{z} + \overline{w}$. Далее $\overline{zw} = \overline{(a+bi)(c+di)} = \overline{ac-bd+(ad+bc)i} = ac-bd-(ad+bc)i = (a-bi)(c-di) = \overline{z}\cdot\overline{w}$. Свойство (3) получается индукцией по k из (2).

Пример 1. Вычислить $\frac{3+2i}{7-2i}$ и $\left(\frac{1-2i}{1+2i}\right)^5$.

△ Умножим числитель и знаменатель на число сопряженное знаменателю

$$\frac{3+2i}{7-2i}\cdot\frac{7+2i}{7+2i} = \frac{(21-4)+(6+14)i}{7^2-(2i)^2} = \frac{17}{53} + \frac{20}{53}i$$

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

$$\left(\frac{1-2i}{1+2i}\right)^5 = \left(-\frac{3}{5} - \frac{4}{5}i\right)^5 = \frac{-1}{5^5}(3+4i)^5 = -\frac{1}{125}(27+108i-$$

$$-144-64i) = -\frac{1}{125}(-117+44i).$$

ИЗВЛЕЧЕНИЕ КВАДРАТНОГО КОРНЯ. Пусть нам надо извлечь квадратный корень из комплексного числа $z = a + bi$. Положим $x + yi = \sqrt{a+bi}$. Возведем обе части в квадрат $x^2 - y^2 + 2yxi = a + bi$. Приравнивая действительные и мнимые части, получаем систему

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \qquad \begin{cases} (x^2-y^2)^2 = a^2 \\ 4x^2y^2 = b^2 \end{cases}$$

$$(x^2+y^2) = a^2+b^2$$

$$\begin{cases} x^2+y^2 = \sqrt{a^2+b^2} \\ x^2-y^2 = a \end{cases}$$

$$2x^2 = \sqrt{a^2+b^2} + a \qquad x = \delta_1\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}$$

$$2y^2 = \sqrt{a^2+b^2} - a \qquad y = \delta_2\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

где $\delta_1 = \pm 1 = \delta_2$. Но из первой системы $xy = \frac{b}{2}$. Поэтому при $b > 0$ произведение $\delta_1\delta_2 = 1$, а при $b < 0$ – $\delta_1\delta_2 = -1$. В общем случае эту зависимость можно записать используя функцию "знак": $\delta_2 = \delta_1 \operatorname{sgn} b$. Итак,

$$(4) \qquad \sqrt{a+bi} = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\operatorname{sgn} b\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right).$$

Пример 3. Вычислить $\sqrt{6+8i}$.

△ По формуле (4) имеем $\sqrt{6+8i} = \pm(\sqrt{3}+i\sqrt{1})$.

Проверка: $(\pm\sqrt{3}+i\sqrt{1})^2 = 3-1+2i\sqrt{3}\cdot 1 = 6+8i$. ▲

Так как $i^2 = -1$, то i – корень уравнения (I). Другой корень – число $(-i)$.

Пусть $az^2 + bz + c = 0$ – квадратное уравнение над полем комплексных чисел, т.е. $a, b, c \in \mathbb{C}$. Повторяя вывод формулы корней квадратного уравнения с действительными коэффициентами, который известен из школьного курса математики, для квадратного уравнения с комплексными коэффициентами, получаем ту же формулу

$$(5) \qquad z_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

Пример 4. Решить квадратное уравнение

$$z^2-(2+4i)z+\left(-\frac{9}{2}+2i\right)=0$$

△ Находим дискриминант $D=v^2-4uw=6+8i$.

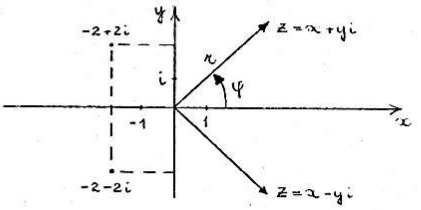
$$z_1=\frac{2+4i+\sqrt{3}+i\sqrt{2}}{2}=1+\sqrt{2}+\left(2+\frac{\sqrt{2}}{2}\right)i,$$

$$z_2=\frac{2+4i-(\sqrt{3}+i\sqrt{2})}{2}=1-\sqrt{2}+\left(2-\frac{\sqrt{2}}{2}\right)i.$$

§ 7. ТРИГОНОМЕТРИЧЕСКАЯ ФОРМА КОМПЛЕКСНЫХ ЧИСЕЛ

Действительные числа можно изображать точками на числовой оси. Комплексное число $z=a+bi$ задается двумя действительными числами a и b, поэтому естественно изображать комплексные числа точками на плоскости.

ИЗОБРАЖЕНИЕ КОМПЛЕКСНЫХ ЧИСЕЛ НА ПЛОСКОСТИ. Введем на плоскости прямоугольную систему координат и будем изображать комплексное число $z=a+bi$ точкой на плоскости с координатами $(a;b)$. В частности, числу i ставится в соответствие точка $(0;1)$. Действительным числам соответствуют точки оси абсцисс, а чисто мнимым числам – точки оси ординат.



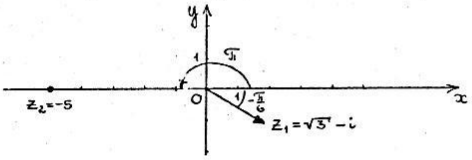
Положение точки $z=x+yi$ вполне определяется ее полярными координатами r и φ, где r – расстояние от начала координат до z, а φ – угол между положительным направлением оси абсцисс и направлением из начала координат на точку z. Полярные координаты точки $z=x+yi$ определяют x и y по известным формулам: $x=r\cos\varphi$, $y=r\sin\varphi$, поэтому $z=x+yi=r(\cos\varphi+i\sin\varphi)$. Запись

$$z=r(\cos\varphi+i\sin\varphi)$$

называется **тригонометрической формой комплексного числа** z. Неотрицательное число r называют **модулем** комплексного числа z и обозначают через $|z|$. Ясно, что $|z|=\sqrt{x^2+y^2}$. Угол φ называют **аргументом** числа z и обозначают через $\arg z$. Очевидно $\varphi=\arg z=\operatorname{arctg}\frac{y}{x}$. Аргумент любого комплексного числа $z\neq 0$ имеет бесконечно много значений, отличающихся друг от друга на числа, кратные 2π.

Пример 1. Представить в тригонометрической форме числа $z_1=\sqrt{3}-i$; $z_2=-5$; $z_3=-3\left(\cos\frac{\pi}{5}-i\sin\frac{\pi}{5}\right)$.

△ Изобразим числа z_1, z_2 на плоскости



Для числа $z_1=\sqrt{3}-i$ имеем: $|z_1|=\sqrt{(\sqrt{3})^2+(-1)^2}=2$, $\sin\varphi=-\frac{1}{2}$, $\cos\varphi=\frac{\sqrt{3}}{2}$ и $\varphi=-\frac{\pi}{6}$. Значит, $z_1=\sqrt{3}-i=2(\cos(-\pi/6)+i\sin(-\pi/6))$.

Для $z_2=-5$ имеем $|z_2|=5$, $\varphi=\pi$ и $z_2=-5=5(\cos\pi+i\sin\pi)$.

Комплексное число $z_3=-3\left(\cos\frac{\pi}{5}-i\sin\frac{\pi}{5}\right)$ записано не в тригонометрической форме, так как отрицательное число

-3 нельзя считать модулем z_3. Кроме того, коэффициент мнимой части равен $-\sin\frac{\pi}{5}$, а в тригонометрической форме мнимая часть должна быть записана так: $i\sin\varphi$. Представим число z_3 в виде

$$z_3 = 3\left(-\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)$$

Отсюда заключаем, что аргументом комплексного числа z_3 является такой угол φ, что $\cos\varphi = -\cos\frac{\pi}{5}$, а $\sin\varphi = \sin\frac{\pi}{5}$. Такой угол легко найти: $\varphi = \pi - \frac{\pi}{5} = \frac{4}{5}\pi$. Итак, искомое представление в тригонометрической форме есть

$$z_3 = 3\left(\cos\tfrac{4}{5}\pi + i\sin\tfrac{4}{5}\pi\right)$$

Ответ: $z_1 = 2\left(\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)\right)$

$$z_2 = 5\left(\cos\pi + i\sin\pi\right)$$

$$z_3 = 3\left(\cos\tfrac{4}{5}\pi + i\sin\tfrac{4}{5}\pi\right)$$

УМНОЖЕНИЕ И ДЕЛЕНИЕ КОМПЛЕКСНЫХ ЧИСЕЛ В ТРИГОНОМЕТРИЧЕСКОЙ ФОРМЕ

Теорема 7.1. При умножении комплексных чисел в тригонометрической форме их модули перемножаются, а аргументы складываются.

△ Возьмем два произвольных комплексных числа $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$ и перемножим их

$$z_1 \cdot z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\cos\varphi_1\sin\varphi_2 +$$

$$+ \sin\varphi_1\cos\varphi_2)) = r_1 r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)).$$

Так как $r_1 r_2 \geq 0$, то $r_1 r_2 = |z_1 z_2|$ – модуль, а $\varphi_1 + \varphi_2$ – аргумент произведения двух данных чисел.

Теорема 7.2. При делении комплексных чисел их модули делятся, а аргументы вычитаются. В частности,

$$z^{-1} = \frac{1}{|z|}\left(\cos(-\arg z) + i\sin(-\arg z)\right).$$

△ Если $z_3 = z_1/z_2$, то $z_1 = z_3 z_2$ и можно применить теорему 7.1: $|z_1| = |z_3||z_2|$, $\arg z_1 = \arg z_3 + \arg z_2$. Отсюда $|z_3| = |z_1|/|z_2|$ и $\arg z_3 = \arg z_1 - \arg z_2$, т.е. при делении комплексных чисел их модули делятся, а аргументы вычитаются.

Так как $1 = \cos 0 + i\sin 0$, то $z^{-1} = \frac{1}{z} =$

$$= \frac{\cos 0 + i\sin 0}{|z|(\cos(\arg z) + i\sin(\arg z))} = \frac{1}{|z|}\left(\cos(0 - \arg z) +\right.$$

$$\left. + i\sin(0 - \arg z)\right) = |z|^{-1}(\cos(-\arg z) + i\sin(-\arg z)).$$

Пример 2. Вычислить $z_1 z_2 z_3$, $z_1 z_2 / z_3$ и z_1^{-1}, где z_1, z_2 и z_3 – комплексные числа из примера I.

△ $z_1 z_2 z_3 = 2\cdot 5\cdot 3\left(\cos\left(-\frac{\pi}{6} + \pi + \frac{4}{5}\pi\right) +\right.$

$$\left. + i\sin\left(-\frac{\pi}{6} + \pi + \frac{4}{5}\pi\right)\right) = 30\left(\cos\tfrac{49}{30}\pi + i\sin\tfrac{49}{30}\pi\right);$$

$$\frac{z_1 z_2}{z_3} = \frac{2\cdot 5}{3}\left(\cos\left(-\frac{\pi}{6} + \pi - \frac{4}{5}\pi\right) + i\sin\left(-\frac{\pi}{6} + \pi - \frac{4}{5}\pi\right)\right) =$$

$$= \frac{10}{3}\left(\cos\tfrac{\pi}{30} + i\sin\tfrac{\pi}{30}\right);$$

$$z_1^{-1} = \frac{1}{2}\left(\cos\tfrac{\pi}{6} + i\sin\tfrac{\pi}{6}\right).$$

ВОЗВЕДЕНИЕ В СТЕПЕНЬ КОМПЛЕКСНОГО ЧИСЛА. ФОРМУЛА МУАВРА.

Теорема 7.3. При возведении в степень комплексного числа $z = |z|(\cos\varphi + i\sin\varphi)$ с целым показателем n его модуль возводится в степень, а аргумент умножается на показатель:

(I) $\left(|z|(\cos\varphi+i\sin\varphi)\right)^n=|z|^n(\cos n\varphi+i\sin n\varphi)$

△ При натуральном n утверждение следует из теоремы 7.1 по индукции. Так как $z^0=1$, то для $n=0$ утверждение также имеет место. Поэтому формула (I) справедлива для всех $n\geq 0$. При отрицательном n число $(-n)$ натуральное и к комплексному числу z^{-1} применима формула (I):

$$z^n=(z^{-1})^{-n}=\left(|z^{-1}|\left(\cos(-\varphi)+i\sin(-\varphi)\right)\right)^{(-n)}=$$

$$=|z^{-1}|^{(-n)}\left(\cos(-n)(-\varphi)+i\sin(-n)(-\varphi)\right)=$$

$$=|z|^n(\cos n\varphi+i\sin n\varphi).\quad\blacktriangle$$

Формула (I) называется формулой Муавра.
При $|z|=1$ получаем

$$\cos n\varphi+i\sin n\varphi=(\cos\varphi+i\sin\varphi)^n.$$

Последнее равенство можно использовать для выражения синусов и косинусов кратных углов через синусы и косинусы угла φ. Например, при $n=3$ имеем $\cos 3\varphi+i\sin 3\varphi=(\cos\varphi+i\sin\varphi)^3=\cos^3\varphi+3\cos^2\varphi\sin\varphi\cdot i-3\cos\varphi\sin^2\varphi-\sin^3\varphi\cdot i$. Приравнивая действительные и мнимые части, получаем

$$\cos 3\varphi=\cos^3\varphi-3\cos\varphi\cdot\sin^2\varphi$$

$$\sin 3\varphi=-\sin^3\varphi+3\cos^2\varphi\sin\varphi.$$

Пример 3. Вычислить $(z_1z_3)^{30}$, где z_1 и z_3 – комплексные числа из примера 1:

△ $(z_1z_3)^{30}=(2\cdot 3)^{30}\left(\cos 30\left(-\frac{\pi}{6}+\frac{4}{5}\pi\right)+i\sin 30\left(-\frac{\pi}{6}+\right.\right.$

$\left.\left.+\frac{4}{5}\pi\right)\right)=6^{30}\left(\cos 19\pi+i\sin 19\pi\right)=6^{30}(\cos\pi+i\sin\pi)=-6^{30}$.

ИЗВЛЕЧЕНИЕ КОРНЯ ИЗ КОМПЛЕКСНОГО ЧИСЛА. Корнем n-й степени из комплексного числа z называется такое комплексное число c, что $c^n=z$. Корень n-й степени из z обозначается через $\sqrt[n]{z}$. Таким образом, если $c=\sqrt[n]{z}$, то $c^n=z$.

Теорема 7.4. Пусть z – комплексное и n – натуральное числа. В поле комплексных чисел корень $\sqrt[n]{z}$ при $z=0$ имеет единственное значение $z=0$, а при $z\neq 0$ n различных значений. Если $z=|z|(\cos\varphi+i\sin\varphi)$, то эти значения находятся по формуле

(2) $\sqrt[n]{z}=\sqrt[n]{|z|}\left(\cos\frac{\varphi+2k\pi}{n}+i\sin\frac{\varphi+2k\pi}{n}\right)$,

$k=0,1,\ldots,n-1$.

△ Поскольку $0^n=0$ и $z^n=0$ следует, что $z=0$, то $\sqrt[n]{0}$ имеет единственное значение $z=0$. Пусть теперь $z=|z|(\cos\varphi+i\sin\varphi)$. Из положительных действительных чисел корни извлекать можно, поэтому существует число $\sqrt[n]{|z|}$ и можно рассматривать комплексное число

$$c_k=\sqrt[n]{|z|}\left(\cos\frac{\varphi+2k\pi}{n}+i\sin\frac{\varphi+2k\pi}{n}\right)$$

при любом целом k. По формуле Муавра

$$c_k^n=|z|\left(\cos(\varphi+2k\pi)+i\sin(\varphi+2k\pi)\right),$$

т.е. c_k – корень n-й степени из комплексного числа z.

При $k=0,1,\ldots,n-1$ значения c_k попарно различны, так как увеличение k на единицу влечет увеличение аргумента на $2\pi/n$.

Пусть теперь k произвольно и $k=nq+r$, $0\leq r\leq n-1$. Тогда $\frac{\varphi+2k\pi}{n}=\frac{\varphi+2(nq+r)\pi}{n}=$ $=\frac{\varphi+2r\pi}{n}+2q\pi$, а так как $\cos\varphi$ и $\sin\varphi$ – периодические функции с периодом 2π, то $c_k=c_r$. Итак, только при $k=0,1,\ldots,n-1$ получаются различные значения корня.

Наконец, если $\rho(\cos\alpha+i\sin\alpha)$ – произвольный корень n-й степени из z, то $\rho^n(\cos n\alpha+i\sin n\alpha)=z=$ $=|z|(\cos\varphi+i\sin\varphi)$, откуда $\rho=\sqrt[n]{|z|}$, $\alpha=\varphi/n$, т.е.

любой корень представим формулой (2).

Пример 4. Вычислить $\sqrt[3]{-5}$.

△ Число (-5) в тригонометрической форме записывается так $-5=5(\cos\pi+i\sin\pi)$. По формуле (2) имеем

$$c_k=\sqrt[3]{-5}=\sqrt[3]{5}\left(\cos\frac{\pi+2\pi k}{3}+i\sin\frac{\pi+2\pi k}{3}\right)$$

$k=0,1,2$. Отсюда

$$c_0=\sqrt[3]{5}\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)=\sqrt[3]{5}\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=\frac{\sqrt[3]{5}}{2}(1+i\sqrt{3});$$

$$c_1=\sqrt[3]{5}\left(\cos\pi+i\sin\pi\right)=-\sqrt[3]{5};$$

$$c_2=\sqrt[3]{5}\left(\cos\frac{5}{3}\pi+i\sin\frac{5}{3}\pi\right)=\sqrt[3]{5}\left(\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)=\frac{\sqrt[3]{5}}{2}(1-i\sqrt{3}).$$

КОРНИ ИЗ ЕДИНИЦЫ. Так как $1=\cos0+i\sin0$, то из теоремы 7.4 получаем следующее утверждение.

Теорема 7.5. В поле комплексных чисел имеется n различных значений корня n-й степени из единицы, которые находятся по формуле

(3) $\varepsilon_k=\sqrt[n]{1}=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, $k=0,1,\dots,n-1$.

Пример 5. Вычислить $\sqrt[n]{1}$ при $n\le4$.

△ При $n=2$ имеем два корня $\varepsilon_0=1$; $\varepsilon_1=-1$.
При $n=3$ имеем три корня: $\varepsilon_0=1$; $\varepsilon_1=\cos\frac{2}{3}\pi+i\sin\frac{2}{3}\pi=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$; $\varepsilon_2=\cos\frac{4}{3}\pi+i\sin\frac{4}{3}\pi=-\frac{1}{2}-i\frac{\sqrt{3}}{2}$.
При $n=4$ имеем четыре корня: $\varepsilon_0=1$; $\varepsilon_1=\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}=i$; $\varepsilon_2=\cos\pi+i\sin\pi=-1$; $\varepsilon_3=\cos\frac{3}{2}\pi+i\sin\frac{3}{2}\pi=-i$.

Теорема 7.6. Корни n-й степени из единицы составляют циклическую группу $\langle\varepsilon_1\rangle$ порядка n, порожденную корнем ε_1.

△ Множество $\mathbb{C}^*=\mathbb{C}\setminus\{0\}$ комплексных чисел, отличных от нуля, образует мультипликативную группу. Из (3) получаем

$\varepsilon_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$, а по формуле Муавра $\varepsilon_1^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}=\varepsilon_k$. В частности, $\varepsilon_1^n=\varepsilon_0$ и ε_1 - элемент порядка n в группе $\mathbb{C}^*$. Кроме того, из равенства $\varepsilon_1^k=\varepsilon_k$ следует, что циклическая группа $\langle\varepsilon_1\rangle$, порожденная элементом ε_1, совпадает с множеством $\{\varepsilon_0,\varepsilon_1,\dots,\varepsilon_{n-1}\}$ всех корней из единицы. ▲

Корень n-й степени из единицы называется примитивным или первообразным, если он не является корнем из единицы никакой меньшей степени. Итак, ε_m - примитивный корень степени n из единицы, если $\varepsilon_m^n=1$ и $\varepsilon_m^k\ne1$ для всех $0<k<n$.

Теорема 7.7. Корень ε_m n-й степени из единицы будет примитивным тогда и только тогда, когда m и n взаимно просты. В частности, ε_1 и ε_{n-1} - примитивные корни n-й степени.

△ Пусть $d=НОД(m,n)$. Тогда $m=dm_1$, $n=dn_1$ и $(\varepsilon_m)^{n_1}=\varepsilon_{m_1}^{mn_1}=\varepsilon_1^{mn_1}=\varepsilon_1^{mn}=1$.
Если $d>1$, $1<n_1<n$ и ε_m не примитивный. Поэтому если ε_m примитивный, то m и n взаимно просты.
Пусть $d=1$, т.е. m и n взаимно просты. Допустим, что ε_m является корнем k-й степени из единицы, $k<n$. Тогда $\varepsilon_m^k=\varepsilon_1^{mk}=1$. Так как ε_1 имеет порядок n, то mk делится на n. Теперь k делится на n по теореме 1.7, противоречие.

Пример 6. Корни четвертой степени из единицы исчерпываются числами $\varepsilon_1=i$, $\varepsilon_2=-1$, $\varepsilon_3=-i$, $\varepsilon_4=1$. Поэтому $\langle\varepsilon_4\rangle=\{1,-1,-i,i\}$ - циклическая группа порядка 4. Примитивными будут корни $\varepsilon_1=i$ и $\varepsilon_3=-i$.

§8. ПОСТРОЕНИЕ КОЛЬЦА МНОГОЧЛЕНОВ

Пусть A - произвольное кольцо с единицей 1. Построим новое кольцо B, элементами которого являются бесконечные

упорядоченные последовательности

(I) $f=(f_0, f_1, \dots, f_n, \dots)$, $f_i \in A$

с конечным числом ненулевых элементов. В каждой такой последовательности, начиная с некоторого номера, все члены равны нулевому элементу кольца A.

Две последовательности $f=(f_0,\dots)$ и $g=(g_0,\dots)$ считаются р а в н ы м и лишь тогда, когда $f_i=g_i$ для всех i.

Введем на множестве B операцию сложения

(2) $f+g=(f_0, f_1, \dots, f_n, \dots)+(g_0, g_1, \dots, g_n, \dots)=$
$=(f_0+g_0, f_1+g_1, \dots, f_n+g_n, \dots)$.

Если в последовательности f нулевыми будут члены, начиная с номера k, а в последовательности g – с номера ℓ, то в последовательности $f+g$ нулевыми будут все члены, начиная с номера $\max\{k,\ell\}$. Поэтому $f+g \in B$ и сложение определено на множестве B.

Ясно, что сложение ассоциативно и коммутативно. Последовательность $(0,0,\dots)$ будет нулевым элементом, а $(-f_0,-f_1,\dots)=-f$ – противоположным элементом к последовательности f.

Итак, множество B с операцией сложения (2) становится абелевой группой.

Введем умножение на множестве B:

(3) $f\cdot g=h=(h_0, h_1, \dots, h_n, \dots)$,

где $h_s=\sum_{i+j=s} f_i g_j$, $s=0,1,\dots$.

В частности, $h_0=f_0g_0$, $h_1=f_0g_1+f_1g_0$, $h_2=f_0g_2+f_1g_1+f_2g_0$, $h_3=f_0g_3+f_1g_2+f_2g_1+f_3g_0$, и т.д.

Если в последовательности f нулевыми будут члены, начиная с номера k, а в g – с номера ℓ, то в последовательности $h=fg$ нулевыми будут все члены, начиная с номера $k+\ell$. Действительно $h_{k+\ell-1}=\sum_{i+j=k+\ell-1} f_i g_j = f_0 g_{k+\ell-1} + f_1 g_{k+\ell-2} + \dots + f_{k-1} g_\ell + f_k g_{\ell-1} + \dots + f_{k+\ell-1} g_0 = 0$

для всех $k, \ell \geq 0$. Поэтому умножение определено на множестве B.

Так как $h_s=\sum_{i+j=s} f_i g_j = \sum_{j+i=s} g_j f_i$ и $\sum_{j+i=s} g_j f_i$ является s-м членом последовательности gf, то $fg=gf$ и умножение коммутативно.

Проверим ассоциативность умножения и дистрибутивность умножения относительно сложения. Пусть $f=(f_0,\dots,f_n,\dots)$; $g=(g_0,\dots,g_n,\dots)$; $h=(h_0,\dots,h_n,\dots)$ – три произвольных элемента множества B. Пусть $fg=d=(d_0,\dots,d_n,\dots)$, где $d_k=\sum_{i+j=k} f_i g_j$, $k=0,1,\dots$; $gh=b=(b_0,\dots,b_n,\dots)$, где $b_t=\sum_{j+\ell=t} g_j h_\ell$.

Тогда $(fg)h=dh=a=(a_0,\dots,a_n,\dots)$, где

$$a_s=\sum_{k+\ell=s} d_k h_\ell = \sum_{k+\ell=s}\Big(\sum_{i+j=k} f_i g_j\Big) h_\ell = \sum_{i+j+\ell=s} f_i g_j h_\ell .$$

Далее, $f(gh)=fb=c=(c_0,\dots,c_n,\dots)$, где

$c_s=\sum_{i+t=s} f_i b_t = \sum_{i+t=s} f_i\Big(\sum_{j+\ell=t} g_j h_\ell\Big)=\sum_{i+j+\ell=s} f_i g_j h_\ell$ и $a_s=c_s$. Поэтому $(fg)h=f(gh)$ и умножение ассоциативно.

Далее, $fg+hg=fg+gh=d+b=(d_0+b_0,\dots,d_n+b_n,\dots)$, где $d_k+b_k=\sum_{i+j=k} f_i g_j+\sum_{j+i=k} g_j h_i=\sum_{i+j=k}(f_i g_j+h_i g_j)=$

$=\sum_{i+j=k}(f_i+h_i)g_j$ и $fg+hg=(f+h)g$.

Таким образом, умножение дистрибутивно относительно сложения.

Так как $(f_0,\dots,f_n,\dots)(1,0,\dots,0,\dots)=(f_0,\dots,f_n,\dots)$, то B – ассоциативное кольцо с единицей $(1,0,\dots,0,\dots)$.

Последовательности $(a,0,\dots,0,\dots)$ складываются и умножаются также, как элементы кольца A. Это позволяет отождествить такие последовательности с соответствующими элементами A, т.е. положить $a=(a,0,\dots)$ для всех $a\in A$. Тем самым A становится подкольцом кольца B. Обозначим далее $(0,1,0,\dots,0,\dots)$ через x и назовем x – п е р е м е н н о й над A или н е и з в е с т н о й над A. Используя введенные на B операции умножения, находим, что

$$x = (0,1,0,0,\dots,0,\dots)$$

$$x^2 = (0,0,1,0,\dots,0,\dots)$$

$$x^3 = (0,0,0,1,\dots,0,\dots)$$

$$\cdot \quad \cdot \quad \cdot$$

$$x^n = (0,0,0,0,\dots,f_n=1,\dots,0).$$

Кроме того, $(0,\dots,0,f_n=a,0,\dots) = (a,0,0,\dots)\times$
$\times(0,0,\dots,0,f_n=1,0,\dots) = a x^n = x^n a = (0,0,\dots$
$\dots,0,f_n=1,0,\dots)(a,0,0,\dots)$.

Итак, если f_n – последний отличный от нуля член последовательности $f=(f_0,\dots,f_n,\dots)$, то в новых обозначениях

$$f = (f_0,f_1,\dots,f_n,0,0,\dots) = (f_0,\dots,f_{n-1},0,0,\dots) + f_n x^n = (f_0,f_1,\dots,f_{n-2},0,\dots) + f_{n-1}x^{n-1} + f_n x^n = \dots$$
$$\dots = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n.$$

Таким образом, каждый элемент кольца B принимает вид

$$f = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n.$$

Построенное кольцо B называют **кольцом многочленов над A от одной переменной x** и обозначают через $A[x]$. Элементы кольца $A[x]$ называют **многочленами** или **полиномами**. Более привычной является запись многочлена по убывающим степеням x, т.е. в виде

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

Элементы $a_0, a_1, \dots, a_n$ называются **коэффициентами**. **Нулевой** многочлен – это многочлен, все коэффициенты которого равны нулю. Если $a_0 \neq 0$, то a_0 называют **старшим коэффициентом**, а n – **степенью** многочлена $f(x)$, которую обозначим через $\deg f$.

Если $f(x) = a \in A$, $a \neq 0$, то $\deg f(x) = 0$. Нулевому многочлену $f(x) = 0$ присваивают степень $-\infty$ и считают, что $-\infty < n$ для каждого $n = 0,1,2,\dots$. Из свойств умножения в кольце $A[x]$ на нулевой элемент вытекают соотношения $-\infty + (-\infty) = -\infty$; $-\infty + n = -\infty$. Коэффициент a_n называют **постоянным** членом. Многочлены степени $1,2,3$ называют соответственно **линейными**, **квадратичными** (или **квадратными**), **кубичными**. Очевидно, что степень суммы двух многочленов не превышает максимум степеней слагаемых, а степень произведения двух многочленов не превышает сумму степеней сомножителей, т.е.

$$\deg(f+g) \leq \max\{\deg f, \deg g\}; \deg fg \leq \deg f + \deg g.$$

Теорема 8.1 Если A – целостное кольцо, то и кольцо многочленов $A[x]$ над A является целостным. В этом случае степень произведения многочленов равна сумме степеней сомножителей.

△ Пусть A – целостное кольцо, и пусть

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

$$g = b_0 x^m + b_1 x^{m-1} + \dots + b_m$$

два ненулевых многочлена степеней n и m соответственно. Тогда $a_0 \neq 0 \neq b_0$ и $fg = a_0 b_0 x^{n+m} + \dots + (a_{n-1}b_m + a_n b_{m-1})x + a_n b_m$. Так как в A нет делителей нуля, то $a_0 b_0 \neq 0$ и fg – ненулевой многочлен степени $n+m$. Поскольку f и g – произвольные ненулевые многочлены из $A[x]$, то в $A[x]$ нет делителей нуля и $A[x]$ – целостное кольцо.

Следствие. Если A – поле, то кольцо многочленов $A[x]$ является целостным и степень произведения многочленов равна сумме степеней сомножителей.

§ 9. ДЕЛИМОСТЬ МНОГОЧЛЕНОВ

Пусть P – произвольное поле. Тогда $P[x]$ – целостное кольцо многочленов. По аналогии с кольцом $\mathbb{Z}$ целых чисел в кольце $P[x]$ многочленов можно рассмотреть вопросы делимости.

Говорят, что многочлен $g \in P[x]$ *делит* многочлен $f \in P[x]$, если существует такой многочлен $\varphi \in P[x]$, что $f = g\varphi$. В этом случае говорят также, что f *делится на* g. Многочлен g называют *делителем* многочлена f, а φ – *частным*. Запись $f \vdots g$ означает, что f делится на g, а запись $g \mid f$ – многочлен g *делит* f.

Лемма 9.1. Для многочленов над полем P справедливы следующие свойства:

1) $f \vdots f$;
2) если $f \vdots g$, $g \vdots h$, то $f \vdots h$;
3) если $f_1 \vdots g$, $f_2 \vdots g$, то $f_1\varphi_1 \pm f_2\varphi_2 \vdots g$ для любых φ_1 и $\varphi_2 \in P[x]$;
4) $f \vdots a$, для всех $a \in P^*$;
5) если $f \vdots g$, то $f \vdots ag$ для всех $a \in P^*$;
6) если $f \vdots g$, а $g \vdots f$, то $f = ag$, где $a \in P^*$;
7) всякий делитель f является делителем af, $a \in P^*$ и наоборот.

△ 1) Так как $f = 1 \cdot f$, то $f \vdots f$.

2) Если $f \vdots g$ и $g \vdots h$, то $f = g\varphi$ и $g = h\psi$. Поэтому $f = g\varphi = (h\psi)\varphi = h(\psi\varphi)$, т.е. $f \vdots h$.

3) Если $f_1 \vdots g$ и $f_2 \vdots g$, то $f_1 = g\psi_1$, $f_2 = g\psi_2$. Поэтому $f_1\varphi_1 \pm f_2\varphi_2 = g\psi_1\varphi_1 \pm g\psi_2\varphi_2 = g(\psi_1\varphi_1 \pm \psi_2\varphi_2)$ и $f_1\varphi_1 \pm f_2\varphi_2 \vdots g$.

4) Так как в поле P каждый ненулевой элемент обладает обратным, то $f = a(a^{-1}f)$ и $f \vdots a$, для всех $a \in P^*$.

5) Если $f \vdots g$, то $f = g\varphi$. Для любого $a \in P^*$ существует $a^{-1} \in P^*$ и $f = ag(a^{-1}\varphi)$, т.е. $f \vdots ag$.

6) Если f и g делятся друг на друга, то $f = g\varphi$, а $g = f\psi$. Теперь $f = f(\psi\varphi)$. По теореме 8.1

$\deg f = \deg f + \deg\psi\varphi$, т.е. $\deg\psi\varphi = 0$ и $\psi\varphi \in P$. Так как f и g – ненулевые многочлены, то $\varphi, \psi \in P^*$ и $\psi = a \in P^*$. Поэтому $f = ag$.

7) Если $f \vdots g$, $f = g\varphi$ и $af = g(a\varphi)$, т.е. af делится на g. Если $af \vdots g$, то $af = g\psi$ и $f = a^{-1}(af) = a^{-1}g\psi = g(a^{-1}\psi)$, т.е. f делится на g.

ДЕЛЕНИЕ С ОСТАТКОМ. Для многочленов, как и для целых чисел, справедлива теорема о делении с остатком.

Теорема 9.2. Пусть P – поле и g – ненулевой многочлен кольца $P[x]$. Тогда каждому многочлену $f \in P[x]$ соответствует единственная пара многочленов q и $r \in P[x]$, для которых $f = gq + r$ и $\deg r < \deg g$.

△ Пусть $g = b_0x^m + b_1x^{m-1} + \dots + b_m$ – ненулевой многочлен, а $f = a_0x^n + a_1x^{n-1} + \dots + a_n$ – произвольный многочлен кольца $P[x]$.

Если $m > n$, то считаем, что $q = 0$, $r = f$. Поэтому $f = g \cdot 0 + f$ и $n = \deg f < \deg g = m$.

Если $m = 0$, то $g = b_0 \neq 0$ и, полагая, $r = 0$, $q = b_0^{-1}f$ имеем $gq + r = b_0b_0^{-1}f + 0 = f$, причем $-\infty = \deg r < \deg g = 0$.

Пусть теперь $n \geq m > 0$. Воспользуемся индукцией по n. Сначала умножим многочлен g на $a_0b_0^{-1}x^{n-m}$ и вычтем из f. Получим

$$f - a_0b_0^{-1}x^{n-m}g = a_0x^n + a_1x^{n-1} + \dots + a_n - a_0x^n - a_0b_0^{-1}b_1x^{n-1} - \dots - a_0b_0^{-1}b_mx^{n-m} = \overline{f}$$

Многочлен $\overline{f}$ имеет степень $< n$. По индуктивному предположению существуют многочлены $\overline{q}$ и $\overline{r}$ такие, что $\overline{f} = g\overline{q} + \overline{r}$ и $\deg\overline{r} < \deg g$. Поэтому $f = a_0b_0^{-1}x^{n-m}g + \overline{f} = a_0b_0^{-1}x^{n-m}g + g\overline{q} + \overline{r} = g(a_0b_0^{-1}x^{n-m} + \overline{q}) + \overline{r} = gq + r$,
где $q = a_0b_0^{-1}x^{n-m} + \overline{q}$, $\overline{r} = r$ и $\deg r < \deg g$.

Итак, существование многочленов q и r доказано.

Проверим их единственность. Допустим, что $f=gq+r=gq'+r'$, $\deg r \le \deg r' < \deg g = m$. Тогда $g(q-q')=r'-r$. Если $q=q'$, то $r=r'$, и теорема доказана. Допустим, что $q \neq q'$. Тогда $\deg(r'-r)=\deg g+\deg(q-q') \ge m$. Но r' и r – многочлены степени $< m$, поэтому и $r'-r$ – многочлен степени $< m$. Противоречие. Следовательно, допущение $q \neq q'$ неверно и теорема доказана полностью. ▲

Итак, для любой пары многочленов f и g, $g \neq 0$ существует единственная пара многочленов q и r такая, что $f=gq+r$ и $\deg r < \deg g$. Многочлен q называют **неполным частным**, а r – **остатком** при делении f на g. В частности, f делится на g тогда и только тогда, когда остаток от деления f на g равен 0.

Пример 1. Разделить многочлен x^3-x^2+x+1 на x^2-1.

△ Как и в доказательстве теоремы 9.2, нам надо на первом этапе домножить делитель x^2+1 на $a_1 b_0^{-1} x^{n-m} = x$ и вычесть из делимого $x^3-x^2+x+1-x(x^2-1)=-x^2+2x+1$. Теперь надо повторить этот прием и уничтожить старший член $(-x^2)$. Деление удобно записывать уголком

$$\begin{array}{r|l} x^3-x^2+x+1 & x^2-1 \\ \underline{x^3\quad -x} & \\ -x^2+2x+1 & \\ \underline{-x^2\quad +1} & \\ 2x & \end{array}$$

Ответ: $x^3-x^2+x+1=(x^2-1)(x-1)+2x$.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. Если многочлен d делит многочлены f и g, то d называется **общим делителем** f и g. Если, кроме того, d делится на любой другой общий делитель многочленов f и g, то d называется **наибольшим общим делителем** и обозначается через $НОД(f,g)$. Другими словами, $d=НОД(f,g)$, если выполняются два требования:

1) $d \mid f$, $d \mid g$;

2) если $d_1 \mid f$ и $d_1 \mid g$, то $d_1 \mid d$.

Отметим, что НОД определяется неоднозначно. Если $d=НОД(f,g)$, то требованиям 1) и 2) удовлетворяют и все многочлены ad, где a – ненулевой элемент поля.

Лемма 9.3. Если d и d' – НОД многочленов f и g, то $d=ad'$, где a – ненулевой элемент поля.

△ Так как $d=НОД(f,g)$, а d' – общий делитель f и g, то $d' \mid d$ по требованию 2). Так как $d'=НОД(f,g)$, а d – общий делитель f и g, то $d \mid d'$. Из леммы 9.1 получаем, что $d=ad'$, где a – ненулевой элемент поля. ▲

Итак, несмотря на то, что НОД определяется неоднозначно, все наибольшие общие делители двух многочленов f и g отличаются друг от друга на ненулевой элемент поля. Среди всех НОД многочленов f и g выделим тот, у которого старший коэффициент равен 1, и обозначим его через $НОД^1(f,g)$. Ясно, что $НОД^1(f,g)$ определен однозначно.

АЛГОРИТМ ЕВКЛИДА. Алгоритм Евклида основан на многократном применении теоремы о делении с остатком. Пусть f и g – два многочлена над полем P. Если $g \mid f$, то $НОД(f,g)=g$. Пусть g не делит f. Тогда мы можем написать цепочку равенств

$$\begin{array}{ll} f=gq_1+r_1, & \deg r_1 < \deg g; \\ g=r_1q_2+r_2, & \deg r_2 < \deg r_1; \\ r_1=r_2q_3+r_3, & \deg r_3 < \deg r_2; \\ \quad\cdots & \\ r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}, & \deg r_{n-1} < \deg r_{n-2}; \\ r_{n-2}=r_{n-1}q_n+r_n, & \deg r_n < \deg r_{n-1}; \\ r_{n-1}=r_nq_{n+1} & \end{array} \qquad (1)$$

Каждое из равенств (1) есть по теореме о делении с остатком. Поскольку степени остатков строго убывают

$$\deg g > \deg r_1 > \deg r_2 > \ldots > \deg r_{n-1} > \deg r_n,$$

то через конечное число шагов должен появиться остаток равный нулю, т.е. на каком-то этапе деление произойдет без остатков. В (I) деление без остатка записано в последней строке.

Алгоритм Евклида для многочленов f и g заключается в нахождении равенств (I).

Т е о р е м а 9.4. НОД любых двух ненулевых многочленов всегда существует. Если $g \mid f$, то $НОД(f,g) = g$. Если g не делит f, то $НОД(f,g)$ равен последнему отличному от нуля остатку в алгоритме Евклида.

△ Двигаясь снизу вверх в алгоритме Евклида, получаем, что r_n – общий делитель многочленов f и g. Действительно, из последнего равенства следует, что $r_n \mid r_{n-1}$. Из предпоследнего – $r_n \mid r_{n-2}$, здесь используется лемма 9.1. Из третьего снизу равенства следует, что $r_n \mid r_{n-3}$, и т.д. Если мы уже доказали, что $r_n \mid r_2$ и r_3, то из третьего сверху равенства на основании леммы 9.1 заключаем, что $r_n \mid r_1$. Из второго, а затем и первого равенств получаем, что $r_n \mid g$ и $r_n \mid f$.

Пусть теперь d – произвольный общий делитель многочленов f и g. Тогда двигаясь в алгоритме Евклида сверху вниз и применяя каждый раз лемму 9.1 получим, что d делит r_n. ▲

Отметим, что $НОД(f,0) = f$, где f – ненулевой многочлен, а $НОД(0,0)$ не существует.

П р и м е р 2. **Найти** $НОД^1(x^3-1, x^2+1)$.

△ Построим алгоритм Евклида для этих многочленов

$$\begin{array}{r|l} x^3-1 & x^2+1 \\ \hline -x^3+x & x \\ \hline -x^2+1 & -x-1 \\ \hline -x^2+x & -x+1 \\ \hline -x+1 & \\ \hline -x-1 & \\ \hline -x-1 & 2 \\ \hline -x & -\frac{1}{2}x-\frac{1}{2} \\ \hline -1 & \\ \hline -1 & \\ \hline 0 & \end{array}$$

$$\begin{aligned} x^3-1 &= (x^2+1)x + (-x-1) \\ x^2+1 &= (-x-1)(-x+1) + 2 \\ -x-1 &= 2\left(-\tfrac{1}{2}x-\tfrac{1}{2}\right) \end{aligned} \qquad (2)$$

Итак, $НОД(x^3-1, x^2+1) = 2$. Ясно, что $НОД^1(x^3-1, x^2+1) = 1$.

О т в е т: $НОД^1(x^3-1, x^2+1) = 1$.

Т е о р е м а 9.5. Если $d = НОД(f,g)$, то существуют такие многочлены φ и ψ, что $d = \varphi f + \psi g$.

Д о к а з а т е л ь с т в о проведем индукцией по числу строк в алгоритме Евклида.

Если для многочленов f и g в алгоритме Евклида одна строка, то $f = gq_1$ и $НОД(f,g) = g = 0 \cdot f + 1 \cdot g$.

Допустим, что теорема верна для всех пар многочленов, у которых в алгоритме Евклида n строк. Пусть у многочленов f и g в алгоритме Евклида (I) $n+1$ строка. Уберем из (I) первую строку. Оставшиеся n строк дадут алгоритм Евклида для многочленов g и r_1. По индукции существуют многочлены $\overline{\varphi}$ и $\overline{\psi}$ такие, что $r_n = \overline{\varphi} g + \overline{\psi} r_1$. Поставим сюда выражение $r_1 = f - gq_1$ из первого равенства (I). Получим:

$$r_n = \overline{\varphi} g + \overline{\psi} r_1 = \overline{\varphi} g + \overline{\psi}(f - gq_1) = \overline{\psi} f +$$
$$+ (\overline{\varphi} - \overline{\psi} q_1) g = \varphi f + \psi g, \text{ где } \varphi = \overline{\psi}, \psi = \overline{\varphi} - \overline{\psi} q_1.$$

В з а и м н о п р о с т ы е м н о г о ч л е н ы – это многочлены, у которых $НОД^1$ равен I.

С л е д с т в и е. Многочлены f и g взаимно просты тогда и только тогда, когда существуют такие многочлены φ и ψ, что $1 = \varphi f + \psi g$.

△ Если f и g – взаимно просты, то $1 = \varphi f + \psi g$ по теореме.

Обратно, Пусть $1 = \varphi f + \psi g$ и $d = НОД^1(f,g)$. Тогда $d \mid \varphi f + \psi g$ по лемме 9.1 и $d = 1$.

П р и м е р 3. Выразить $НОД^1(x^3-1, x^2+1)$ через исходные многочлены.

Δ Для многочленов x^3-1 и x^2+1 алгоритм Евклида состоит из трех равенств, см. (2). Из второго и первого равенств получаем:

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

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

$$+x(-x+1)).$$

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

Теорема 9.6. Если произведение многочленов fg делится на многочлен h, причем f и h взаимно просты, то g делится на h.

Δ Так как f и h взаимно просты, то по следствию теоремы 9.5 существуют такие многочлены φ и ψ, что $1 = \varphi f + \psi h$. Умножим обе части на g: $g = gqf + gqh$. По условию $fg \vdots h$, второе слагаемое gqh также делится на h, поэтому и $g \vdots h$.

§ 10. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ

Пусть f – произвольный многочлен над полем P степени ≥ 1. Тогда f делится на a и af, где a – ненулевой элемент поля P. Если f других делителей не имеет, то f называется неприводимым многочленом. Другими словами, многочлен f степени ≥ 1 называется неприводимым, если его нельзя представить в виде двух других многочленов $f = g_1 g_2$ меньших степеней: $1 \leq \deg g_1, \deg g_2 < \deg f$.

Многочлен, который не является неприводимым, называется приводимым. Приводимый многочлен представим в виде произведения двух многочленов меньших степеней.

Приводимость многочленов зависит от поля.

Пример 1. $x^2+1 = (x-i)(x+i)$ неприводим над $\mathbb{Q}$

и $\mathbb{R}$, но приводим над $\mathbb{C}$.

$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ неприводим над $\mathbb{Q}$, но приводим над $\mathbb{R}$.

Лемма 10.1. Многочлены над полем P обладают следующими свойствами:

1) многочлены первой степени неприводимы;

2) если f неприводим, то af неприводим для всех $a \in P^*$;

3) если f неприводим, то для любого многочлена g либо f делит g, либо f и g взаимно просты;

4) если произведение fg делится на неприводимый многочлен h, то либо f делится на h, либо g делится на h.

Δ Первые два свойства вытекают из определения.

3) Пусть $d = НОД(f,g)$. Так как f неприводим, то $d = af$, либо $d = a$, где $a \in P^*$. В первом случае $f \mid g$, во втором f и g взаимно просты.

4) Пусть $fg \vdots h$. Если f не делится на h, то f и h взаимно просты по свойству 3). Теперь из теоремы 9.6 следует, что g делится на h.

Теорема 10.2. Всякий многочлен f над полем P степени $n \geq 1$ можно представить в виде произведения неприводимых над P многочленов. Если имеются два таких разложения $f = \varphi_1 \varphi_2 \dots \varphi_s = \psi_1 \psi_2 \dots \psi_t$, то $s = t$ и при подходящей нумерации $\psi_i = a_i \varphi_i$, $i = 1, 2, \dots, s$.

Доказательство проводим индукцией по степени n многочлена f. При $n = 1$ многочлен f неприводим и утверждение выполняется.

Пусть утверждение верно для всех многочленов степени $< n$, и пусть f – многочлен степени n. Если f неприводим, то требуемое разложение имеется с числом сомножителей равным единице.

Если f приводим, то $f = f_1 f_2$, где f_1 и f_2 – многочлены степеней меньше, чем n. По индукции эти многочлены разложимы в произведение неприводимых: $f_1 = \varphi_1 \varphi_2 \dots \varphi_k$, $f_2 = \varphi_{k+1} \varphi_{k+2} \dots \varphi_s$. Теперь $f = \varphi_1 \varphi_2 \dots \varphi_s$, и разложение доказано.

Проверим единственность. Пусть $f = \varphi_1 \dots \varphi_s = \psi_1 \dots \psi_t$ –

два разложения многочлена f в произведение неприводимых. Так как ψ_1 делит $\varphi_1\varphi_2\dots\varphi_s$, то по лемме 10.1 один из сомножителей φ_i делится на ψ_1. Без ограничения общности считаем, что φ_1 делится на ψ_1. Так как φ_1 неприводим, то $\varphi_1 = a\psi_1$. Поделив обе части равенства $\varphi_1\varphi_2\dots\varphi_s = \psi_1\psi_2\dots\psi_t$ на ψ_1, получим $a\varphi_2\dots\varphi_s = \psi_2\dots\psi_t$. Но $a\varphi_2\dots\varphi_s$ – многочлен степени $< n$, для него однозначность разложения на неприводимые множители выполняется по индукции. Значит, $s-1 = t-1$ и $\varphi_i = a_i\psi_i$, $i = 2,3,\dots,s$. Но теперь $s = t$ и $\varphi_i = a_i\psi_i$, $i = 1,2,\dots,s$. ▲

Многочлен, старший коэффициент которого равен 1, называется **унитарным**.

Теорема 10.3. Над любым полем унитарных неприводимых многочленов бесконечно много.

Δ Допустим, что над некоторым полем P унитарных неприводимых многочленов конечное число. Пусть $p_1, p_2, \dots, p_t$ – все неприводимые унитарные многочлены. Рассмотрим многочлен $f = 1 + p_1p_2\dots p_t$. По теореме 10.2 многочлен f делится на некоторый неприводимый многочлен, пусть f делится на p_i. Теперь p_i делит $f - p_1p_2\dots p_t = 1$, что невозможно. Поэтому допущение неверно, и унитарных неприводимых многочленов бесконечно много.

Следствие. Над любым конечным полем существуют неприводимые многочлены сколь угодно высокой степени.

Δ Пусть P – конечное поле. Для любого n существует лишь конечное число многочленов степени не выше n с коэффициентами из P. Но неприводимых многочленов над P бесконечно много по теореме 10.3. Поэтому над конечным полем P будут существовать неприводимые многочлены степени $> n$. ▲

Пусть P – неприводимый делитель многочлена $f \in P[x]$. Если p^k делит f, но p^{k+1} не делит f, то p назовем **k-кратным неприводимым множителем**. Если $k = 1$, то p называется **простым** неприводимым множителем.

По теореме 10.2 каждый многочлен представим в виде неприводимых многочленов $f = \varphi_1\varphi_2\dots\varphi_s$. Если вынести за скобки старшие коэффициенты всех неприводимых множителей, а затем собрать совпадающие множители вместе, то мы придем к **каноническому разложению** многочлена

$$f = a\,p_1^{k_1}p_2^{k_2}\dots p_n^{k_n}.$$

В этом разложении все p_i – унитарные неприводимые попарно взаимно простые многочлены.

Теорема 10.4. Если $f = ap_1^{k_1}\dots p_s^{k_s}$, $g = bp_1^{\ell_1}\dots p_s^{\ell_s}$ – канонические разложения двух многочленов, то $НОД(f,g) = p_1^{m_1}\dots p_s^{m_s}$, где $m_i = \min\{k_i, \ell_i\}$.

Δ Пусть $d = p_1^{m_1}\dots p_s^{m_s}$, где $m_i = \min\{k_i, \ell_i\}$. Ясно, что d – унитарный многочлен. Так как $m_i = \min\{k_i, \ell_i\}$, то $d \mid f$ и g, т.е. d – общий делитель f и g. Пусть d' – произвольный общий делитель f и g. Так как d' делит f и g, то $d' = a'p_1^{t_1}\dots p_s^{t_s}$, где $t_i \le k_i$ и $t_i \le \ell_i$. Отсюда следует, что $t_i \le \min\{k_i, \ell_i\}$ и $d' \mid d$.

Пример 2. Пусть $f = x(x+1)^3(x-1)^2(x^2+1)$, $g = (x+1)^2(x-1)^4(x-5)(x^2+1) \in \mathbb{R}[x]$. Тогда $НОД(f,g) = (x+1)^2(x-1)^2(x^2+1)$.

ПРОИЗВОДНАЯ МНОГОЧЛЕНА. Пусть P – поле нулевой характеристики. Это означает, что $na = \underbrace{a + a + \dots + a}_{n\text{ раз}} \neq 0$ для всех $n \in \mathbb{N}$ и $a \in P^*$.

Для многочлена $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ над полем P определим его производную

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}.$$

Так как P – поле нулевой характеристики, то $na_0 \neq 0$ и f' – многочлен степени $n-1$.

Лемма 10.5. Пусть P – поле нулевой характеристики, f и $g \in P[x]$. Тогда

1) $(cf)' = cf'$, где $c \in P$;
2) $(f+g)' = f' + g'$;

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

4) $(f^k)' = k f^{(k-1)} f'$, где $k \in \mathbb{N}$.

I) Пусть $f = a_0 x^n + \ldots + a_n \in P[x]$. Тогда

$(cf)' = (ca_0 x^n + \ldots + ca_n)' = nca_0 x^{n-1} + \ldots$

$+ ca_{n-1} = c(na_0 x^{n-1} + \ldots + a_{n-1}) = cf'$.

2) Запишем многочлены f и g по возрастающим степеням x:

$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$,

$g = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$.

Пусть $n \geq m$. Тогда многочлен g можно записать в виде

$$g = b_0 + b_1 x + \ldots + b_n x^n,$$

где $b_i = 0$, для $i = m+1, \ldots, n$.

Теперь $(f+g)' = ((a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + \ldots$

$\ldots + (a_n+b_n)x^n)' = a_1 + b_1 + 2(a_2+b_2)x + \ldots$

$\ldots + n(a_n+b_n)x^{n-1} = a_1 + 2a_2 x + \ldots + na_n x^{n-1} + b_1 +$

$+ b_2 x + \ldots + b_n \cdot n x^{n-1} = f' + g'$.

3) Рассмотрим вначале одночлены ax^n и bx^m , где a и $b \in P$. Для них имеем: $(ax^n \cdot bx^m)' =$

$= (abx^{n+m})' = (n+m)abx^{n+m-1} = nabx^{n+m-1} +$

$+ mabx^{n+m-1} = nax^{n-1} bx^m + ax^n mbx^{m-1} =$

$= (ax^n)' bx^m + ax^n (bx^m)'$.

Итак, для одночленов утверждение доказано.

Пусть f и g произвольные многочлены. Многочлен fg равен сумме всевозможных произведений uv , где u – член многочлена f , а v – член многочлена g . Запишем это так $fg = \sum uv$. Согласно свойству 2 имеем $(fg)' = \sum (uv)'$. С другой стороны, $f'g = \sum u'v$, а $fg' = \sum uv'$. Так как для одночленов утверждение доказано, то $(uv)' = u'v + uv'$ и $(fg)' = \sum (uv)' =$

$= \sum (u'v + uv') = \sum u'v + \sum uv' = f'g + fg'$.

4) Воспользуемся индукцией по k . Считаем, что для $k-1$ утверждение уже получено: $(f^{(k-1)})' = (k-1) f^{(k-2)} f'$.

Теперь $(f^k)' = (f^{(k-1)} f)' = (f^{(k-1)})' f + f^{(k-1)} f' =$

$= (k-1) f^{(k-2)} f' f + f^{(k-1)} f' = k f^{(k-1)} f'$.

Т е о р е м а 10.6. Если p – k-кратный неприводимый множитель многочлена f над полем нулевой характеристики, то он является $(k-1)$-кратным множителем производной f' . В частности, если p – простой множитель многочлена f , то p взаимно прост с производной f' .

△ Пусть $f = p^k q$, где p и q – взаимно простые многочлены. Тогда $f' = (p^k)' q + p^k q' = k p^{k-1} p' q +$

$+ p^k q' = p^{(k-1)} (k p' q + p q')$. Допустим, что $kp'q + pq'$ делится на p . Тогда p' делится на p и имеем противоречие с тем, что $\deg p' < \deg p$. Значит, допущение неверно и q не делится на p . Поэтому f' не делится на p^k .

С л е д с т в и е . Если $f = a p_1^{k_1} \ldots p_s^{k_s}$ – каноническое разложение многочлена f над полем нулевой характеристики, то $НОД(f, f') = p_1^{k_1 - 1} \ldots p_s^{k_s - 1}$. В частности, f не содержит кратных множителей тогда и только тогда, когда f взаимно прост со своей производной.

△ По теореме 10.6 каноническое разложение производной будет иметь вид

$$f' = b p_1^{k_1 - 1} \ldots p_s^{k_s - 1} p_{s+1}^{k_{s+1}} \ldots p_t^{k_t}.$$

Здесь $p_{s+1}, \ldots, p_t$ – унитарные неприводимые многочлены, которые в разложении f входят с нулевым показателем. По теореме 10.4 $НОД(f, f') = p_1^{k_1 - 1} \ldots p_s^{k_s - 1}$.

Если f не содержит кратных множителей, то $k_1 = k_2 = \ldots = k_s = 1$ и $НОД(f, f') = 1$, т.е. многочлен взаимно прост со своей производной.

Обратно. Пусть многочлен f взаимно прост со своей производной. Допустим, что f содержит k-кратный множи-

тель p, где $k \geq 2$. Тогда p будет $(k-1)$-кратным множителем производной f', и p – общий делитель f и f', противоречие.

Пример 3. Определить кратные неприводимые множители многочлена $f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1 \in \mathbb{R}[x]$.

△ Находим производную $f' = 8x^7 - 6x^5 - 10x^4 + 6x^2 + 2x = 2x(4x^6 - 3x^4 - 5x^3 + 3x + 1)$.

Так как f не делится на x, то $НОД(f, f') = НОД(f, 4x^6 - 3x^4 - 5x^3 + 3x + 1)$. С помощью алгоритма Евклида находим, что $НОД(f, f') = x^4 - x^3 - x + 1 = (x^3 - 1)(x - 1) = (x-1)^2(x^2 + x + 1)$. По теореме 10.6 кратными неприводимыми множителями многочлена f являются: $x - 1$ кратности 3 и $x^2 + x + 1$ кратности 2. Разделив f на $(x-1)^3(x^2+x+1)^2$, получим полное разложение f на неприводимые множители:

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

§ 11. КОРНИ МНОГОЧЛЕНА

Пусть P – поле и $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ многочлен над полем P. Для элемента $c \in P$ сумму $a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c + a_n$ будем обозначать через $f(c)$ и называть **значением** многочлена для аргумента c. Если $f(c) = 0$, то элемент c называют **корнем** многочлена $f(x)$.

Теорема 11.1 (теорема Безу). Элемент $c \in P$ является корнем многочлена $f(x) \in P[x]$ тогда и только тогда, когда $x - c$ делит $f(x)$.

△ Пусть c – произвольный элемент поля P. Разделим многочлен $f(x)$ на $x - c$:

$$f(x) = (x-c)q(x) + r(x), \quad \deg r(x) < \deg(x-c) = 1$$

Итак, $r(x) = r \in P$. Подставив $x = c$ получаем $f(c) = r$. Итак,

$$f(x) = (x-c)q(x) + r \tag{1}$$

Мы доказали, что при делении многочлена $f(x)$ на $x - c$ остаток равен значению многочлена $f(c)$.

Если c – корень многочлена $f(x)$, то $f(c) = 0$ и $x - c$ делит $f(x)$.

Если $x - c$ делит $f(x)$, то остаток $f(c)$ равен 0 и c – корень многочлена $f(x)$.

СХЕМА ГОРНЕРА. Пусть нам надо разделить многочлен $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ на $x - c$. Найдем коэффициенты неполного частного $q(x)$. Многочлен $q(x)$ имеет степень $n-1$ и его можно записать так:

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

По (1) получаем $f(x) = (x-c)q(x) + f(c) = xq(x) - cq(x) + f(c) = b_0x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_{n-2}x^2 + b_{n-1}x - (b_0cx^{n-1} + b_1cx^{n-2} + \ldots + b_{n-3}cx^2 + b_{n-2}cx + b_{n-1}c) + f(c)$.

Приравнивая коэффициенты при одинаковых показателях степеней:

$$\begin{aligned}
a_0 &= b_0 & b_0 &= a_0\\
a_1 &= b_1 - b_0c & b_1 &= a_1 + b_0c\\
a_2 &= b_2 - b_1c & b_2 &= a_2 + b_1c\\
&\ldots & &\ldots\\
a_{n-2} &= b_{n-2} - b_{n-3}c & b_{n-2} &= a_{n-2} + b_{n-3}c\\
a_{n-1} &= b_{n-1} - b_{n-2}c & b_{n-1} &= a_{n-1} + b_{n-2}c\\
a_n &= f(c) - b_{n-1}c & f(c) &= a_n + b_{n-1}c
\end{aligned} \tag{2}$$

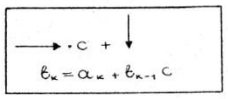
Равенства (2) удобнее записать в виде следующей таблицы.

(3)

	a_0	a_1	...	a_k	...	a_{n-1}	a_n
c	$b_c = a_0$	$b_1 = a_1 + b_0 c$	...	$b_k = a_k + b_{k-1} c$	...	$b_{n-1} = a_{n-1} + b_{n-2} c$	$f(c) = a_n + b_{n-1} c$

Для ее составления надо в первую строку выписать коэффициенты делимого $f(x)$, в первой клетке второй строки записывается элемент c, а во второй клетке $b_c = a_0$. Остальные клетки второй строки заполняются по принципу

(4)



В последней клетке второй строки получается остаток $f(c)$, в остальных клетках – коэффициенты частного.

Пример 1. В кольце $\mathbb{C}[x]$ разделить многочлен
$f(x) = 2x^5 + (1+2i)x^4 + (2+i)x^2 + (1+4i)x + i$
на многочлен $g(x) = x + i$.

Δ Применим схему Горнера

	2	$1+2i$	0	$2+i$	$1+4i$	i
$-i$	2	1	$-i$	$1+i$	$2+3i$	$3-i$

Так как $g(x) = x + i$, то первый элемент второй строки равен $(-i)$. Во второй клетке стоит коэффициент $b_0 = a_0$, остальные клетки заполняются по схеме (4). Остаток $f(c) = 3 - i$, частное $q_1(x) = 2x^4 + x^3 - ix^2 + (1+i)x + 2 + 3i$.

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

Элемент $c \in P$ называется k-кратным корнем многочлена $f(x) \in P[x]$ или корнем кратности k, если $f(x)$ делится на $(x-c)^k$, но не делится на $(x-c)^{k+1}$. Корень кратности 1 называется простым корнем. При $k=2$ говорят о двойном корне, а при $k=3$ – о тройном.

Лемма II.2. **Элемент c является k-кратным корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = (x-c)^k q(x)$ и $q(c) \neq 0$.**

Δ **Пусть c – k-кратный корень многочлена $f(x)$. Тогда $(x-c)^k$ делит $f(x)$ и $(x-c)^{k+1}$ не делит $f(x)$. Поэтому $f(x) = (x-c)^k q(x)$. Если $q(c) = 0$, то $x-c$ делит $q(x)$ по теореме Безу и $(x-c)^{k+1}$ делит $f(x)$, противоречие. Итак, $q(c) \neq 0$ и необходимость доказана.**

Пусть наоборот $f(x) = (x-c)^k q(x)$ и $q(c) \neq 0$. Тогда $(x-c)^k$ делит $f(x)$. Если $(x-c)^{k+1}$ делит $f(x)$, то $x-c$ делит $q(x)$ и $q(c) \neq 0$, противоречие. Поэтому $(x-c)^{k+1}$ не делит $f(x)$ и c – k-кратный корень многочлена $f(x)$.

Теорема II.3. **Если $c_1, c_2, \ldots, c_r$ – корни кратностей $k_1, k_2, \ldots, k_r$ многочлена $f(x)$, то $f(x) = (x-c_1)^{k_1}(x-c_2)^{k_2}\ldots(x-c_r)^{k_r} q(x)$ и $q(c_i) \neq 0$, $i = 1, 2, \ldots, r$.**

Δ **Для корня c_1 по лемме II.2 получаем, что $f(x) = (x-c_1)^{k_1} q_1(x)$ и $q_1(c_1) \neq 0$. Теперь c_2 – k_2-кратный корень $q_1(x)$, поэтому $q_1(x) = (x-c_2)^{k_2} q_2(x)$, $q_2(c_2) \neq 0$ и**

$f(x)=(x-c_1)^{k_1}(x-c_2)^{k_2}q_2(x)$. Ясно, что $q_2(c_1)\neq 0$. Через r шагов приходим к равенству $f(x)=(x-c_1)^{k_1}\dots(x-c_r)^{k_r}q(x)$ и $q(c_i)\neq 0$ для всех i.

Следствие. Число корней многочлена, рассматриваемых вместе с их кратностями, не превосходит его степени.

△ Пусть $c_1, c_2, \dots, c_r$ – корни многочлена $f(x)$ кратности $k_1, \dots, k_r$, и пусть других корней многочлен $f(x)$ не имеет. Тогда

$$f(x)=(x-c_1)^{k_1}\dots(x-c_r)^{k_r}q(x)$$ и

$q(c)\neq 0$, для всех $c\in P$. Теперь $\deg f = k_1+\dots+k_r+\deg q$, откуда $k_1+\dots+k_r\le \deg f$.

Пример 2. Найти кратность корня $x=2$ многочлена $f(x)=x^5-5x^4+7x^3-2x^2+4x-8\in\mathbb{R}[x]$.

△ Делим $f(x)$ на $x-2$, затем получившееся частное на $x-2$ и т.д., пока не получится ненулевой остаток. Деление удобно производить по схеме Горнера

	1	-5	7	-2	4	8
2	1	-3	1	0	4	0
2	1	-1	-1	-2	0	
2	1	1	1	0		
2	1	3	7	14		

Итак, $f(x)$ делится на $(x-2)^3$, но не делится на $(x-2)^4$.

Ответ: корень $x=2$ кратности 3.

Теорема II.4. Если c – k-кратный корень многочлена $f(x)$ над полем нулевой характеристики, то c – $(k-1)$-кратный корень производной $f'(x)$. В частности, c – простой корень многочлена $f(x)$, если $f(c)=0$ и $f'(c)\neq 0$.

△ Если c – k-кратный корень многочлена $f(x)$, то $x-c$ – k-кратный множитель $f(x)$ по лемме II.2. Так как $x-c$ – неприводимый многочлен, то по теореме I0.6 $x-c$ – $(k-1)$-кратный множитель производной, а по лемме II.2 элемент c – $(k-1)$-кратный корень $f'(x)$.

Пример 3. Определить a и b так, чтобы многочлен $f(x)=ax^4+bx^3+1$ имел $x=1$ двойным корнем.

△ Число I будет корнем многочлена $f(x)$ не ниже 2-й кратности, если значения многочлена $f(x)$ и его производной $f'(x)=4ax^3+3bx^2$ при $x=1$ равны нулю. Приравнивая $f(1)$ и $f'(1)$ к нулю, получим систему уравнений

$$\begin{cases} a+b=-1, \\ 4a+3b=0, \end{cases} \quad b=-4,\ a=3$$

Ответ: $a=3$, $b=-4$.

ФОРМУЛА ВИЕТА. В случае, когда число корней многочлена совпадает со степенью, справедливы формулы Виета.

Пусть $f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\dots+a_{n-2}x^2+a_{n-1}x+a_n$ – многочлен степени n со старшим коэффициентом равным I. Допустим, что этот многочлен имеет n корней: $c_1, c_2, \dots, c_n$. Тогда по теореме II.3 получаем разложение

$$f(x)=(x-c_1)(x-c_2)\dots(x-c_n).$$

Перемножая линейные множители в правой части и приводя подобные члены, мы получаем следующие равенства, называемые формулами Виета:

$$\begin{aligned} a_1 &= -(c_1+c_2+\dots+c_n) \\ a_2 &= c_1c_2+c_1c_3+\dots+c_1c_n+c_2c_3+\dots+ \\ &\quad +c_2c_n+\dots+c_{n-1}c_n=\sum_{(i_1<i_2<n)} c_{i_1}c_{i_2} \\ &\dots \end{aligned} \tag{5}$$

$$a_k = (-1)^k \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} c_{i_1} c_{i_2} \dots c_{i_k}$$

$$\dots$$

$$a_n = (-1)^n c_1 c_2 \dots c_n .$$

Для $n = 2$ и $P = \mathbb{R}$ эти формулы известны из школьного курса математики.

Повторим вывод этих формул для

$$f(x) = x^3 + a_1 x^2 + a_2 x + a_3 = (x - c_1)(x - c_2)(x - c_3) =$$

$$= x^3 + x^2(-c_3 - c_2 - c_1) + x(c_1 c_2 + c_1 c_3 + c_2 c_3) - \quad (6)$$

$$- c_1 c_2 c_3$$

$$a_1 = -(c_1 + c_2 + c_3)$$

$$a_2 = c_1 c_2 + c_1 c_3 + c_2 c_3$$

$$a_3 = -c_1 c_2 c_3 .$$

Пример 4. Найти многочлен над $\mathbb{R}$ третьей степени, имеющий двукратным корнем число 3 и простым корнем число (-2).

△ Многочлен $f(x) = x^3 + a_1 x^2 + a_2 x + a_3$ имеет корни $c_1 = 3$, $c_2 = 3$, $c_3 = -2$. По (6) получаем

$$a_1 = -(3 + 3 - 2) = -4,$$

$$a_2 = 9 - 6 - 6 = -3,$$

$$a_3 = 18.$$

Ответ: $f(x) = x^3 - 4x^2 - 3x + 18$.

Если многочлен $f(x)$ не является унитарным, т.е. его старший коэффициент $a_0 \neq 1$, то полученные формулы (5) давали бы выражения для a_i / a_0, $i = 1, 2, \dots, n$.

§ 12. МНОГОЧЛЕНЫ НАД ЧИСЛОВЫМИ ПОЛЯМИ

В этом параграфе мы рассмотрим многочлены над полем $\mathbb{C}$ комплексных чисел и над полем $\mathbb{R}$ действительных чисел.

МНОГОЧЛЕНЫ НАД $\mathbb{C}$.

Теорема 12.1. Всякий многочлен степени $n \ge 1$ над полем $\mathbb{C}$ имеет хотя бы один корень.

Эта теорема будет доказана в II семестре в курсе "Алгебра и теория чисел".

Следствие. Всякий многочлен степени $n \ge 1$ над полем $\mathbb{C}$ имеет точно n корней.

Доказательство проведем индукцией по степени многочлена. Многочлены первой степени имеют вид: $ax + b$, где a и $b \in \mathbb{C}$, $a \neq 0$. Корнем будет комплексное число $x = -b/a$.

Пусть утверждение верно для всех многочленов степени $n-1$, и пусть $f(x)$ – многочлен степени n. По теореме 12.1 многочлен имеет хотя бы один корень. Пусть $c \in \mathbb{C}$ – корень многочлена $f(x)$. По теореме Безу $f(x) = (x - c) g(x)$. По индукции многочлен $g(x)$ имеет $n-1$ корень. Эти корни вместе с корнем c будет корнями многочлена $f(x)$. Их ровно n штук.

Теорема 12.2. Неприводимыми над полем комплексных чисел являются только многочлены первой степени.

△ Многочлены первой степени неприводимы над любым полем. Пусть $f(x)$ – многочлен степени $n \ge 2$. По теореме 12.1 этот многочлен имеет хотя бы один комплексный корень. Пусть c – корень многочлена $f(x)$. По теореме Безу $f(x) = (x - c) g(x)$, поэтому $f(x)$ приводим. Значит, каждый многочлен степени $n \ge 2$ приводим над $\mathbb{C}$. ▲

Итак, над полем комплексных чисел каждый многочлен разложим в произведение многочленов первой степени. Если $f(x) \in \mathbb{C}[x]$ и $\deg f(x) = n$, то

$$f(x) = a_0 (x - c_1)(x - c_2) \dots (x - c_n),$$

где $a_0 \neq 0$, $c_1, c_2, \ldots, c_n \in \mathbb{C}$.

Пример 1. Разложить над полем $\mathbb{C}$ на неприводимые множители многочлен $f(x) = x^4 + x^3 - x - 1$.

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

Решим уравнение $x^2 + x + 1 = 0$

$$x_{1,2} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} - 1} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}.$$

Ответ: $x^4 + x^3 - x - 1 = (x+1)(x-1)\left(x + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$.

Произвольное поле P называется **алгебраически замкнутым** полем, если каждый многочлен степени $\geqslant 1$ над полем P имеет хотя бы один корень. В этом случае каждый многочлен над алгебраически замкнутым полем будет иметь ровно столько корней, какова его степень. Теперь теорему 12.1 можно сформулировать так

Теорема 12.1. Поле комплексных чисел алгебраически замкнуто.

Эту теорему доказал в 1799 году немецкий математик Карл Фридрих ГАУСС.

МНОГОЧЛЕНЫ НАД $\mathbb{R}$. Поле $\mathbb{R}$ действительных чисел не является алгебраически замкнутым. Многочлен $x^2 + 1$ не имеет действительных корней. Однако $\mathbb{R}$ содержится в поле $\mathbb{C}$ комплексных чисел. Поэтому всякий многочлен с действительными коэффициентами имеет столько комплексных корней, какова его степень.

Теорема 12.3. Если $z = a + bi$ – корень многочлена $f(x) \in \mathbb{R}[x]$, то сопряженное число $\overline{z} = a - bi$ – также корень $f(x)$.

Δ Напомним, что сопряженные числа обладают следующими свойствами:

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

$$\overline{z^k} = (\overline{z})^k, \ \overline{a} = a \quad \text{для} \quad a \in \mathbb{R}, z_1, z_2, z \in \mathbb{C}.$$

Пусть $z = a + bi$ – корень многочлена $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in \mathbb{R}[x]$.
Тогда $f(z) = 0$. Поэтому

$$f(\overline{z}) = a_0 \overline{z}^n + a_1 \overline{z}^{n-1} + \ldots + a_{n-1} \overline{z} + a_n =$$

$$= \overline{a}_0 \overline{z^n} + \overline{a}_1 \overline{z^{n-1}} + \ldots + \overline{a}_{n-1} \overline{z} + \overline{a}_n =$$

$$= \overline{f(z)} = \overline{0} = 0,$$

т.е. $\overline{z} = a - bi$ – также корень многочлена $f(x)$.

Доказанная теорема утверждает, что у многочлена с действительными коэффициентами комплексные корни попарно сопряжены между собой. Поэтому число комплексных недействительных корней будет четным.

Следствие. Многочлен над полем $\mathbb{R}$ нечетной степени имеет действительный корень.

Теорема 12.4. Неприводимыми над полем действительных чисел являются многочлены первой степени и многочлены второй степени с отрицательным дискриминантом.

Δ Пусть $f(x) \in \mathbb{R}[x]$ – неприводимый многочлен степени > 2 . По теореме Безу он не имеет действительных корней. Пусть $z = a + bi$ – комплексный недействительный корень многочлена $f(x)$. Он существует по теореме 12.1. По теореме 12.3 сопряженное число $\overline{z} = a - bi$ также будет корнем $f(x)$. Поэтому многочлен $f(x)$ делится на

$$(x - (a + bi))(x - (a - bi)) = (x - a - bi)(x - a + bi) =$$

$$= (x - a)^2 - (bi)^2 = x^2 - 2ax + a^2 + b^2.$$

Этот многочлен имеет действительные коэффициенты и его дискриминант $D = 4a^2 - 4(a^2+b^2) = -4b^2 < 0$. Поэтому многочлен $x^2 - 2ax + a^2 + b^2$ неприводим над полем $\mathbb{R}$. Теперь $f(x) = (x^2 - 2ax + a^2 + b^2)\,g(x)$, а так как $f(x)$ – неприводимый многочлен, то $g(x) = a_0 \in \mathbb{R}$ и $f(x) = a_0(x^2 - 2ax + a^2 + b^2)$ – неприводимый многочлен с отрицательным дискриминантом.

Теорема 12.5. Каждый многочлен степени $n \geq 1$ с действительными коэффициентами разлагается над $\mathbb{R}$ в произведение $m \leq n$ многочленов первой степени, соответствующих действительным корням, и $\frac{n-m}{2}$ неприводимых над $\mathbb{R}$ многочленов второй степени, соответствующих парам комплексных сопряженных корней.

△ Пусть многочлен $f(x)$ имеет m действительных корней $c_1, c_2, \ldots, c_m$. Тогда

$$f(x) = (x-c_1)(x-c_2)\ldots(x-c_m)\,g(x),$$

причем многочлен $g(x)$ степени $n-m$ не имеет ни одного действительного корня. Все корни многочлена $g(x)$ комплексные недействительные, поэтому они попарно сопряжены. Значит, число корней многочлена $g(x)$ четное и равно $n-m$. Каждой паре комплексных сопряженных корней соответствует многочлен второй степени с отрицательным дискриминантом, см. доказательство теоремы 12.4. Всего таких неприводимых многочленов второй степени будет $(n-m)/2$.

Пример 2. Разложить над полем $\mathbb{R}$ на неприводимые множители многочлен $x^4 + x^3 - 8x - 8$.

△ $x^4 + x^3 - 8x - 8 = x^3(x+1) - 8(x+1) =$

$= (x+1)(x^3 - 8) = (x+1)(x-2)(x^2 + 2x + 4)$.

Многочлен $x^2 + 2x + 4$ имеет отрицательный дискриминант $D = 4 - 16 < 0$, поэтому неприводим над $\mathbb{R}$.

Ответ: $x^4 + x^3 - 8x - 8 = (x+1)(x-2)(x^2+2x+4)$.

Пример 3. Разложить над полями $\mathbb{C}$ и $\mathbb{R}$ на неприводимые множители многочлен $f(x) = x^4 + 4$.

△ Вначале над полем комплексных чисел найдем корни многочлена $x^4 + 4$.

$$x_k = \sqrt[4]{-4} = \sqrt[4]{4(\cos\pi + i\sin\pi)} = \sqrt{2}\left(\cos\frac{\pi + 2\pi k}{4} + i\sin\frac{\pi + 2\pi k}{4}\right),\ k = 0,1,2,3.$$

$$x_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = 1 + i;$$

$$x_1 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = \sqrt{2}\left(\cos\left(\pi - \frac{\pi}{4}\right) + i\sin\left(\pi - \frac{\pi}{4}\right)\right) = \sqrt{2}\left(-\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = -1 + i;$$

$$x_2 = \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = \sqrt{2}\left(\cos\left(\pi + \frac{\pi}{4}\right) + i\sin\left(\pi + \frac{\pi}{4}\right)\right) = \sqrt{2}\left(-\cos\frac{\pi}{4} - i\sin\frac{\pi}{4}\right) = -1 - i;$$

$$x_3 = \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) = \sqrt{2}\left(\cos\left(2\pi - \frac{\pi}{4}\right) + i\sin\left(2\pi - \frac{\pi}{4}\right)\right) = \sqrt{2}\left(\cos\frac{\pi}{4} - i\sin\frac{\pi}{4}\right) = 1 - i.$$

Над полем $\mathbb{C}$ получаем разложение

$f(x) = (x-(1+i))(x-(-1+i))(x-(-1-i))(x-(1-i)) = (x-1-i)(x+1-i)(x+1+i)(x-1+i)$.

Перемножим скобки, отвечающие сопряженным корням

$$(x-1-i)(x-1+i)=(x-1)^2-i^2=x^2-2x+2,$$

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

Над полем $\mathbb{R}$ получаем разложение

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

§ 13. ИНТЕРПОЛЯЦИЯ

Интерполяция – это конструктивное восстановление функции определенного класса, в данном случае многочлена, по известным ее значениям. Задачу об интерполяции можно сформулировать так. Дана таблица, в которой значениям независимой переменной сопоставлены значения функции. Требуется найти функцию (многочлен) с такой таблицей значений.

Теорема 13.1. Для данного натурального n существует, и притом только один, многочлен степени $\leq n$, который принимает любые наперед заданные значения при $n+1$ различных значениях переменного.

△ Пусть $a_1, a_2, \dots, a_{n+1}$ – попарно различные элементы, $b_1, b_2, \dots, b_{n+1}$ – произвольные элементы поля P. Построим многочлен $f(x) \in P[x]$ степени $\leq n$ такой, что $f(a_i)=b_i$ для всех i. Положим

$$(1) \qquad f(x)=\sum b_j \varphi_j(x),$$

где

$$(2) \quad \varphi_j(x)=\frac{(x-a_1)\dots(x-a_{j-1})(x-a_{j+1})\dots(x-a_{n+1})}{(a_j-a_1)\dots(a_j-a_{j-1})(a_j-a_{j+1})\dots(a_j-a_{n+1})}.$$

Проверим, что $f(x)$ обладает нужными свойствами. Так как $\deg \varphi_j(x)=n$, $j=1,2,\dots,n+1$, то $\deg f(x)\leq n$. Ясно, что

$$\varphi_j(a_i)=\begin{cases}1, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

Поэтому $f(a_i)=\sum_{j=1}^{n+1} b_j \varphi_j(a_i)=b_i$, $i=1,2,\dots,n+1$.

Таким образом, мы построили многочлен $f(x)$ по формулам (1) и (2), который принимает любые наперед заданные значения $b_1, b_2, \dots, b_{n+1}$ при $n+1$ различных значениях переменного $a_1, a_2, \dots, a_{n+1}$.

Допустим, что существует еще один многочлен $g(x)$ степени $\leq n$, который принимает те же значения $b_1, \dots, b_{n+1}$ при $n+1$ различных значениях $a_1, a_2, \dots, a_{n+1}$ переменного, т.е. $g(a_i)=b_i$, $i=1,2,\dots,n+1$. Тогда многочлен $\psi(x)=f(x)-g(x)$ имеет $n+1$ корень $a_1, \dots, a_{n+1}$, а степень $\psi(x)$ не превышает n. Так как число корней ненулевого многочлена не превышает его степень (см. следствие теоремы II.3), то $\psi(x)$ – нулевой многочлен, и $f(x)=g(x)$.

Формула (1) носит название **интерполяционной формулы Лагранжа**.

Пример 1. В кольце $\mathbb{Q}[x]$ найти многочлен $f(x)$ степени ≤ 3, если $f(-1)=1$, $f(0)=5$, $f(1)=3$, $f(2)=0$.

△ Составим таблицу

	a_1	a_2	a_3	a_4
x	-1	0	1	2
$f(x)$	1	5	3	2
	b_1	b_2	b_3	b_4

Вначале найдем $\varphi_1(x)$ по формуле (2):

$$\varphi_1(x)=\frac{(x-a_2)(x-a_3)(x-a_4)}{(a_1-a_2)(a_1-a_3)(a_1-a_4)}=\frac{x(x-1)(x-2)}{(-1)(-2)(-3)}=$$

$$=\frac{x(x^2-3x+2)}{-6}=\frac{x^3-3x^2+2x}{-6};$$

$$\varphi_2(x) = \frac{(x-a_1)(x-a_3)(x-a_4)}{(a_2-a_1)(a_2-a_3)(a_2-a_4)} = \frac{(x+1)(x-1)(x-2)}{1\cdot(-1)(-2)} =$$

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

$$\varphi_3(x) = \frac{(x-a_1)(x-a_2)(x-a_4)}{(a_3-a_1)(a_3-a_2)(a_3-a_4)} = \frac{(x+1)\,x\,(x-2)}{2\cdot 1\cdot(-1)} =$$

$$= \frac{x^3-x^2-2x}{-2};$$

$$\varphi_4(x) = \frac{(x-a_1)(x-a_2)(x-a_3)}{(a_4-a_1)(a_4-a_2)(a_4-a_3)} = \frac{(x+1)\,x\,(x-1)}{3\cdot 2\cdot 1} =$$

$$= \frac{x^3-x}{6}.$$

Теперь, по формуле (1) получаем, что

$f(x) = b_1\varphi_1(x) + b_2\varphi_2(x) + b_3\varphi_3(x) + b_4\varphi_4(x) =$

$= 1\cdot\frac{x^3-3x^2+2x}{-6} + 5\cdot\frac{x^3-3x^2-x+2}{2} + 3\cdot\frac{x^3-x^2-2x}{-2} +$

$+ 2\cdot\frac{x^3-x}{6} = x^3\left(-\frac{1}{6}+\frac{5}{2}-\frac{3}{2}+\frac{1}{3}\right) + x^2\left(\frac{1}{2}-5+\frac{3}{2}\right) + x\left(-\frac{1}{3}-\right.$

$\left.-\frac{5}{2}+3-\frac{1}{3}\right)+5 = \frac{5}{6}x^3 - 3x^2 - \frac{1}{6}x + 5$

Проверка. $f(-1)=1$, $f(0)=5$, $f(1)=3$, $f(2)=2$.

Ответ: $f(x) = \frac{5}{6}x^3 - 3x^2 - \frac{1}{6}x + 5$.

В параграфе 8 мы определили многочлены над полем A как бесконечные последовательности с конечным числом ненулевых элементов. Эти последовательности складываются и умножаются по формулам (2) и (3) § 8. Это формально алгебраический взгляд на многочлен.

По любой многочлен $f(x) \in A[x]$ определяет функцию $\widetilde{f}: a \mapsto f(a)$, ставящую в соответствие каждому элементу $a \in A$ элемент $f(a) \in A$. Поэтому многочлен $f(x)$ можно рассматривать как функцию $\widetilde{f}$. Это функциональный взгляд на многочлен. Следующая теорема показывает, что над бесконечным полем формально алгебраический и функциональный взгляд на многочлен совпадает.

Т е о р е м а 13.2. Многочлены f и g над бесконечным полем равны тогда и только тогда, когда равны определяемые ими функции $\widetilde{f}$ и $\widetilde{g}$.

Δ Если f и g - равные многочлены, то $f(a)=g(a)$ для всех $a \in A$. Поэтому определяемые ими функции $\widetilde{f}$ и $\widetilde{g}$ совпадают.

Обратно, пусть для двух многочленов f и g определяемые ими функции $\widetilde{f}$ и $\widetilde{g}$ совпадают. Через n обозначим наибольшую из степеней многочленов f и g. В бесконечном поле A можно выбрать $n+1$ попарно различных элементов $a_1, a_2, \ldots, a_{n+1}$. Так как $f(a_i)=g(a_i)$ для всех i, то по теореме 13.1 многочлены f и g совпадают. $\blacktriangle$

Над конечными полями ситуация иная. Различные многочлены могут определять одну и ту же функцию.

П р и м е р 2. Пусть $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$ - конечное поле из двух элементов и $f(x)=x+\bar{1}$, $g(x)=x^2+\bar{1}$ - два различных многочлена над полем $\mathbb{Z}_2$. Так как $f(\bar{0})=\bar{1}$, $f(\bar{1})=\bar{0}$; $g(\bar{0})=\bar{1}$, $g(\bar{1})=\bar{0}$, то как функции f и g совпадают.

§ 14. РАЦИОНАЛЬНЫЕ ДРОБИ

Р а ц и о н а л ь н а я дробь над полем A это функция $\varphi(x) = \frac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ - многочлены над полем A и $g(x) \neq 0$. Дробь $\varphi(x)$ имеет своей

областью определения все те элементы $x_0 \in A$, для которых $g(x_0) \neq 0$. Таким образом, область определения $\varphi(x)$ получается в результате удаления из поля A всех корней многочлена $g(x)$.

Две рациональные дроби $\varphi_1(x) = \frac{f_1(x)}{g_1(x)}$ и $\varphi_2(x) = \frac{f_2(x)}{g_2(x)}$ считаются **р а в н ы м и**, если их области определения совпадают и $\frac{f_1(x_0)}{g_1(x_0)} = \frac{f_2(x_0)}{g_2(x_0)}$ для любого x_0 из области определения. Последнее равенство перепишем в виде

(1) $$f_1(x_0)\,g_2(x_0) = f_2(x_0)\,g_1(x_0).$$

В бесконечном поле A элемент x_0 может принимать бесконечно много значений из области определения $\varphi_1(x)$ и $\varphi_2(x)$, поэтому условие (1) по теореме I3.2 равносильно равенству многочленов

(2) $$f_1(x)\,g_2(x) = f_2(x)\,g_1(x).$$

Обратно, Если выполняется (2), то для любого $x_0 \in A$ имеет место (1). Это означает, что рациональные дроби $\varphi_1(x)$ и $\varphi_2(x)$ принимают одинаковые значения в общей области определения. Поэтому рациональные дроби $\varphi_1(x)$ и $\varphi_2(x)$ можно считать равными, если выполняется (2).

Через $A(x)$ обозначим совокупность всех рациональных дробей над полем A.

Сложение и умножение рациональных дробей определим следующими равенствами:

(3) $$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2}$$

(4) $$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}.$$

Вполне естественно возникает вопрос: не изменится ли результат сложения и умножения при замене дробей на равные.

Пусть $\frac{f_1}{g_1} = \frac{f_3}{g_3}$, $\frac{f_2}{g_2} = \frac{f_4}{g_4}$. В силу (2) получаем, что $f_1 g_3 = f_3 g_1$ и $f_2 g_4 = f_4 g_2$.

Рассмотрим сложение:

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2}, \quad \frac{f_3}{g_3} + \frac{f_4}{g_4} = \frac{f_3 g_4 + f_4 g_3}{g_3 g_4}$$

и $g_3 g_4 (f_1 g_2 + f_2 g_1) - g_1 g_2 (f_3 g_4 + f_4 g_3) = g_2 g_4 (f_1 g_3 - f_3 g_1) + g_1 g_3 (f_2 g_4 - f_4 g_2) = 0$. Таким образом, результат сложения не зависит от замены слагаемых на равные.

Теперь рассмотрим умножение:

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}, \quad \frac{f_3}{g_3} \cdot \frac{f_4}{g_4} = \frac{f_3 f_4}{g_3 g_4}$$

и $f_1 f_2 g_3 g_4 - f_3 f_4 g_1 g_2 = f_1 f_2 g_3 g_4 - f_3 f_2 g_1 g_4 + f_3 f_2 g_1 g_4 - f_3 f_4 g_1 g_2 = f_2 g_4 (f_1 g_3 - f_3 g_1) + f_3 g_1 (f_2 g_4 - f_4 g_2) = 0$.

Значит, результат умножения также не зависит от замены сомножителей на равные.

Следовательно, равенства (3) и (4) определяют бинарные алгебраические операции на $A(x)$.

Т е о р е м а I4.1. Множество $A(x)$ рациональных дробей над полем A с операциями сложения (3) и умножения (4) является полем.

Δ Ясно, что сложение определено на $A(x)$, ассоциативно и коммутативно. Нулевым элементом будет $\frac{0}{1}$, где 0 и $1 \in A$, противоположным к $\frac{f}{g}$ элементом будет элемент $\frac{-f}{g} = -\frac{f}{g}$. Поэтому $A(x)$ с операцией сложения (3) является абелевой группой.

Умножение определено на $A(x)$ и легко проверить, что умножение ассоциативно и коммутативно. Элемент $\frac{1}{1}$ является единицей. Если f/g - ненулевой элемент, то $f \neq 0$ и дробь g/f будет обратным элементом к f/g:

$$\frac{f}{g} \cdot \frac{g}{f} = \frac{fg}{gf} = \frac{1}{1}.$$

Поэтому ненулевые элементы $A(x)$ с операцией умножения (4) также образуют абелеву группу.

Проверим дистрибутивность.

$$\left(\frac{f_1}{g_1}+\frac{f_2}{g_2}\right)\frac{f_3}{g_3}=\frac{(f_1g_2+f_2g_1)f_3}{g_1g_2g_3}=\frac{f_1g_2f_3+f_2g_1f_3}{g_1g_2g_3},$$

$$\frac{f_1}{g_1}\cdot\frac{f_3}{g_3}+\frac{f_2}{g_2}\cdot\frac{f_3}{g_3}=\frac{f_1f_3g_2+f_2f_3g_1}{g_1g_2g_3}.$$

Так как правые части совпали, то равны левые части, и сложение дистрибутивно относительно умножения. ▲

Рациональная дробь называется п р а в и л ь н о й, если степень ее числителя меньше степени знаменателя.

Л е м м а I4.2. Любая рациональная дробь есть сумма многочлена и правильной дроби.

△ Пусть $\frac{f}{g}$ – произвольная рациональная дробь. Разделим f на g с остатком:

$$f=gq+r,\quad \deg r<\deg g.$$

Теперь $\frac{f}{g}=\frac{gq+r}{g}=q+\frac{r}{g}$, где q – многочлен, а $\frac{r}{g}$ – правильная рациональная дробь.

Л е м м а I4.3. Сумма, разность и произведение правильных дробей есть правильная дробь.

△ Пусть дроби $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ – правильные. Они останутся правильными и в записи $\frac{f_1g_2}{g_1g_2}$, $\frac{f_2g_1}{g_1g_2}$. Так как $\frac{f_1}{g_1}\pm\frac{f_2}{g_2}=\frac{f_1g_2\pm f_2g_1}{g_1g_2}$ и степени обоих слагаемых в числителе меньше степени знаменателя, то сумма и разность правильных дробей – правильная дробь.

Для произведения $\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}=\frac{f_1f_2}{g_1g_2}$ имеем

$\deg f_1f_2=\deg f_1+\deg f_2<\deg g_1+\deg g_2=\deg g_1g_2$, т.е. дробь f_1f_2/g_1g_2 – правильная.

С л е д с т в и е. Совокупность всех правильных дробей является подкольцом поля $A(x)$.

Л е м м а I4.4. Если знаменатель $g=g_1g_2$ правильной рациональной дроби $f/g\in A(x)$ есть произведение двух

взаимно простых многочленов g_1 и g_2, то дробь представляется в виде суммы двух правильных дробей со знаменателями g_1 и g_2.

△ Так как g_1 и g_2 взаимно просты, то существуют такие многочлены h_1 и h_2, что $1=h_1g_1+h_2g_2$. Поэтому

$$\frac{f}{g_1g_2}=\frac{f}{g_1g_2}(h_1g_1+h_2g_2)=\frac{fh_1}{g_2}+\frac{fh_2}{g_1}.$$

Разделим fh_2 на g_1 с остатком

$$fh_2=g_1q+r,\quad \deg r<\deg g_1.$$

Теперь $\frac{fh_2}{g_1}=q+\frac{r}{g_1}$.

Присоединим q к первому слагаемому. Получим

$$\frac{f}{g_1g_2}=\frac{fh_1}{g_2}+q+\frac{r}{g_1}=\frac{fh_1+qg_2}{g_2}+\frac{r}{g_1}.$$

Здесь первое слагаемое $\frac{fh_1+qg_2}{g_2}$

автоматически становится правильной дробью как разность правильных дробей f/g_1g_2 и r/g_1.

Л е м м а I4.5. Всякая правильная рациональная дробь разлагается в сумму нескольких правильных дробей, каждая из которых имеет своим знаменателем степень некоторого неприводимого многочлена.

Д о к а з а т е л ь с т в о проведем индукцией по числу неприводимых множителей знаменателя. Пусть f/q – правильная рациональная дробь и $g=p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}$ – каноническое разложение знаменателя g на неприводимые многочлены. Тогда

$$\frac{f}{p_1^{k_1}(p_2^{k_2}\dots p_s^{k_s})}=\frac{f_1}{p_1^{k_1}}+\frac{\overline{f}_1}{p_2^{k_2}\dots p_s^{k_s}}$$ по лемме I4.4

По индукции, мы можем считать, что уже имеется разложение

$$\frac{\bar f_1}{p_2^{\kappa_2}\dots p_s^{\kappa_s}} = \frac{f_2}{p_2^{\kappa_2}} + \dots + \frac{f_s}{p_s^{\kappa_s}}.$$

Поэтому

$$\frac{f}{p_1^{\kappa_1}p_2^{\kappa_2}\dots p_s^{\kappa_s}} = \frac{f_1}{p_1^{\kappa_1}} + \frac{f_2}{p_2^{\kappa_2}} + \dots + \frac{f_s}{p_s^{\kappa_s}}$$

требуемое разложение. ▲

Правильная рациональная дробь $\frac{f}{g}$ называется **простейшей**, если ее знаменатель g является степенью неприводимого многочлена p, т.е. $g = p^\kappa$, $\kappa \geq 1$, а степень числителя f меньше степени p.

Пример 1. Над полем $\mathbb{C}$ неприводимыми являются только многочлены 1-й степени. Поэтому над полем $\mathbb{C}$ простейшими будут дроби $\frac{A}{(x-c)^\kappa}$, $\kappa \geq 1$, $A, c \in \mathbb{C}$.

Пример 2. Над полем $\mathbb{R}$ неприводимыми являются многочлены первой и второй степени с отрицательным дискриминантом. Поэтому простейшими над полем $\mathbb{R}$ будут дроби

$$\frac{A}{(x-c)^\kappa};\ \frac{Ax+B}{(x^2+px+q)^\kappa},\ p^2-4q<0;\ A, B \in \mathbb{C}.$$

Лемма 14.6. *Любая правильная рациональная дробь, знаменатель которой есть степень неприводимого многочлена, разлагается в сумму простейших дробей.*

△ Пусть f/g^κ – правильная рациональная дробь, знаменатель которой есть степень неприводимого многочлена g. Поделим f на g с остатком: $f = gq_1 + r_1$, $\deg r_1 < \deg g$. Тогда

$$\frac{f}{g^\kappa} = \frac{gq_1 + r_1}{g^\kappa} = \frac{q_1}{g^{\kappa-1}} + \frac{r_1}{g^\kappa},$$

где r_1/g^κ – простейшая дробь. Разделим q_1 на g: $q_1 = gq_2 + r_2$, $\deg r_2 < \deg g$. Теперь

$$\frac{q_1}{g^{\kappa-1}} = \frac{gq_2 + r_2}{g^{\kappa-1}} = \frac{q_2}{g^{\kappa-2}} + \frac{r_2}{g^{\kappa-1}}.$$

Дробь $r_2/g^{\kappa-1}$ – простейшая.

Теперь делим q_2 на g и т.д. Продолжая процесс, приходим к простейшей дроби $q_{\kappa-1}/g$.

Итак, $\frac{f}{g^\kappa} = \frac{r_1}{g^\kappa} + \frac{r_2}{g^{\kappa-1}} + \dots + \frac{r_\kappa}{g}$, где $r_\kappa = q_{\kappa-1}$.

Теорема 14.7. *Всякая рациональная дробь представима в виде суммы многочлена и простейших дробей.*

△ По лемме 14.2 всякая рациональная дробь представима в виде многочлена и правильной дроби. По лемме 14.5 и 14.6 всякая рациональная дробь есть сумма простейших.

РАЗЛОЖЕНИЕ ПРАВИЛЬНОЙ РАЦИОНАЛЬНОЙ ДРОБИ НА ПРОСТЕЙШИЕ НАД $\mathbb{C}$. Над полем $\mathbb{C}$ неприводимыми будут только многочлены первой степени, поэтому каждый многочлен $g(x)$ над $\mathbb{C}$ разложим в произведение

$$g(x) = a(x-c_1)^{\kappa_1}(x-c_2)^{\kappa_2}\dots(x-c_m)^{\kappa_m}.$$

Простейшими будут дроби $A/(x-c)^\kappa$, $\kappa \geq 1$, $A \in \mathbb{C}$.

Следовательно,

$$\frac{f}{g} = \frac{A_{11}}{a(x-c_1)} + \frac{A_{12}}{(x-c_1)^2} + \dots + \frac{A_{1\kappa_1}}{(x-c_1)^{\kappa_1}} +$$
$$+ \frac{A_{21}}{x-c_2} + \frac{A_{22}}{(x-c_2)^2} + \dots + \frac{A_{2\kappa_2}}{(x-c_2)^{\kappa_2}} + \dots +$$
$$+ \frac{A_{m1}}{x-c_m} + \frac{A_{m2}}{(x-c_m)^2} + \dots + \frac{A_{m\kappa_m}}{(x-c_m)^{\kappa_m}}.$$

РАЗЛОЖЕНИЕ ПРАВИЛЬНОЙ РАЦИОНАЛЬНОЙ ДРОБИ НАД $\mathbb{R}$. Над $\mathbb{R}$ неприводимыми являются многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. Поэтому каждый многочлен $g(x)$ над полем $\mathbb{R}$ разложим в произ-

ведение

$$q(x) = a(x-c_1)^{\kappa_1} \dots (x-c_m)^{\kappa_m}(x^2+p_1x+q_1)^{\ell_1} + \dots + (x^2+p_t x+q_t)^{\ell_t}.$$

Простейшими над $\mathbb{R}$ будут дроби

$$\frac{A}{(x-c)^\kappa} \quad \text{и} \quad \frac{Bx+C}{(x^2+px+q)^\ell}, \text{ где } p^2-4q<0, A,B,C\in\mathbb{R}$$

Следовательно,

$$\frac{f}{g} = \frac{A_{11}}{a(x-c_1)} + \frac{A_{12}}{(x-c_1)^2} + \dots + \frac{A_{1\kappa_1}}{(x-c_1)^{\kappa_1}} + \dots +$$

$$+ \frac{A_{m1}}{x-c_m} + \frac{A_{m2}}{(x-c_m)^2} + \dots + \frac{A_{m\kappa_m}}{(x-c_m)^{\kappa_m}} +$$

$$+ \frac{B_{11}x+C_{11}}{x^2+p_1x+q_1} + \frac{B_{12}x+C_{12}}{(x^2+p_1x+q_1)^2} + \dots + \frac{B_{1\ell_1}x+C_{1\ell_1}}{(x^2+p_1x+q_1)^{\ell_1}} +$$

$$+ \dots + \frac{B_{t1}x+C_{t1}}{x^2+p_tx+q_t} + \frac{B_{t2}x+C_{t2}}{(x^2+p_tx+q_t)^2} + \dots$$

$$\dots + \frac{B_{t\ell_t}x+C_{t\ell_t}}{(x^2+p_tx+q_t)^{\ell_t}}.$$

Пример 3. Разложить над $\mathbb{R}$ рациональную дробь

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

△ Исходная рациональная дробь неправильная. Разложим ее в сумму многочлена и правильной дроби

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

Итак, $\dfrac{x^3+x+1}{x^2+2x+1} = x-2 + \dfrac{4x+3}{x^2+2x+1}$.

Правильную рациональную дробь $\dfrac{4x+3}{(x+1)^2}$ разложим в сумму простейших

$$\frac{4x+3}{(x+1)^2} = \frac{A}{x+1} + \frac{B}{(x+1)^2} = \frac{A(x+1)+B}{(x+1)^2} = \frac{Ax+(A+B)}{(x+1)^2}.$$

Приравниваем коэффициенты при одинаковых степенях неизвестного:

$$\begin{cases} 4 = A, \\ 3 = A+B, \end{cases} \qquad \begin{cases} A = 4, \\ B = -1. \end{cases}$$

Ответ: $\dfrac{x^3+x+1}{x^2+2x+1} = (x-2) + \dfrac{4}{x+1} - \dfrac{1}{(x+1)^2}$.

Пример 4. Разложить над $\mathbb{R}$ рациональную дробь

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

△ Многочлен x^2+x+1 имеет отрицательный дискриминант, поэтому неприводим над $\mathbb{R}$. Имеем

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

$$= \frac{A(x+1)(x^2+x+1)+B(x^2+x+1)+(Cx+D)(x+1)^2}{(x+1)^2(x^2+x+1)}.$$

Приравниваем числители

$$2x-1 = A(x+1)(x^2+x+1)+B(x^2+x+1)+(Cx+D)(x+1)^2.$$

Пусть $x=-1$. Тогда $-3=B$, т.е. $B=-3$.

Пусть $x=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$. Тогда

$$2\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right)-1=\left(C\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right)+D\right)\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right),$$

$$-2+i\sqrt{3} = C\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right)^2+D\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right)=$$

$$= C\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right)+D\left(-\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right).$$

Приравнивая действительные и мнимые части, получаем

$$\begin{cases} -2=-\frac{1}{2}(C+D), \\ \sqrt{3}=\frac{\sqrt{3}}{2}(-C+D), \end{cases} \quad \begin{cases} C+D=4, \\ -C+D=2, \end{cases}$$

$D=6$, $C=1$.

Пусть $x=0$. Тогда $-1=A-3+3$ и $A=-1$.

Ответ:

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

Учебное издание
МОНАХОВ Виктор Степанович

Числа и многочлены
Тексты лекций по курсу "Алгебра и теория чисел"

Ответственный за выпуск В.С.Монахов

Редактор Е.Ф.Зайцева

Подписано к печати 20.05.92 Формат 60x84 1/16.
Бумага писчая №1. Печать офсетная. Усл.п.л.4,7.
Усл.кр.-отт. 4,5 . Уч.-изд.л. 4,0 . Тираж 250 экз. Заказ 8
Цена 35 р.20 к.

Отпечатано на ротапринте ГГУ им. Ф.Скорины. г.Гомель
ул.Советская, 104.