Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Е. Д. Стройникова

АЛГЕБРА В ПРИМЕРАХ И ЗАДАЧАХ

*Рекомендовано УМО по образованию в области информатики
и радиоэлектроники в качестве учебно-методического пособия
для специальности 1-40 04 01 «Информатика и технологии программирования»*

Минск БГУИР 2018

УДК 512(076.2)
ББК 22.14я73
С86

Р е ц е н з е н т ы:

кафедра высшей математики учреждения образования
«Белорусский государственный экономический университет»
(протокол №11 от 30.05.2016);

доцент кафедры высшей математики №1
Белорусского национального технического университета,
кандидат технических наук, доцент Т. И. Чепелева

Стройникова, Е. Д.

С86 Алгебра в примерах и задачах : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2018. – 100 с. : ил.

ISBN 978-985-543-369-0.

Приведены краткие теоретические сведения, основные формулы и задачи из разделов высшей алгебры: теории чисел, теории групп, теории колец и полей, а также (как вспомогательного для изучения двух последних разделов) раздела дискретной математики – отображения. В качестве задач прикладной направленности представлены задачи, связанные с решением диофантовых линейных уравнений, классическими шифрами и криптоалгоритмом *RSA*. К задачам для самостоятельного решения даны ответы и указания. Приводимый теоретический материал и большое количество подробно разобранных примеров решений задач позволяют использовать данное учебно-методическое пособие для всех форм обучения.

Предназначено для студентов высших учебных заведений, изучающих дисциплину «Математика. Геометрия и алгебра». Может быть полезно преподавателям и студентам математических специальностей при изучении родственных курсов.

УДК 512(076.2)
ББК 22.14я73

ISBN 978-985-543-369-0

Оглавление

Предисловие

Учебно-методическое пособие «Алгебра в примерах и задачах» составлено в соответствии с государственным образовательным стандартом, типовым учебным планом и типовой учебной программой учебной дисциплины «Математика. Геометрия и алгебра» для высших учебных заведений Республики Беларусь, обеспечивающих подготовку по специальности 1-40 04 01 «Информатика и технологии программирования». В основу данной книги положен односеместровый курс лекций и практических занятий для студентов специальностей «Информатика» и «Информатика и технологии программирования» факультета компьютерных систем и сетей БГУИР. Целью учебно-методического пособия является ознакомление читателя со специальными главами высшей алгебры и их важными приложениями к информатике, в особенности вопросами защиты информации от несанкционированного доступа, а также приобретение навыков исследования и решения практических задач с помощью современных методов алгебры. Издание может быть полезно студентам вузов математических специальностей при изучении родственных курсов, а также преподавателям.

Учебно-методическое пособие состоит из четырех глав. В книге дано краткое изложение теоретического материала, приведены примеры решения задач, представлены задачи для самостоятельного решения по основам теории чисел, теории групп, колец и полей. Для изучения материала третьей и четвертой глав во второй главе с использованием аппарата дискретной математики рассмотрены основные виды соответствий и более подробно – функциональных отображений, понятие мощности множества. В каждом параграфе разобраны примеры, иллюстрирующие изложенный теоретический материал и дающие образцы решения задач, в том числе прикладной направленности. В конце каждого параграфа размещены задачи для самостоятельного решения и ответы к ним. Для некоторых задач имеются указания к решению. Подобранные примеры и упражнения способствуют усвоению излагаемого материала и делают книгу удобной для самостоятельного изучения курса, в частности для студентов заочной и дистанционной форм обучения.

Автор выражает глубокую признательность заведующему кафедрой высшей алгебры и защиты информации Белорусского государственного университета, доктору физико-математических наук, профессору В. В. Беняш-Кривцу за ряд ценных замечаний, использованных при редактировании данного учебно-методического пособия. Автор искренне благодарит кандидата технических наук, доцента кафедры высшей математики №1 Белорусского национального технического университета Т. И. Чепелеву, а также коллектив кафедры высшей математики учреждения образования «Белорусский государственный экономический университет» (и лично – заведующего кафедрой, доктора физико-математических наук, профессора М. П. Дымкова) за обстоятельное рецензирование, способствовавшее улучшению содержания рукописи.

Глава 1. Основы теории чисел

§1.1. Делимость целых чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Соотношение Безу

Наиболее известными числовыми множествами являются следующие:
N – множество натуральных чисел;
Z – множество целых чисел;
Q – множество рациональных чисел;
R – множество вещественных чисел;
C – множество комплексных чисел.
Они связаны следующим отношением включения: $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

Если $A \subseteq \mathbf{R}$ и $a \in A$, то в дальнейшем будем обозначать $A_{>a}$, $A_{<a}$, $A_{\geq a}$ и $A_{\leq a}$ подмножества A, состоящие из всех чисел, больших a, меньших a, больших или равных a и меньших или равных a соответственно.

Множество целых чисел **Z** состоит из элементов $0, \pm 1, \pm 2, \ldots, \pm n, \ldots$. На нем определены две алгебраические операции – сложение и умножение. Отметим, что знак умножения «·» в записи можно опускать для сокращения. Операции сложения и умножения обладают следующими общими свойствами (для любых $a, b, c \in \mathbf{Z}$):

1) ассоциативностью: $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$;

2) коммутативностью: $a + b = b + a$, $ab = ba$;

3) существованием нейтральных элементов – 0 относительно сложения и 1 относительно умножения соответственно: $a + 0 = a$, $a \cdot 1 = a$;

4) существованием для каждого a такого $-a \in \mathbf{Z}$, что $a + (-a) = 0$.

Ясно, что здесь $-a$ – противоположное целое. Это свойство позволяет ввести на **Z** вспомогательную операцию – вычитание. Так, $a - b = a + (-b)$ – целое число – разность чисел a и b, получаемое вычитанием b из a.

Аналог свойства 4 для умножения выполняется лишь для двух целых чисел: 1 и –1.

Умножение и сложение связаны следующим свойством:

5) законом дистрибутивности умножения относительно сложения:

$$(a + b)c = ac + bc.$$

Теорема 1.1.1 (о делении с остатком). *Для любых целых чисел a и b, $b \neq 0$, существуют единственные целые числа q и r, $0 \leq r < |b|$, такие, что*

$$a = bq + r. \qquad (1.1.1)$$

Определение 1.1.1. В равенстве (1.1.1) r называют *остатком*, а q – *частным* (*неполным частным* при $r \neq 0$) от деления a на b.

Для нахождения частного и остатка от деления можно использовать метод деления «уголком».

Определение 1.1.2. Если в равенстве (1.1.1) $r = 0$, т. е. $a = bq$, то говорят, что *a делится* на *b* (и пишут $a \vdots b$), что *a* является *кратным* числа *b*, что *b делит a* (и пишут $b \mid a$), а также называют *b делителем*, или *множителем*, числа *a*. Все вышесказанное для *b* справедливо и для *q* при $q \neq 0$. Будем обозначать $a \not\vdots b$, если *a* не делится на *b*, и $b \nmid a$, если *b* не делит *a*.

Свойства делимости целых чисел:

1. $b \mid 0, \forall\, b \neq 0$.

2. $\pm 1 \mid a, \forall\, a \in \mathbf{Z}$.

3. $b \mid a \;\&\; a \mid c \Rightarrow b \mid c$ (свойство транзитивности).

4. $b \mid a \;\&\; a \mid b \Leftrightarrow |a| = |b|$.

5. $b \mid a_1 \;\&\ldots\&\; b \mid a_k \Rightarrow b \mid (a_1 w_1 + \ldots + a_k w_k), \forall\, k \in \mathbf{N}, \forall\, w_1, \ldots, w_k \in \mathbf{Z}$.

6. Если в равенстве $a_1 + \ldots + a_k = b_1 + \ldots + b_s$, $\forall\, k, s \in \mathbf{N}$, все слагаемые делятся на *d*, кроме, быть может, одного a_i, где $1 \le i \le k$, то и это слагаемое также делится на *d*.

7. $b \mid a \Leftrightarrow |b| \mid |a|$.

Определение 1.1.3. Если целые числа $a_1, a_2, \ldots, a_k$, где $k \ge 2$, делятся на целое $d \neq 0$, то *d* называют их *общим делителем* (*ОД*). Максимальный из общих натуральных делителей целых чисел $a_1, a_2, \ldots, a_k$, из которых хотя бы одно отлично от нуля, называется их *наибольшим общим делителем* (*НОД*) и обозначается НОД $(a_1, a_2, \ldots, a_k)$ или $(a_1, a_2, \ldots, a_k)$, если последнее не вызывает разночтений.

НОД целых чисел определен однозначно. Из свойства 7 делимости целых чисел и определения 1.1.3 вытекает, что $(a_1, a_2, \ldots, a_k) = (|a_1|, |a_2|, \ldots, |a_k|)$.

Очевидно, что если $b \mid a$, то $(a, b) = |b|$.

Теорема 1.1.2 (Евклид). *Наибольший общий делитель целых чисел a и b при условии, что* $|a| > |b|$, $b \nmid a$, *равен последнему отличному от нуля остатку от деления в цепочке равенств*:

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2, \text{ если } r_1 \neq 0,$$
$$\ldots$$
$$r_{n-2} = r_{n-1} q_n + r_n, \text{ если } r_{n-1} \neq 0,$$
$$r_{n-1} = r_n q_{n+1}, \text{ если } r_n \neq 0.$$

То есть $r_n = (a, b)$.

Теорема 1.1.2 дает *алгоритм Евклида* нахождения НОД целых чисел. С помощью рекурсии он легко преобразуется в алгоритм нахождения НОД не только двух, но и большего количества целых чисел: $(a_1, \ldots, a_{k-1}, a_k) = ((a_1, \ldots, a_{k-1}), a_k)$, где $k = 3, 4, \ldots$.

Расширенный алгоритм Евклида представляет собой выражение на каждом шаге остатка от деления r_i, где $i = \overline{1, n}$, в виде целочисленной линейной комбинации *a* и *b* в процессе вычисления (a, b). Вначале полагаем $r_{-1} = a$, $u_{-1} = 1$, $v_{-1} = 0$, $r_0 = b$, $u_0 = 0$, $v_0 = 1$. Далее для $i = \overline{1, n}$ последовательно вычисляем

$$r_i = r_{i-2} - r_{i-1}q_i,$$
$$u_i = u_{i-2} - u_{i-1}q_i,$$
$$v_i = v_{i-2} - v_{i-1}q_i.$$

Тогда для всех $i = \overline{-1, n}$ имеем $r_i = au_i + bv_i$.

Теорема 1.1.3. *Пусть* $d = (a_1, a_2, \ldots, a_k)$. *Тогда существуют такие* $w_1, w_2, \ldots, w_k \in \mathbf{Z}$, *что*

$$d = \sum_{i=1}^{k} a_i w_i. \qquad (1.1.2)$$

Определение 1.1.4. Равенство (1.1.2) называют *соотношением Безу* для наибольшего общего делителя целых чисел.

Коэффициенты соотношения Безу для НОД двух целых чисел a и b могут быть получены на последнем шаге расширенного алгоритма Евклида. Применение цепочки равенств алгоритма Евклида в обратном порядке для выражения НОД в виде целочисленной линейной комбинации a и b дает те же значения коэффициентов соотношения Безу. При $k \geq 3$ коэффициенты $w_1, w_2, \ldots, w_k$ в соотношении (1.1.2) вычисляются рекурсивно в соответствии с вычислением НОД.

Замечание. Коэффициенты $w_1, w_2, \ldots, w_k$ в равенстве (1.1.2) не являются единственными с таким условием. Это следует из теории диофантовых линейных уравнений.

Определение 1.1.5. Если целые отличные от нуля числа $a_1, a_2, \ldots, a_k$, где $k \geq 2$, делят целое m, то m называют их *общим кратным* (*ОК*). Минимальное из натуральных общих кратных целых чисел $a_1, a_2, \ldots, a_k$ называется их *наименьшим общим кратным* (*НОК*) и обозначается $\text{НОК}(a_1, a_2, \ldots, a_k)$ или $[a_1, a_2, \ldots, a_k]$, если последнее не вызывает разночтений.

НОК целых чисел определено однозначно. Из свойства 7 делимости целых чисел и определения 1.1.5 вытекает, что $[a_1, a_2, \ldots, a_k] = [|a_1|, |a_2|, \ldots, |a_k|]$.

Очевидно, что если $b \mid a$, то $[a, b] = |a|$ при $a \neq 0$.

Исходя из определений 1.1.3 и 1.1.5, можно получить формулу

$$[a, b] = \frac{|a||b|}{(a, b)}. \qquad (1.1.3)$$

С помощью рекурсии вычисляется НОК не только двух, но и большего количества целых чисел: $[a_1, \ldots, a_{k-1}, a_k] = [[a_1, \ldots, a_{k-1}], a_k]$, где $k = 3, 4, \ldots$.

Примеры

1. Найти частные и остатки от деления a на b:

а) $a = 0$, $b \neq 0$.

$0 = 0 \cdot b + 0$. Итак, $q = 0$, $r = 0$;

б) $a = 119$, $b = -852$.

$119 = 0 \cdot (-852) + 119$. Значит, $q = 0$, $r = 119$;

в) $a = 4357$, $b = 38$.

$q = 114$, $r = 25$;

$$
\begin{array}{r|l}
4357 & 38 \\
\underline{38} & 114 \\
55 & \\
\underline{38} & \\
177 & \\
\underline{152} & \\
25 &
\end{array}
$$

г) $a = -2023$, $b = 116$.

$2023 = 116 \cdot 17 + 51$;

$$
\begin{array}{r|l}
2023 & 116 \\
\underline{116} & 17 \\
863 & \\
\underline{812} & \\
51 &
\end{array}
$$

$-2023 = 116 \cdot (-17) - 51 = 116 \cdot (-18) + 116 - 51 = 116 \cdot (-18) + 65$.

Таким образом, $q = -18$, $r = 65$;

д) $a = -11078$, $b = -31$.

$11078 = 31 \cdot 357 + 11$;

$$
\begin{array}{r|l}
11078 & 31 \\
\underline{93} & 357 \\
177 & \\
\underline{155} & \\
228 & \\
\underline{217} & \\
11 &
\end{array}
$$

$-11078 = (-31) \cdot 357 - 11 = (-31) \cdot 358 + 31 - 11 = (-31) \cdot 358 + 20$.

Итак, $q = 358$, $r = 20$.

2. Пусть $z \in \mathbf{Z}$ и $z = \operatorname{sgn}(z)\overline{a_n \ldots a_1 a_0}$ – десятичная запись числа z, где $n \in \mathbf{Z}_{\geq 0}$ и функция *сигнум* вещественного числа x определяется как $\operatorname{sgn}(x) = \begin{cases} -1 & \text{при } x < 0; \\ 0 & \text{при } x = 0; \\ 1 & \text{при } x > 0. \end{cases}$

Доказать признаки делимости целых чисел:

а) на 2 и 5: $2 \mid z \Leftrightarrow 2 \mid a_0$, $5 \mid z \Leftrightarrow 5 \mid a_0$.

$|z| = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 = b + a_0$. Так как $2 \mid 10$ и $5 \mid 10$, то $2 \mid b$ и $5 \mid b$ согласно свойству 5 делимости целых чисел.

Необходимость: если $2 \mid z$ или $5 \mid z$, то $2 \mid a_0$ или $5 \mid a_0$ по свойству 6 делимости целых чисел. Достаточность: если $2 \mid a_0$ или $5 \mid a_0$, то поскольку $2 \mid b$ и $5 \mid b$, получаем $2 \mid z$ или $5 \mid z$ по свойству 5 делимости целых чисел;

б) на 4 и 25: $4 \mid z \Leftrightarrow 4 \mid \overline{a_1 a_0}$, $25 \mid z \Leftrightarrow 25 \mid \overline{a_1 a_0}$.

$|z| = a_n \cdot 10^n + \ldots + a_2 \cdot 100 + a_1 \cdot 10 + a_0 = b + \overline{a_1 a_0}$. Так как $4 \mid 100$ и $25 \mid 100$, то $4 \mid b$ и $25 \mid b$ согласно свойству 5 делимости целых чисел.

Необходимость: если $4 \mid z$ или $25 \mid z$, то $4 \mid \overline{a_1 a_0}$ или $25 \mid \overline{a_1 a_0}$ по свойству 6 делимости целых чисел. Достаточность: если $4 \mid \overline{a_1 a_0}$ или $25 \mid \overline{a_1 a_0}$, то поскольку $4 \mid b$ и $25 \mid b$, получаем $4 \mid z$ или $25 \mid z$ по свойству 5 делимости целых чисел;

в) на 3 и 9: $3 \mid z \Leftrightarrow 3 \mid (a_n + \ldots + a_1 + a_0)$, $9 \mid z \Leftrightarrow 9 \mid (a_n + \ldots + a_1 + a_0)$.

$|z| = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 = a_n(9+1)^n + \ldots + a_1(9+1) + a_0 = b + a_n + \ldots + a_1 + a_0 = b + c$. Согласно формуле бинома Ньютона и свойству 5 делимости целых чисел $9 \mid b$. По свойству 3 делимости целых чисел $3 \mid b$, т. к. $3 \mid 9$ и $9 \mid b$.

Необходимость: если $3 \mid z$ или $9 \mid z$, то $3 \mid c$ или $9 \mid c$ по свойству 6 делимости целых чисел. Достаточность: если $3 \mid c$ или $9 \mid c$, то поскольку $3 \mid b$ и $9 \mid b$, получаем $3 \mid z$ или $9 \mid z$ по свойству 5 делимости целых чисел.

3. Доказать следующие утверждения:

а) $\left(\overline{a_1a_0} - \overline{a_0a_1}\right) \vdots 9$, где a_0 и a_1 – десятичные цифры числа, $0 \le a_0, a_1 \le 9$.

$\overline{a_1a_0} - \overline{a_0a_1} = a_1 \cdot 10 + a_0 - (a_0 \cdot 10 + a_1) = (a_1 - a_0) \cdot 10 + (a_0 - a_1) = (a_1 - a_0) \cdot 9 \vdots 9$, поскольку $(a_1 - a_0) \in \mathbf{Z}$;

б) $\overline{a_0a_0a_0} \vdots 37$, где a_0 – десятичная цифра числа, $0 \le a_0 \le 9$.

$\overline{a_0a_0a_0} = a_0 \cdot 100 + a_0 \cdot 10 + a_0 = a_0 \cdot 111 = (a_0 \cdot 3) \cdot 37 \vdots 37$;

в) среди любых трех последовательных чисел a, $a+1$, $a+2$, где $a \in \mathbf{Z}$, одно и только одно делится на 3. Обобщить утверждение для любых k последовательных целых чисел, где $k \in \mathbf{N}$.

1) Пусть $a = 3q$, где $q \in \mathbf{Z}$, тогда $a + 1 = 3q + 1$, $a + 2 = 3q + 2$. В этом случае только $a \vdots 3$, поскольку у $a+1$ и $a+2$ остатки от деления на 3 равны 1 и 2 соответственно.

2) Пусть $a = 3q + 1$, где $q \in \mathbf{Z}$, тогда $a + 1 = 3q + 2$, $a + 2 = 3q + 3 = 3(q + 1)$. В этом случае только $(a+2) \vdots 3$, поскольку у a и $a+1$ остатки от деления на 3 равны 1 и 2 соответственно.

3) Пусть $a = 3q + 2$, где $q \in \mathbf{Z}$, тогда $a + 1 = 3q + 3 = 3(q + 1)$, $a + 2 = 3(q + 1) + 1$. В этом случае только $(a+1) \vdots 3$, поскольку у a и $a+2$ остатки от деления на 3 равны 2 и 1 соответственно.

Рассматривая остатки от деления на k любых последовательных k целых чисел, можно видеть, что все остатки различны, принимают значения от 0 до $k-1$ и во всех возможных k случаях каждый раз только один из остатков нулевой. Таким образом, получаем обобщение утверждения: среди любых k последовательных целых чисел одно и только одно из них делится на натуральное число k.

4. Найти НОД целых чисел с помощью алгоритма Евклида:

а) (831, 2022).

$$
\begin{array}{rl}
2022 & \big| \underline{831} \\
\underline{1662} & \big| 2 \\
831 & \big| \underline{360} \quad — r_1 \\
\underline{720} & \big| 2 \\
360 & \big| \underline{111} \quad — r_2 \\
\underline{333} & \big| 3 \\
111 & \big| \underline{27} \quad — r_3 \\
\underline{108} & \big| 4 \\
27 & \big| \underline{3} \quad — r_4 \\
\underline{27} & \big| 9 \\
0 &
\end{array}
$$

$(831, 2022) = r_4 = 3$;

б) (−2584, 1824, −171).

1-й способ

$d = (-2584, 1824, -171) = \big((-2584, 1824), -171\big)$;

$$\begin{array}{r|l} 2584 & 1824 \\ \underline{1824} & 1 \end{array}$$
$$\begin{array}{r|l} 1824 & 760 \\ \underline{1520} & 2 \end{array} \text{ — } r_1$$
$$\begin{array}{r|l} 760 & 304 \\ \underline{608} & 2 \end{array} \text{ — } r_2$$
$$\begin{array}{r|l} 304 & 152 \\ \underline{304} & 2 \end{array} \text{ — } r_3$$
$$0$$

$$\begin{array}{r|l} 171 & 152 \\ \underline{152} & 1 \end{array}$$
$$\begin{array}{r|l} 152 & 19 \\ \underline{152} & 8 \end{array} \text{ — } r_1$$
$$0$$

$(-2584, 1824) = r_3 = 152$; $d = (152, -171) = r_1 = 19$.

2-й способ

$d = (-2584, 1824, -171) = \big((-2584, -171), 1824\big)$;

$$\begin{array}{r|l} 2584 & 171 \\ \underline{171} & 15 \end{array}$$
$$\underline{874}$$
$$\underline{855}$$
$$\begin{array}{r|l} 171 & 19 \\ \underline{171} & 9 \end{array} \text{ — } r_1$$
$$0$$

$$\begin{array}{r|l} 1824 & 19 \\ \underline{171} & 96 \end{array}$$
$$\underline{114}$$
$$\underline{114}$$
$$0$$

$(-2584, -171) = r_1 = 19$; $d = (19, 1824) = 19$.

Как видно, вычисление НОД 2-м способом требует меньшего количества шагов, чем 1-м способом. Здесь еще возможен 3-й способ вычисления, содержащий на 1 шаг меньше, чем 1-й способ: $(1824, -171) = r_2 = 57$; $d = (57, -2584) = r_1 = 19$. Таким образом, оптимальным является здесь 2-й способ.

5. Записать соотношение Безу для НОД чисел из примера 4:

а) $(831, 2022) = r_4 = 3$. Найдем выражение НОД в виде целочисленной линейной комбинации чисел 831 и 2022, используя расширенный алгоритм Евклида:

$$r_{-1} = 2022,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 831,\ u_0 = 1,\ v_0 = 0;$$
$$q_1 = 2,\ u_1 = u_{-1} - u_0 q_1 = -2,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 360 = 831 \cdot (-2) + 2022;$$
$$q_2 = 2,\ u_2 = u_0 - u_1 q_2 = 5,\ v_2 = v_0 - v_1 q_2 = -2 \Rightarrow r_2 = 111 = 831 \cdot 5 + 2022 \cdot (-2);$$
$$q_3 = 3,\ u_3 = u_1 - u_2 q_3 = -17,\ v_3 = v_1 - v_2 q_3 = 7 \Rightarrow r_3 = 27 = 831 \cdot (-17) + 2022 \cdot 7;$$
$$q_4 = 4,\ u_4 = u_2 - u_3 q_4 = 73,\ v_4 = v_2 - v_3 q_4 = -30 \Rightarrow r_4 = 3 = 831 \cdot 73 + 2022 \cdot (-30).$$

Итак, $3 = 831u + 2022v$, где $u = 73$, $v = -30$.

б) Согласно 1-му способу вычисления $(-2584, 1824, -171) = (152, -171) = r_1 = 19$, причем $(-2584, 1824) = r_3 = 152$. Найдем выражение НОД в виде целочисленной линейной комбинации чисел −2584, 1824 и −171, используя расширенный алгоритм Евклида:

1) $r_{-1} = 2584,\ u_{-1} = 1,\ v_{-1} = 0;\ r_0 = 1824,\ u_0 = 0,\ v_0 = 1;$
$$q_1 = 1,\ u_1 = u_{-1} - u_0 q_1 = 1,\ v_1 = v_{-1} - v_0 q_1 = -1 \Rightarrow r_1 = 760 = 2584 + 1824 \cdot (-1);$$
$$q_2 = 2,\ u_2 = u_0 - u_1 q_2 = -2,\ v_2 = v_0 - v_1 q_2 = 3 \Rightarrow r_2 = 304 = 2584 \cdot (-2) + 1824 \cdot 3;$$
$$q_3 = 2,\ u_3 = u_1 - u_2 q_3 = 5,\ v_3 = v_1 - v_2 q_3 = -7 \Rightarrow r_3 = 152 = 2584 \cdot 5 + 1824 \cdot (-7);$$

$$2)\ r_{-1} = 171,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 152,\ u_0 = 1,\ v_0 = 0;$$

$$q_1 = 1,\ u_1 = u_{-1} - u_0 q_1 = -1,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 19 = 152 \cdot (-1) + 171 =$$

$$= 2584 \cdot (-5) + 1824 \cdot 7 + 171 = (-2584) \cdot 5 + 1824 \cdot 7 + (-171) \cdot (-1).$$

Таким образом, $19 = (-2584)u + 1824v + (-171)w$, где $u = 5$, $v = 7$, $w = -1$, согласно 1-му способу вычисления НОД.

Согласно 2-му способу вычисления $(-2584, 1824, -171) = (19, 1824) = 19$, причем $(-2584, -171) = r_1 = 19$. Тогда

$$r_{-1} = 2584,\ u_{-1} = 1,\ v_{-1} = 0;\ r_0 = 171,\ u_0 = 0,\ v_0 = 1;$$

$$q_1 = 15,\ u_1 = u_{-1} - u_0 q_1 = 1,\ v_1 = v_{-1} - v_0 q_1 = -15 \Rightarrow r_1 = 19 = 2584 + 171 \cdot (-15) =$$

$$= (-2584) \cdot (-1) + 1824 \cdot 0 + (-171) \cdot 15.$$

То есть коэффициенты соотношения Безу $u = -1$, $v = 0$, $w = 15$ находятся гораздо быстрее при 2-м способе вычисления НОД, являющемся оптимальным.

6. Найти НОК целых чисел из примера 4:

а) согласно формуле (1.1.3) получим

$$[831, 2022] = \frac{831 \cdot 2022}{(831, 2022)} = \frac{1680282}{3} = 560094;$$

б) с использованием формулы (1.1.3) получим формулу НОК трех чисел:

$$[a, b, c] = [[a, b], c] = \left[\frac{|a||b|}{(a, b)}, c\right] = \frac{|a||b||c|}{(a, b)\left(\frac{|a||b|}{(a,b)}, c\right)}.$$

Тогда согласно 1-му способу рекурсивного вычисления НОК, соответствующему 1-му способу вычисления НОД данных чисел, получим

$$[-2584, 1824, -171] = \frac{2584 \cdot 1824 \cdot 171}{152\left(\frac{2584 \cdot 1824}{152}, 171\right)} = \frac{31008 \cdot 171}{(31008, 171)} = \frac{5302368}{57} = 93024.$$

Так как $31008 = 171 \cdot 181 + 57$, $171 = 57 \cdot 3$, то $(31008, 171) = r_1 = 57$.

Два других способа дают тот же результат для $[-2584, 1824, -171]$, но при известных значениях $(-2584, -171) = 19$ и $(1824, -171) = 57$ содержат на 1 шаг больше при вычислении $(23256, 1824) = r_2 = 456$ и $(5472, 2584) = r_2 = 152$ соответственно.

Задачи

1. Найти частные и остатки от деления a на b:

а) $a = 13677$, $b = -189$; **б)** $a = -3198$, $b = 7293$; **в)** $a = -1958$, $b = -2275$.

2. Пусть $z \in \mathbf{Z}$ и $z = \operatorname{sgn}(z)\overline{a_n \ldots a_1 a_0}$ – десятичная запись числа z, где $n \in \mathbf{Z}_{\geq 0}$. Доказать признаки делимости целых чисел:

а) на 8 и 125: $8 \mid z \Leftrightarrow 8 \mid \overline{a_2 a_1 a_0}$, $125 \mid z \Leftrightarrow 125 \mid \overline{a_2 a_1 a_0}$;

б) на 11: $11 \mid z \Leftrightarrow 11 \mid \left((-1)^n a_n + \ldots - a_1 + a_0\right)$. Указание: $10 = 11 - 1$.

3. Доказать утверждение: $(k^n - 1) \vdots (k - 1)$ для любых $k \in \mathbf{N}_{\geq 2}$ и $n \in \mathbf{Z}_{\geq 0}$. Указание: для $n = 0$ утверждение очевидно, для $n \in \mathbf{N}$ использовать представление $k = (k - 1) + 1$ и метод математической индукции или формулу бинома Ньютона либо использовать формулу сокращенного умножения для $k^n - 1$.

4. Найти $(-2057, -1496, 451)$ с помощью алгоритма Евклида.

5. Записать соотношение Безу для НОД из задачи 4.

6. Найти НОК целых чисел из задачи 4.

Ответы

1. а) $q = -72,\ r = 69$; **б)** $q = -1,\ r = 4095$; **в)** $q = 1,\ r = 317$. **4.** 11. **5.** $u = 36$, $v = -48,\ w = 5$, если использовать порядок вычислений $((-2057, -1496), 451)$; $u = 0,\ v = -19,\ w = -63$, если использовать оптимальный порядок вычислений $((-1496, 451), -2057)$. **6.** 674696.

§1.2. Простые числа. Взаимно простые числа. Основная теорема арифметики

Определение 1.2.1. Натуральное число $p > 1$ называется *простым*, если из натуральных чисел оно делится только на 1 и само себя, в противном случае p называется *составным*. Число 1 не является ни простым, ни составным. Таким образом,

$$\mathbf{N} = \{1\} \cup \{\text{простые числа}\} \cup \{\text{составные числа}\}.$$

Теорема 1.2.1. *Наименьший делитель* $p > 1$ *натурального числа* $n > 1$ *есть число простое, причем если* n *– составное число, то* $p \le \sqrt{n}$.

Свойства простых чисел:

1. Для любого $n \in \mathbf{N}$ и любого простого p имеем $(n,\ p) = \begin{cases} 1 & \text{при } p \nmid n; \\ p & \text{при } p \mid n. \end{cases}$

2. $(p_1, p_2) = 1$, если $p_1 \ne p_2$ – различные простые числа.

Заметим, что из соотношения $n = pq$ натуральных чисел при $1 < p, q < n$ следует, что либо p, либо q принадлежит отрезку $[2; \sqrt{n}]$. Исторически первый метод проверки числа n на простоту заключался в делении его на простые числа, не превосходящие $\sqrt{n}$. Если среди таких чисел делителей не найдено, то n – простое число. Это один из вариантов так называемого «*решета*» Эратосфена – алгоритма поиска всех простых чисел, не превосходящих заданного n.

Для нахождения всех простых чисел, не превосходящих заданного числа n, следуя методу Эратосфена, нужно выполнить следующие шаги:

1) выписать подряд все целые числа от 2 до n;

2) пусть переменная p изначально равна 2 – первому простому числу;

3) зачеркнуть в списке все незачеркнутые ранее числа, кратные p, начиная с числа p^2, потому что все составные числа, меньшие p^2, уже будут зачеркнуты к этому времени;

4) найти первое незачеркнутое число в списке, большее p, и присвоить значению переменной p это число;

5) повторять шаги 3 и 4, пока $p \le [\sqrt{n}]$, где $[\sqrt{n}]$ – целая часть $\sqrt{n}$.

В результате все составные числа будут зачеркнуты, а незачеркнутыми останутся все простые числа из $[2; n]$.

В целом «решето» Эратосфена решает более общую задачу нахождения всех простых чисел на отрезке натурального ряда $[m; n]$, где $m < n$. В этом слу-

чае сначала находятся все простые числа, не превосходящие $[\sqrt{n}]$, затем из $[m; n]$ исключаются все кратные этим простым составные числа.

Теорема 1.2.2 (Евклид). *Простых чисел бесконечно много.*

Теорема 1.2.3 (П. Л. Чебышев). *При любом* $n > 1$ *между натуральными числами* n *и* $2n$ *обязательно найдутся простые.*

Определение 1.2.2. Целые числа $a_1, a_2, \ldots, a_k$, где $k \geq 2$, называются *взаимно простыми*, если $(a_1, a_2, \ldots, a_k) = 1$.

Такие числа не имеют общих простых делителей. Развитием теоремы 1.1.3 является следующая теорема.

Теорема 1.2.4 (критерий взаимной простоты). *Целые числа* $a_1, a_2, \ldots, a_k$, *где* $k \geq 2$, *взаимно просты тогда и только тогда, когда существуют такие целые числа* $w_1, w_2, \ldots, w_k$, *что*

$$\sum_{i=1}^{k} a_i w_i = 1.$$

Свойства взаимно простых чисел:

1. $(a_1, a_2, \ldots, a_k) = d \Leftrightarrow (a_1/d, a_2/d, \ldots, a_k/d) = 1$.

2. $c \mid ab \;\&\; (c, a) = 1 \Rightarrow c \mid b$.

3. $(a, c) = 1 \;\&\; (b, c) = 1 \Leftrightarrow (ab, c) = 1$.

4. Следствие из свойства 3. Простое число p делит произведение $n_1 n_2 \ldots n_k$, где $k \in \mathbf{N}$, тогда и только тогда, когда $\exists\, n_i$, $1 \leq i \leq k$, со свойством $p \mid n_i$.

Теорема 1.2.5 (основная теорема арифметики). *Всякое натуральное число* $n > 1$ *однозначно раскладывается в произведение простых чисел с точностью до порядка следования множителей*:

$$n = p_1 \ldots p_s. \qquad (1.2.1)$$

Определение 1.2.3. Если в равенстве (1.2.1) собрать одинаковые множители в степени, то получим *каноническое разложение* натурального числа $n > 1$: $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, где $\alpha_i \in \mathbf{N}$, $i = \overline{1, t}$, $p_i \neq p_j$ при $i \neq j$. Если z – целое, не равное 0 и ± 1 число, то $z = \operatorname{sgn}(z) p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ – *каноническое разложение* z.

По каноническому разложению целых чисел легко находятся их НОД и НОК, решаются иные задачи.

Пусть $a_1, a_2, \ldots, a_k$, где $k \geq 2$, – ненулевые целые числа, хотя бы одно из которых отлично от ± 1. Запишем их канонические разложения:

$$a_i = \operatorname{sgn}(a_i) p_1^{\alpha_{i1}} \ldots p_t^{\alpha_{it}},\ t \in \mathbf{N},\ \alpha_{ij} \in \mathbf{Z}_{\geq 0},\ j = \overline{1, t},\ i = \overline{1, k},$$

где $p_1, \ldots, p_t$ – простые числа, входящие во все разложения a_i, $i = \overline{1, k}$, причем в случае отсутствия множителя p_j в разложении a_i полагается $\alpha_{ij} = 0$.

Тогда, исходя из определений 1.1.3, 1.1.5 и 1.2.3, получаем следующие формулы для канонических разложений НОД и НОК чисел $a_1, a_2, \ldots, a_k$:

$$(a_1, a_2, \ldots, a_k) = p_1^{\gamma_1} \ldots p_t^{\gamma_t}, \text{ где } \gamma_j = \min_{1 \leq i \leq k} \alpha_{ij},\ j = \overline{1, t}; \qquad (1.2.2)$$

$$[a_1, a_2, \ldots, a_k] = p_1^{\delta_1} \ldots p_t^{\delta_t}, \text{ где } \delta_j = \max_{1 \leq i \leq k} \alpha_{ij},\ j = \overline{1, t}. \qquad (1.2.3)$$

Примеры

1. Проверить на простоту числа методом «решета» Эратосфена:

а) 179.

Поскольку $\left[\sqrt{179}\right] = 13$, то рассмотрим простые числа в пределах от 2 до 13: 2, 3, 5, 7, 11, 13. Можно проверить, что 179 не делится ни на одно из этих чисел. Поэтому 179 – простое число.

б) 719.

Поскольку $\left[\sqrt{719}\right] = 26$, то рассмотрим простые числа в пределах от 2 до 26: 2, 3, 5, 7, 11, 13, 17, 19, 23. Можно проверить, что 719 не делится ни на одно из этих чисел. Поэтому 719 – простое число.

2. Выписать все простые числа из диапазона от 200 до 225.

Так как $\sqrt{225} = 15$, то простыми числами из данного диапазона будут все числа, не кратные простым числам 2, 3, 5, 7, 11, 13. Находим, что только 211 и 223 – простые числа из отрезка [200; 225].

3. Доказать, что для любого $n \in \mathbf{N}_{>2}$ между n и $n!$ найдутся простые числа. Здесь $n! = 1 \cdot 2 \cdot \ldots \cdot n$ для $n \in \mathbf{N}$, $0! = 1$.

1-й способ

Рассмотрим число $n! - 1 > 1$ при $n > 2$. Так как $n! - (n! - 1) = 1$, то числа $n!$ и $n! - 1$ взаимно просты по теореме 1.2.4. Делителями $n!$ являются все делители чисел от 1 до n, простыми делителями $n!$ являются все простые числа из отрезка $[2; n]$, поскольку $n! = 2 \cdot 3 \cdot \ldots \cdot n$.

$n < n! - 1 < n!$ при $n > 2$. Поэтому либо $n! - 1$ – простое число, либо составное и имеет простые делители, большие n и, естественно, меньшие $n!$. Таким образом, существует простое число p с условием $n < p < n!$.

2-й способ

Согласно теореме 1.2.3 между натуральными числами n и $2n$ при $n > 2$ обязательно найдутся простые числа. Так как $n < 2n \le n!$ при $n > 2$, то для таких n существуют простые числа p с условием $n < p < n!$.

4. Доказать, что для всякого натурального n существует $k \in \mathbf{N}$ и отрезок $[k; k+n]$ натурального ряда, все числа которого составные.

При $k = (n+2)! + 2$ все следующие числа составные: $k, k+1, \ldots, k+n$. Действительно,

$$k = 2 \cdot (3 \cdot \ldots \cdot (n+2) + 1),\ k+1 = 3 \cdot (2 \cdot 4 \cdot \ldots \cdot (n+2) + 1), \ldots$$

$$\ldots,\ k+n = (n+2) \cdot (2 \cdot \ldots \cdot (n+1) + 1).$$

5. Найти каноническое разложение числа 8279848.

$8279848 = 2 \cdot 4139924 = 2^2 \cdot 2069962 = 2^3 \cdot 1034981$, $2 \nmid 1034981$.

$\left[\sqrt{1034981}\right] = 1017$. Ищем минимальное простое p_1, такое, что $2 < p_1 < 1017$ и $p_1 \mid 1034981$. Находим $p_1 = 29$, тогда $1034981 = 29 \cdot 35689$, $29 \nmid 35689$.

$\left[\sqrt{35689}\right] = 188$. Ищем минимальное простое p_2, такое, что $29 < p_2 < 188$ и $p_2 \mid 35689$. Находим $p_2 = 89$, тогда $35689 = 89 \cdot 401$, $89 \nmid 401$.

$[\sqrt{401}] = 20$. Поскольку $20 < 29 < 89$, то не существует простого $p_3 < 20$, такого, что $p_3 \mid 401$. Значит, 401 – простое число.

Итак, получаем каноническое разложение: $8279848 = 2^3 \cdot 29 \cdot 89 \cdot 401$.

6. Найти канонические разложения чисел $a = 244604911$ и $b = -61875907$ и канонические разложения их НОД и НОК.

$[\sqrt{a}] = 15639$. Ищем минимальное простое p_1, такое, что $2 < p_1 < 15639$ и $p_1 \mid a$. Находим $p_1 = 31$, тогда $a = 31 \cdot 7890481$, $31 \nmid 7890481$.

$[\sqrt{7890481}] = 2809$. Ищем минимальное простое p_2, такое, что $31 < p_2 < 2809$ и $p_2 \mid 7890481$. Находим $p_2 = 53$, и $7890481 = 53 \cdot 148877 = 53^2 \cdot 2809 = 53^3 \cdot 53 = 53^4$.

$[\sqrt{|b|}] = 7866$. Ищем минимальное простое p_1, такое, что $2 < p_1 < 7866$ и $p_1 \mid b$. Находим $p_1 = 31$, и $|b| = 31 \cdot 1995997 = 31^2 \cdot 64387 = 31^3 \cdot 2077 = 31^4 \cdot 67$, $31 \nmid 67$.

$[\sqrt{67}] = 8$. Поскольку $8 < 31$, то не существует простого $p_2 < 8$, такого, что $p_2 \mid 67$. Значит, 67 – простое число.

Имеем канонические разложения чисел: $a = 31 \cdot 53^4$, $b = -31^4 \cdot 67$.

По формулам (1.2.2) и (1.2.3) получаем канонические разложения НОД и НОК: $(a, b) = 31$, $[a, b] = 31^4 \cdot 53^4 \cdot 67$.

Задачи

1. Выписать все простые числа из указанного диапазона:

а) от 2320 до 2350; **б)** от 1300 до 1350.

2. Найти канонические разложения чисел a, b, c и канонические разложения их НОД и НОК:

а) $a = -356216713$, $b = 312380651$, $c = -2212339679$;

б) $a = -16254559$, $b = -44250139$, $c = 1643534754511$.

Ответы

1. а) 2333, 2339, 2341, 2347; **б)** 1301, 1303, 1307, 1319, 1321, 1327. **2. а)** $a = -47^4 \cdot 73$, $b = 11 \cdot 73^4$, $c = -11^2 \cdot 47 \cdot 73^3$, $(a, b, c) = 73$, $[a, b, c] = 11^2 \cdot 47^4 \cdot 73^4$; **б)** $a = -43^2 \cdot 59 \cdot 149$, $b = -43 \cdot 97 \cdot 103^2$, $c = 13^3 \cdot 43^3 \cdot 97^2$, $(a, b, c) = 43$, $[a, b, c] = 13^3 \cdot 43^3 \cdot 59 \cdot 97^2 \cdot 103^2 \cdot 149$.

§1.3. Диофантовы линейные уравнения. Сравнения целых чисел

Определение 1.3.1. *Диофантовым линейным уравнением* называется уравнение вида

$$a_1 x_1 + \ldots + a_n x_n = b, \qquad (1.3.1)$$

где $n \in \mathbf{N}$, коэффициенты и правая часть $a_1, \ldots, a_n, b \in \mathbf{Z}$, $\exists\, a_i \neq 0$, $1 \le i \le n$, а решения $(x_1, \ldots, x_n)$ – множества упорядоченных наборов из n элементов – также ищутся в целых числах.

Теорема 1.3.1. *Уравнение* (1.3.1) *разрешимо в целых числах тогда и только тогда, когда* $\text{НОД}(a_1, \ldots, a_n) \mid b$.

Рассмотрим частный случай уравнения (1.3.1) – уравнение с двумя неизвестными:

$$ax + by = c, \tag{1.3.2}$$

где $a, b, c \in \mathbf{Z}$, $a \neq 0$ либо $b \neq 0$, а пары-решения (x, y) ищутся в целых числах.

Алгоритм решения диофантовых линейных уравнений с двумя неизвестными:

1. Если НОД$(a, b) \nmid c$, то уравнение (1.3.2) не имеет решений в целых числах.

2. При $a \mid c$, $a \neq 0$, $b = 0$ множество всех целочисленных решений уравнения (1.3.2) имеет вид $\{(c/a, t) \mid t \in \mathbf{Z}\}$.

3. При $b \mid c$, $a = 0$, $b \neq 0$ множество всех целочисленных решений уравнения (1.3.2) имеет вид $\{(t, c/b) \mid t \in \mathbf{Z}\}$.

4. При НОД$(a, b) = d$, $d \mid c$, $a \neq 0$, $b \neq 0$ приходим к уравнению

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \tag{1.3.3}$$

и переходим к шагу 5.

5. Поскольку НОД$(a/d, b/d) = 1$ (свойство 1 взаимно простых чисел), то по теореме 1.2.4 (критерий взаимной простоты) существуют и находятся, например по расширенному алгоритму Евклида, $u_*, v_* \in \mathbf{Z}$, такие, что выполняется соотношение Безу

$$\frac{a}{d}u_* + \frac{b}{d}v_* = 1. \tag{1.3.4}$$

Далее переходим к шагу 6.

6. Умножим обе части равенства (1.3.4) на c/d, получим

$$\frac{a}{d}\frac{c}{d}u_* + \frac{b}{d}\frac{c}{d}v_* = \frac{c}{d},$$

откуда $x_* = \frac{c}{d}u_*$, $y_* = \frac{c}{d}v_*$ – частное решение (1.3.3), а значит, и (1.3.2). Переходим к шагу 7.

7. Множество всех целочисленных решений уравнения (1.3.2) имеет вид

$$\left\{\left(x_* + \frac{b}{d}t,\ y_* - \frac{a}{d}t\right) \,\middle|\, t \in \mathbf{Z}\right\}. \tag{1.3.5}$$

Теорема 1.3.2. *Пусть m – натуральное число. Для любых целых чисел a и b следующие условия равносильны*:

1) *a и b имеют одинаковые остатки от деления на m*;

2) *a – b делится на m, т. е. a – b = mq для подходящего целого q*;

3) *a = b + mq для некоторого целого q*.

Определение 1.3.2. Целые числа a и b называются *сравнимыми по модулю m*, если они удовлетворяют условиям теоремы 1.3.2. Этот факт обозначают формулой $a \equiv b \pmod m$ или $a \equiv b\ (m)$. Данное соотношение между целыми числами называют *сравнением по модулю m*.

Свойства сравнений:

1. К обеим частям сравнения можно прибавить или вычесть из обеих частей одно и то же целое число, т. е. для всякого целого c

$$a \equiv b \pmod{m} \Leftrightarrow a \pm c \equiv b \pm c \pmod{m}.$$

2. Сравнения можно почленно складывать и вычитать:

$$a_1 \equiv b_1 \pmod{m} \;\&\; a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}.$$

3. Сравнения можно почленно перемножать:

$$a_1 \equiv b_1 \pmod{m} \;\&\; a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

4. Следствие из свойства 3. Сравнения можно почленно возводить в любую натуральную степень: $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$, $\forall\, n \in \mathbf{N}$.

5. Если в сравнении числа a, b, m имеют общий делитель d, то на него обе части сравнения и модуль можно сократить:

$$a \equiv b \pmod{m} \Leftrightarrow a/d \equiv b/d \pmod{m/d}.$$

6. Обе части сравнения можно сократить на их общий множитель, взаимно простой с модулем: если $d \mid a$, $d \mid b$, $(d, m) = 1$, то

$$a \equiv b \pmod{m} \Leftrightarrow a/d \equiv b/d \pmod{m}.$$

7. Рефлексивность: для любого целого a и всякого натурального m

$$a \equiv a \pmod{m}.$$

8. Симметричность: $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

9. Транзитивность: $a \equiv b \pmod{m} \;\&\; b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Примеры

1. Решить диофантовы линейные уравнения:

а) $$60x + 80y = 440. \qquad (1.3.6)$$

Так как $60 = 2^2 \cdot 3 \cdot 5$, $80 = 2^4 \cdot 5$, то НОД$(60, 80) = 2^2 \cdot 5 = 20$; $20 \mid 440$, поэтому уравнение (1.3.6) имеет решения в целых числах и равносильно уравнению

$$3x + 4y = 22. \qquad (1.3.7)$$

НОД$(3, 4) = 1$, вспомогательное уравнение имеет вид

$$3u + 4v = 1. \qquad (1.3.8)$$

Найдем u_* и v_* по расширенному алгоритму Евклида:

$$r_{-1} = 4,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 3,\ u_0 = 1,\ v_0 = 0;$$

$$q_1 = 1,\ u_1 = u_{-1} - u_0 q_1 = -1,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 1 = 3 \cdot (-1) + 4.$$

Тогда $u_* = -1$, $v_* = 1$ – частное решение уравнения (1.3.8). Поэтому $x_* = -22$, $y_* = 22$ – частное решение уравнения (1.3.7).

По формуле (1.3.5) находим множество всех целочисленных решений уравнения (1.3.6): $\{(-22 + 4t,\ 22 - 3t) \mid t \in \mathbf{Z}\}$.

б) $$39x - 22y = 10. \qquad (1.3.9)$$

Так как $39 = 3 \cdot 13$, $22 = 2 \cdot 11$, то НОД$(39, -22) = 1$; $1 \mid 10$, поэтому уравнение (1.3.9) имеет решения в целых числах. Составим вспомогательное уравнение:

$$39u - 22v = 1. \qquad (1.3.10)$$

Найдем u_* и v_* по расширенному алгоритму Евклида:

$$r_{-1} = 39,\ u_{-1} = 1,\ v_{-1} = 0;\ r_0 = 22,\ u_0 = 0,\ v_0 = 1;$$

$$q_1 = 1,\ u_1 = u_{-1} - u_0 q_1 = 1,\ v_1 = v_{-1} - v_0 q_1 = -1 \Rightarrow r_1 = 17 = 39 + 22 \cdot (-1);$$

$$q_2 = 1,\ u_2 = u_0 - u_1 q_2 = -1,\ v_2 = v_0 - v_1 q_2 = 2 \Rightarrow r_2 = 5 = 39\cdot(-1) + 22\cdot 2;$$
$$q_3 = 3,\ u_3 = u_1 - u_2 q_3 = 4,\ v_3 = v_1 - v_2 q_3 = -7 \Rightarrow r_3 = 2 = 39\cdot 4 + 22\cdot(-7);$$
$$q_4 = 2,\ u_4 = u_2 - u_3 q_4 = -9,\ v_4 = v_2 - v_3 q_4 = 16 \Rightarrow r_4 = 1 = 39\cdot(-9) + 22\cdot 16 =$$
$$= 39\cdot(-9) + (-22)\cdot(-16).$$

Тогда $u_* = -9,\ v_* = -16$ – частное решение уравнения (1.3.10). Поэтому $x_* = -90,\ y_* = -160$ – частное решение уравнения (1.3.9).

По формуле (1.3.5) находим множество всех целочисленных решений уравнения (1.3.9): $\{(-90 - 22t, -160 - 39t) \mid t \in \mathbf{Z}\}$.

2. Используя свойства сравнений, определить, с каким числом r, где $0 \le r \le 5$, по модулю 6 сравнимо число $a = 1001\cdot 23^{10}\cdot 19^{13}\cdot 51^2$.

Отметим, что здесь число a не представлено в каноническом разложении, поскольку $1001 = 7\cdot 11\cdot 13$ и $51 = 3\cdot 17$.

$1001 = 6\cdot 166 + 5 \Leftrightarrow 1001 \equiv 5 \equiv -1 \pmod 6$.

По свойству 4 сравнений получаем:

$23 = 6\cdot 3 + 5 \Leftrightarrow 23 \equiv 5 \equiv -1 \pmod 6 \Rightarrow 23^{10} \equiv 1 \pmod 6$;

$19 = 6\cdot 3 + 1 \Leftrightarrow 19 \equiv 1 \pmod 6 \Rightarrow 19^{13} \equiv 1 \pmod 6$;

$51 = 6\cdot 8 + 3 \Leftrightarrow 51 \equiv 3 \pmod 6 \Rightarrow 51^2 \equiv 9 \equiv 3 \pmod 6$.

Тогда по свойству 3 сравнений $a \equiv -1\cdot 1\cdot 1\cdot 3 = -3 \equiv 3 \pmod 6$. Значит, $r = 3$.

3. Показать, что если n – нечетное целое число, то $n^2 - 1 \equiv 0 \pmod 8$.

$n = 2m + 1$, где $m \in \mathbf{Z}$, $n^2 - 1 = (2m+1)^2 - 1 = 2m(2m+2) = 4m(m+1)$. Тогда согласно утверждению, доказанному в §1.1 (см. пример 3, в), $m(m+1) \vdots 2$. Значит, $4m(m+1) \vdots 8$, что по определению 1.3.2 означает $n^2 - 1 \equiv 0 \pmod 8$.

4. Доказать, что если $3^n \equiv -1 \pmod{10}$ при некотором $n \in \mathbf{N}$, то $3^{n+4} \equiv -1 \pmod{10}$.

По свойству 3 сравнений получаем

$$3^4 = 81 \equiv 1 \pmod{10} \Rightarrow 3^{n+4} = 3^n\cdot 3^4 \equiv -1\cdot 1 = -1 \pmod{10}.$$

5. Доказать, что $2^{11\cdot 31} \equiv 2 \pmod{11\cdot 31}$.

По свойствам 3 и 4 сравнений имеем:

$2^5 = 32 \equiv -1 \pmod{11} \Rightarrow 2^{11} = (2^5)^2\cdot 2 \equiv (-1)^2\cdot 2 = 2 \pmod{11}$,

$(2^{11})^{31} \equiv 2^{31} = (2^5)^6\cdot 2 \equiv (-1)^6\cdot 2 = 2 \pmod{11}$;

$2^5 = 32 \equiv 1 \pmod{31} \Rightarrow 2^{31} = (2^5)^6\cdot 2 \equiv 1\cdot 2 = 2 \pmod{31}$,

$(2^{31})^{11} \equiv 2^{11} = 2^{10}\cdot 2 \equiv 1\cdot 2 = 2 \pmod{31}$.

Таким образом, $2^{11\cdot 31} = 2 + 11m = 2 + 31n$, где $m, n \in \mathbf{N}$, согласно определению 1.3.2. Отсюда $11m = 31n$ и $11 \mid 31n$, $31 \mid 11m$. Поскольку 11 и 31 – различные простые числа, то $\text{НОД}(11, 31) = 1$ по свойству 2 простых чисел. Значит, по свойству 2 взаимно простых чисел $11 \mid n$ и $31 \mid m$, откуда $2^{11\cdot 31} = 2 + (11\cdot 31)q$, где $q \in \mathbf{N}$. Последнее равенство по определению 1.3.2 означает, что $2^{11\cdot 31} \equiv 2 \pmod{11\cdot 31}$.

Задачи

1. Решить диофантово линейное уравнение $7x - 19y = 23$.

2. Определить число и месяц рождения человека, у которого сумма произведений даты дня рождения (x) на 12 и номера месяца (y) на 31 равна 67. При-

чем из всех решений выбирается то единственное, для которого $1 \le x \le 31$, $1 \le y \le 12$.

3. Сколько существует способов составления отрезка длиной 1 м из отрезков длинами 7 см и 12 см?

4. Проверить, что $3^{14} \equiv -1 \pmod{29}$. Указание: сравнить 3^3 с минимальным по абсолютной величине числом по модулю 29 и использовать свойства сравнений.

5. Найти остаток от деления числа $1532^5 - 1$ на 9. Указание: найти остаток от деления 1532 на 9 и использовать свойства сравнений.

6. Согласно гипотезе П. Ферма $2^{2^n} + 1$ – простое число при всех $n \in \mathbf{Z}_{\ge 0}$. Опровергнуть гипотезу, проверив, что при $n = 5$ получается число, кратное 641. Указание: сравнить 2^{10}, 2^{11} с минимальными по абсолютной величине числами по модулю 641 соответственно и использовать свойства сравнений.

Ответы

1. $\{(-184 - 19t, -69 - 7t) \mid t \in \mathbf{Z}\}$. **2.** 3 января. **3.** Единственный способ: 4 отрезка по 7 см и 6 отрезков по 12 см. **5.** 4.

§1.4. Множество классов вычетов. Функция Эйлера

При делении целых чисел на натуральное число m существует m различных остатков: 0, 1, 2,…, $m - 1$. Свойства 7–9 сравнений из §1.3 означают, что отношение сравнимости на множестве целых чисел $\mathbf{Z}$ есть отношение эквивалентности. Множество $\mathbf{Z}$ разбивается на m непересекающихся классов эквивалентности попарно сравнимых друг с другом по модулю m чисел, имеющих один и тот же остаток от деления на m. В соответствии со значениями остатков от деления целых чисел на m будем обозначать эти классы $\bar{0}, \ldots, \overline{m-1}$. Английское слово residue – «остаток» – переводится на русский язык еще и как «вычет».

Определение 1.4.1. *Классом вычетов по модулю m с представителем* $i \in \mathbf{Z}$ называется множество $\bar{i} = \{i + mq \mid q \in \mathbf{Z}\}$, состоящее из всех целых чисел, сравнимых с i по модулю m. Любой представитель класса вычетов однозначно определяет свой класс, т. е. для каждого $i + mq$ класс вычетов $\overline{i + mq} = \bar{i}$. Чаще всего представители i классов вычетов по модулю m выбираются из диапазона $0 \le i \le m - 1$. *Множеством классов вычетов по модулю m* называется множество $\mathbf{Z}/m\mathbf{Z} = \{\bar{0}, \ldots, \overline{m-1}\}$, состоящее из m всех различных классов вычетов по данному модулю.

Заметим, что для любых классов $\bar{k}$, $\bar{l} \in \mathbf{Z}/m\mathbf{Z}$ и для произвольных $k_1, k_2 \in \bar{k}$, $l_1, l_2 \in \bar{l}$ суммы $k_1 + l_1$ и $k_2 + l_2$ принадлежат одному классу из $\mathbf{Z}/m\mathbf{Z}$, а именно $\overline{k + l}$, т. к. эти суммы сравнимы друг с другом по модулю m согласно свойству 2 сравнений из §1.3. Аналогично, согласно свойству 3 сравнений из §1.3 произведения $k_1 l_1$ и $k_2 l_2$ находятся в одном классе из $\mathbf{Z}/m\mathbf{Z}$, а именно в $\overline{kl}$.

Определим операции сложения и умножения на $\mathbf{Z}/m\mathbf{Z}$. Полагаем, что сумма $\bar{k} + \bar{l} = \bar{w}$, где $\bar{w}$ – такой единственный класс из $\mathbf{Z}/m\mathbf{Z}$, в который попадают все суммы $k + l$ для $k \in \bar{k}$, $l \in \bar{l}$, а произведение $\bar{k}\,\bar{l} = \bar{z}$ – тот единственный класс из $\mathbf{Z}/m\mathbf{Z}$, в который попадают все произведения kl для $k \in \bar{k}$, $l \in \bar{l}$:

$$\bar{k} + \bar{l} = \overline{k + l} = \left\{k + l \mid k \in \bar{k},\, l \in \bar{l}\right\},\ \bar{k}\,\bar{l} = \overline{kl} = \left\{kl \mid k \in \bar{k},\, l \in \bar{l}\right\}.$$

Поскольку сложение и умножение в $\mathbf{Z}/m\mathbf{Z}$ однозначно определяются сложением и умножением представителей классов вычетов, то свойства 1–5 операций сложения и умножения в $\mathbf{Z}$ из §1.1 справедливы и в $\mathbf{Z}/m\mathbf{Z}$:

1) $\bar{k} + \left(\bar{l} + \bar{s}\right) = \left(\bar{k} + \bar{l}\right) + \bar{s},\ \bar{k}\left(\bar{l}\,\bar{s}\right) = \left(\bar{k}\,\bar{l}\right)\bar{s}$ – ассоциативность;

2) $\bar{k} + \bar{l} = \bar{l} + \bar{k},\ \bar{k}\,\bar{l} = \bar{l}\,\bar{k}$ – коммутативность;

3) существование нейтральных элементов – $\bar{0}$ относительно сложения и $\bar{1}$ относительно умножения соответственно: $\bar{k} + \bar{0} = \bar{k},\ \bar{k} \cdot \bar{1} = \bar{k}$;

4) существование для всякого $\bar{k}$ противоположного класса $-\bar{k} \in \mathbf{Z}/m\mathbf{Z}$, такого, что $\bar{k} + \left(-\bar{k}\right) = \bar{0}$, при этом $-\bar{k} = \overline{m - k}$;

5) $\left(\bar{k} + \bar{l}\right)\bar{s} = \bar{k}\,\bar{s} + \bar{l}\,\bar{s}$ – дистрибутивность умножения относительно сложения.

Свойства 1–5 выполняются для всех $\bar{k}, \bar{l}, \bar{s} \in \mathbf{Z}/m\mathbf{Z}$.

Определение 1.4.2. Элемент $\bar{k} \in \mathbf{Z}/m\mathbf{Z}$ называется *обратимым*, если найдется такой класс $\bar{k}^{-1} \in \mathbf{Z}/m\mathbf{Z}$, что $\bar{k}\,\bar{k}^{-1} = \bar{1}$. Тогда $\bar{k}^{-1}$ называют *классом вычетов, обратным* $\bar{k}$.

Так как $\bar{1} = \bar{0}$ при $m = 1$, то $\mathbf{Z}/\mathbf{Z} = \left\{\bar{0}\right\}$ и состоит из одного обратимого относительно умножения класса вычетов.

Из ассоциативности сложения и умножения вытекает единственность противоположного и обратного (в случае обратимости $\bar{k}$) класса вычетов соответственно.

Лемма 1.4.1. *Пусть* $\bar{k} \in \mathbf{Z}/m\mathbf{Z}$ *– такой класс, что* $(k, m) = 1$. *Тогда*:

1) $\bar{k}\,\bar{l} \neq \bar{0}$ *для каждого* $\bar{l} \neq \bar{0}$;

2) $\bar{k}\,\overline{l_1} \neq \bar{k}\,\overline{l_2}$, *если* $\overline{l_1} \neq \overline{l_2}$;

3) $\bar{k}$ *– обратимый класс в* $\mathbf{Z}/m\mathbf{Z}$.

Лемма 1.4.2. *Пусть* $\bar{k} \in \mathbf{Z}/m\mathbf{Z}$ *– такой класс, что* $(k, m) = d > 1$. *Тогда*:

1) *существует* $\bar{l} \neq \bar{0}$, *такой, что* $\bar{k}\,\bar{l} = \bar{0}$;

2) *существуют* $\overline{l_1} \neq \overline{l_2}$, *такие, что* $\bar{k}\,\overline{l_1} = \bar{k}\,\overline{l_2}$;

3) $\bar{k}\,\bar{l} \neq \bar{1}$ *для всех* $\bar{l} \neq \bar{0}$, *т. е. класс* $\bar{k}$ *необратим в* $\mathbf{Z}/m\mathbf{Z}$.

Из лемм 1.4.1 и 1.4.2 вытекает следующая важная теорема.

Теорема 1.4.1. *Класс* $\bar{k} \in \mathbf{Z}/m\mathbf{Z}$ *обратим тогда и только тогда, когда* $(k, m) = 1$. *Произведение обратимых классов есть обратимый класс*.

Следствие. *Если* p *– простое число, то в* $\mathbf{Z}/p\mathbf{Z}$ *каждый ненулевой класс вычетов обратим*.

Поскольку $\mathbf{Z}/m\mathbf{Z}$ – конечное множество, то сложение и умножение на нем можно задавать поэлементно в виде *таблиц Кэли*. На пересечении i-й строки и j-го столбца такой таблицы записывается $\overline{x_i} * \overline{x_j}$ (где $*$ – знак операции).

Определение 1.4.3. *Функция Эйлера* (или *тотиент-функция*) φ ставит в соответствие каждому натуральному $m > 1$ количество натуральных чисел, меньших m и взаимно простых с m.

Теорема 1.4.2 (о вычислении значений функции Эйлера):

1. $\varphi(p) = p - 1$ *для каждого простого числа* p.

2. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\forall\ \alpha \in \mathbf{N}$.

3. *Если* $(m, n) = 1$, *то* $\varphi(mn) = \varphi(m)\varphi(n)$.

4. *Если* $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ *– каноническое разложение числа* m, *то*

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \dots \left(p_t^{\alpha_t} - p_t^{\alpha_t - 1}\right) = m(1 - 1/p_1) \dots (1 - 1/p_t).$$

Из теоремы 1.4.1 следует, что при $m \in \mathbf{N}_{>1}$ в $\mathbf{Z}/m\mathbf{Z}$ имеется в точности $\varphi(m)$ обратимых классов вычетов.

Теорема 1.4.3 (Л. Эйлер). *Для любых* $m \in \mathbf{N}_{>1}$ *и* $a \in \mathbf{Z}$ *справедливо утверждение*: $(a, m) = 1$ *тогда и только тогда, когда* $a^{\varphi(m)} \equiv 1 \pmod m$.

Следствие. *В* $\mathbf{Z}/m\mathbf{Z}$ *при* $m \in \mathbf{N}_{>1}$ *всякий обратимый относительно умножения элемент* $\overline{k}$ *обладает свойствами*:

1) $\overline{k}^{\varphi(m)} = \overline{1}$;

2) *обратным классу вычетов* $\overline{k}$ *является класс вычетов* $\overline{k^{\varphi(m)-1}}$.

Теорема 1.4.4 (малая теорема Ферма). *Пусть* p *– простое число. Число* $a \in \mathbf{Z}$ *не делится на* p *тогда и только тогда, когда* $a^{p-1} \equiv 1 \pmod p$.

Следствие. *В* $\mathbf{Z}/p\mathbf{Z}$ *при простом* p *обратным классу вычетов* $\overline{k} \neq \overline{0}$ *является класс вычетов* $\overline{k^{p-2}}$.

Решение линейных сравнений в целых числах

Рассмотрим сравнение вида

$$ax \equiv b \pmod m, \qquad (1.4.1)$$

где $a, b \in \mathbf{Z}$, $a \neq 0$, $m \in \mathbf{N}$, x – искомое значение в $\mathbf{Z}$.

1. Пусть $(a, m) = 1$. Тогда сравнение (1.4.1) имеет в качестве множества решений $\overline{x}$ – единственный класс вычетов по модулю m. По теореме 1.4.1 $\overline{a}$ – обратимый класс в $\mathbf{Z}/m\mathbf{Z}$ и $\overline{a}^{-1}$ – единственный обратный $\overline{a}$ класс. В $\mathbf{Z}/m\mathbf{Z}$ сравнение (1.4.1) соответствует уравнению $\overline{a}\,\overline{x} = \overline{b}$. Умножив обе его части на $\overline{a}^{-1}$, получим $\overline{x} = \overline{a}^{-1}\overline{b}$. Тогда $\overline{x} = \{x_0 + mq \mid q \in \mathbf{Z}\}$ – множество решений сравнения (1.4.1). Представитель класса вычетов $\overline{a}^{-1}$ может быть найден как коэффициент при a в соотношении Безу для 1 и чисел a и m, или $\overline{a}^{-1} = \overline{a^{\varphi(m)-1}}$ согласно следствию из теоремы 1.4.3.

2. Пусть $(a, m) = d > 1$ и $d \nmid b$, тогда (1.4.1) не имеет решений в $\mathbf{Z}$, поскольку не выполняется свойство 6 делимости целых чисел из §1.1.

3. Пусть $(a, m) = d > 1$ и $d \mid b$. Тогда разделим обе части (1.4.1) и m на d согласно свойству 5 сравнений из §1.3. Получим сравнение

$$a_1 x \equiv b_1 \pmod{m_1}, \qquad (1.4.2)$$

где $a_1 = a/d$, $b_1 = b/d$, $m_1 = m/d$, и $(a_1, m_1) = 1$ по свойству 1 взаимно простых чисел.

Сравнение (1.4.2) имеет в качестве множества решений единственный класс вычетов $\bar{x}$ по модулю m_1 согласно случаю 1. Числа из $\bar{x} = \{x_0 + m_1 q \mid q \in \mathbf{Z}\}$, и только они, являются решениями (1.4.1). Все множество решений (1.4.1) – это объединение d классов вычетов по модулю m, на которые разбивается класс вычетов $\bar{x}$ по модулю m_1: $\overline{x_0}$, $\overline{x_0 + m_1}$,…, $\overline{x_0 + (d-1)m_1}$.

Примеры

1. Построить таблицы Кэли сложения и умножения в $\mathbf{Z}/m\mathbf{Z}$. Для всех классов вычетов найти противоположные относительно сложения и обратные относительно умножения классы вычетов, если последние существуют. Проверить обратимость классов вычетов по теореме 1.4.1:

а) $m = 7$.

Противоположные и обратные элементы находим по таблицам Кэли сложения и умножения классов вычетов (рис. 1.4.1, а, б соответственно). Формула для противоположных элементов: $-\bar{i} = \overline{7 - i}$, $0 \le i \le 6$. Все ненулевые классы вычетов, и только они, обратимы согласно теореме 1.4.1 и следствию из нее, поскольку 7 – простое число. Обратные относительно умножения классы вычетов:

$$\bar{1}^{-1} = \bar{1},\ \bar{2}^{-1} = \bar{4},\ \bar{3}^{-1} = \bar{5},\ \bar{4}^{-1} = \bar{2},\ \bar{5}^{-1} = \bar{3},\ \bar{6}^{-1} = \bar{6}.$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

а

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

б

Рис. 1.4.1

Вид столбцов и строк таблицы умножения на рис. 1.4.1, б соответствует выполнению леммы 1.4.1 для всех ненулевых классов вычетов и леммы 1.4.2 для нулевого класса вычетов.

б) $m = 9$.

Противоположные и обратные элементы находим по таблицам Кэли сложения и умножения классов вычетов (рис. 1.4.2, а, б соответственно). Формула для противоположных элементов: $-\bar{i} = \overline{9 - i}$, $0 \le i \le 8$. Здесь 9 – составное число. Обратимыми являются те и только те классы вычетов, представители которых

взаимно просты с 9: 1, 2, 4, 5, 7, 8, что согласуется с теоремой 1.4.1. Обратные относительно умножения классы вычетов:

$$\bar{1}^{-1} = \bar{1},\ \bar{2}^{-1} = \bar{5},\ \bar{4}^{-1} = \bar{7},\ \bar{5}^{-1} = \bar{2},\ \bar{7}^{-1} = \bar{4},\ \bar{8}^{-1} = \bar{8}.$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$

а

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{3}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{6}$	$\bar{2}$	$\bar{7}$	$\bar{3}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

б

Рис. 1.4.2

Вид столбцов и строк таблицы умножения на рис. 1.4.2, б соответствует выполнению леммы 1.4.1 для классов вычетов с представителями 1, 2, 4, 5, 7, 8 и леммы 1.4.2 для классов вычетов с представителями 0, 3, 6.

2. В $\mathbf{Z}/236\mathbf{Z}$ для классов вычетов $\overline{71}$, $\overline{100}$, $\overline{185}$ найти обратные относительно умножения классы вычетов или доказать, что их не существует.

$236 = 2^2 \cdot 59$, 71 – простое число, $100 = 2^2 \cdot 5^2$, $185 = 5 \cdot 37$.

Поскольку (71, 236) = 1, то $\overline{71}$ – обратимый класс в $\mathbf{Z}/236\mathbf{Z}$.

Найдем представитель обратного $\overline{71}$ класса из соотношения Безу для чисел 1, 71 и 236, вычислив коэффициенты по расширенному алгоритму Евклида:

$$r_{-1} = 236,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 71,\ u_0 = 1,\ v_0 = 0;$$

$$q_1 = 3,\ u_1 = u_{-1} - u_0 q_1 = -3,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 23 = 71 \cdot (-3) + 236;$$

$$q_2 = 3,\ u_2 = u_0 - u_1 q_2 = 10,\ v_2 = v_0 - v_1 q_2 = -3 \Rightarrow r_2 = 2 = 71 \cdot 10 + 236 \cdot (-3);$$

$$q_3 = 11,\ u_3 = u_1 - u_2 q_3 = -113,\ v_3 = v_1 - v_2 q_3 = 34 \Rightarrow r_3 = 1 = 71 \cdot (-113) + 236 \cdot 34.$$

Тогда $71 \cdot (-113) \equiv 1 \pmod{236}$ и $\overline{71}^{-1} = \overline{-113} = \overline{236 - 113} = \overline{123}$.

Поскольку (100, 236) = 4 > 1, то $\overline{100}$ – необратимый класс в $\mathbf{Z}/236\mathbf{Z}$.

Поскольку (185, 236) = 1, то $\overline{185}$ – обратимый класс в $\mathbf{Z}/236\mathbf{Z}$.

Найдем представитель обратного $\overline{185}$ класса из соотношения Безу для 1, 185 и 236, вычислив коэффициенты по расширенному алгоритму Евклида:

$$r_{-1} = 236,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 185,\ u_0 = 1,\ v_0 = 0;$$

$$q_1 = 1,\ u_1 = u_{-1} - u_0 q_1 = -1,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 51 = 185 \cdot (-1) + 236;$$

$$q_2 = 3,\ u_2 = u_0 - u_1 q_2 = 4,\ v_2 = v_0 - v_1 q_2 = -3 \Rightarrow r_2 = 32 = 185 \cdot 4 + 236 \cdot (-3);$$

$$q_3 = 1,\ u_3 = u_1 - u_2 q_3 = -5,\ v_3 = v_1 - v_2 q_3 = 4 \Rightarrow r_3 = 19 = 185 \cdot (-5) + 236 \cdot 4;$$

$$q_4 = 1,\ u_4 = u_2 - u_3 q_4 = 9,\ v_4 = v_2 - v_3 q_4 = -7 \Rightarrow r_4 = 13 = 185 \cdot 9 + 236 \cdot (-7);$$

$q_5 = 1$, $u_5 = u_3 - u_4 q_5 = -14$, $v_5 = v_3 - v_4 q_5 = 11 \Rightarrow r_5 = 6 = 185 \cdot (-14) + 236 \cdot 11$;
$q_6 = 2$, $u_6 = u_4 - u_5 q_6 = 37$, $v_6 = v_4 - v_5 q_6 = -29 \Rightarrow r_6 = 1 = 185 \cdot 37 + 236 \cdot (-29)$.

Тогда $185 \cdot 37 \equiv 1 \pmod{236}$ и $\overline{\overline{185}}^{-1} = \overline{37}$.

3. Найти значение функции Эйлера $\varphi(m)$:

а) $m = 480$.

$480 = 2^5 \cdot 3 \cdot 5$ – каноническое разложение. Согласно теореме 1.4.2 получаем

$$\varphi(480) = (2^5 - 2^4) \cdot (3-1) \cdot (5-1) = 16 \cdot 2 \cdot 4 = 128;$$

б) $m = 697$.

$697 = 17 \cdot 41$ – каноническое разложение. Согласно теореме 1.4.2 получаем

$$\varphi(697) = (17-1) \cdot (41-1) = 16 \cdot 40 = 640.$$

4. Исследовать вид формулы бинома Ньютона $(\bar{a} + \bar{b})^n$ в $\mathbf{Z}/p\mathbf{Z}$, где $n \in \mathbf{N}$, p – простое число. Получить формулы в $\mathbf{Z}/11\mathbf{Z}$ для заданных ниже значений степени n.

При $\bar{a} + \bar{b} \neq \bar{0}$ имеем $(a + b, p) = 1$, поэтому $(\bar{a} + \bar{b})^{p-1} = \bar{1}$ согласно малой теореме Ферма (теорема 1.4.4). Тогда, используя теорему 1.1.1 о делении с остатком, для любых $\bar{a}$, $\bar{b} \in \mathbf{Z}/p\mathbf{Z}$ с условием $\bar{a} + \bar{b} \neq \bar{0}$ получим

$$(\bar{a} + \bar{b})^n = (\bar{a} + \bar{b})^{(p-1)q+r} = (\bar{a} + \bar{b})^r = \sum_{k=0}^{r} C_r^k \bar{a}^{r-k} \bar{b}^k,$$

где $q \in \mathbf{Z}_{\geq 0}$, $r \in \mathbf{N}_{<p-1}$, $C_r^k = \dfrac{r!}{k!(r-k)!}$ – число сочетаний из r элементов по k, биномиальный коэффициент. Очевидно, что $\bar{0}^n = \bar{0}^r = \bar{0}$ при $r \in \mathbf{N}_{<p-1}$, поэтому формула остается справедливой при $\bar{a} + \bar{b} = \bar{0}$. Для преобразования формулы биномиальные коэффициенты приводятся по модулю p (т. е. находятся их остатки от деления на p), поскольку $\lambda p \bar{c} = \bar{0}$ для любых $\lambda \in \mathbf{Z}$ и $\bar{c} \in \mathbf{Z}/p\mathbf{Z}$.

В случае $r = 0$ имеем $(\bar{a} + \bar{b})^n = \bar{1}$ при $\bar{a} + \bar{b} \neq \bar{0}$ и $(\bar{a} + \bar{b})^n = \bar{0}$ при $\bar{a} + \bar{b} = \bar{0}$.

а) $n = 28$.

$$(\bar{a} + \bar{b})^{28} = (\bar{a} + \bar{b})^{10 \cdot 2 + 8} = (\bar{a} + \bar{b})^8 = \bar{a}^8 + 8\bar{a}^7\bar{b} + (8 \cdot 7/2)\bar{a}^6\bar{b}^2 + (8 \cdot 7 \cdot 6/(2 \cdot 3))\bar{a}^5\bar{b}^3 +$$
$$+ (8 \cdot 7 \cdot 6 \cdot 5/(2 \cdot 3 \cdot 4))\bar{a}^4\bar{b}^4 + (8 \cdot 7 \cdot 6/(2 \cdot 3))\bar{a}^3\bar{b}^5 + (8 \cdot 7/2)\bar{a}^2\bar{b}^6 + 8\bar{a}\bar{b}^7 + \bar{b}^8 = \bar{a}^8 +$$
$$+ 8\bar{a}^7\bar{b} + 6\bar{a}^6\bar{b}^2 + \bar{a}^5\bar{b}^3 + 4\bar{a}^4\bar{b}^4 + \bar{a}^3\bar{b}^5 + 6\bar{a}^2\bar{b}^6 + 8\bar{a}\bar{b}^7 + \bar{b}^8;$$

б) $n = 44$.

$$(\bar{a} + \bar{b})^{44} = (\bar{a} + \bar{b})^{10 \cdot 4 + 4} = (\bar{a} + \bar{b})^4 = \bar{a}^4 + 4\bar{a}^3\bar{b} + 6\bar{a}^2\bar{b}^2 + 4\bar{a}\bar{b}^3 + \bar{b}^4;$$

в) $n = 75$.

$$(\bar{a} + \bar{b})^{75} = (\bar{a} + \bar{b})^{10 \cdot 7 + 5} = (\bar{a} + \bar{b})^5 = \bar{a}^5 + 5\bar{a}^4\bar{b} + 10\bar{a}^3\bar{b}^2 + 10\bar{a}^2\bar{b}^3 + 5\bar{a}\bar{b}^4 + \bar{b}^5.$$

5. Решить в целых числах линейное сравнение

$$114x \equiv 42 \pmod{87}. \qquad (1.4.3)$$

Поскольку $87 = 3 \cdot 29$, $114 = 2 \cdot 3 \cdot 19$, $42 = 2 \cdot 3 \cdot 7$, то $(87, 114, 42) = 3$, значит, сравнение (1.4.3) имеет решения в целых числах.

Разделим обе части сравнения (1.4.3) и модуль на 3. Получим сравнение

$$38x \equiv 14 \pmod{29}. \qquad (1.4.4)$$

Поскольку $(38, 14) = 2$, то согласно свойству 6 сравнений, разделив обе части (1.4.4) на 2, получим следующее сравнение:

$$19x \equiv 7 \pmod{29}. \qquad (1.4.5)$$

Множества решений сравнений (1.4.4) и (1.4.5) в целых числах совпадают и соответствуют классу вычетов $\bar{x} = \overline{19}^{-1} \cdot \bar{7}$ в $\mathbf{Z}/29\mathbf{Z}$. Найдем вначале $\overline{19}^{-1}$ с использованием следствия из теоремы 1.4.4, поскольку 29 – простое число. Используя свойства сравнений и малую теорему Ферма, получаем

$$19^{27} \equiv (-10)^{27} = -2^{27} \cdot 5^{27} = -2^{27} \cdot (5^2)^{13} \cdot 5 \equiv -2^{27} \cdot (-4)^{13} \cdot 5 = 2^{53} \cdot 5 \equiv 2^{25} \cdot 5 =$$
$$= (2^5)^5 \cdot 5 \equiv 3^5 \cdot 5 = 27 \cdot 9 \cdot 5 \equiv -2 \cdot 9 \cdot 5 = -90 \equiv -3 \pmod{29}.$$

Значит, $\overline{19}^{-1} = \overline{-3}$ в $\mathbf{Z}/29\mathbf{Z}$. Тогда $x_0 \equiv -3 \cdot 7 = -21 \equiv 8 \pmod{29}$. Таким образом, $\bar{x} = \bar{8} = \{8 + 29q \mid q \in \mathbf{Z}\}$ – множество всех решений сравнения (1.4.5), а значит, и сравнения (1.4.4). Класс вычетов $\bar{x}$ является множеством всех решений исходного сравнения (1.4.3); $\bar{x}$ можно представить в виде объединения трех классов вычетов в $\mathbf{Z}/87\mathbf{Z}$: $\bar{8} = \{8 + 87q \mid q \in \mathbf{Z}\}$, $\overline{37} = \{37 + 87q \mid q \in \mathbf{Z}\}$, $\overline{66} = \{66 + 87q \mid q \in \mathbf{Z}\}$.

Задачи

1. Построить таблицы Кэли сложения и умножения в $\mathbf{Z}/12\mathbf{Z}$. Для всех классов вычетов найти противоположные относительно сложения и обратные относительно умножения классы вычетов, если последние существуют. Проверить обратимость классов вычетов по теореме 1.4.1.

2. В $\mathbf{Z}/318\mathbf{Z}$ для классов вычетов $\overline{59}$, $\overline{126}$, $\overline{273}$ найти обратные относительно умножения классы вычетов или доказать, что их не существует.

3. Получить формулы бинома Ньютона $(\bar{a} + \bar{b})^n$ в $\mathbf{Z}/17\mathbf{Z}$ для следующих значений степени n:

а) 38; **б)** 51; **в)** 100.

4. Решить в целых числах линейное сравнение $256x \equiv 179 \pmod{337}$.

Ответы

1. $-\bar{i} = \overline{12 - i}$, $0 \le i \le 11$; $\bar{1}^{-1} = \bar{1}$, $\bar{5}^{-1} = \bar{5}$, $\bar{7}^{-1} = \bar{7}$, $\overline{11}^{-1} = \overline{11}$, остальные классы вычетов необратимы. **2.** $\overline{59}^{-1} = \overline{221}$, $\overline{126}$ и $\overline{273}$ необратимы. **3. а)** $(\bar{a} + \bar{b})^6 = \bar{a}^6 + 6\bar{a}^5\bar{b} + 15\bar{a}^4\bar{b}^2 + 3\bar{a}^3\bar{b}^3 + 15\bar{a}^2\bar{b}^4 + 6\bar{a}\bar{b}^5 + \bar{b}^6$; **б)** $(\bar{a} + \bar{b})^3 = \bar{a}^3 + 3\bar{a}^2\bar{b} + 3\bar{a}\bar{b}^2 + \bar{b}^3$; **в)** $(\bar{a} + \bar{b})^4 = \bar{a}^4 + 4\bar{a}^3\bar{b} + 6\bar{a}^2\bar{b}^2 + 4\bar{a}\bar{b}^3 + \bar{b}^4$. **4.** $\overline{81} = \{81 + 337q \mid q \in \mathbf{Z}\}$.

Глава 2. Отображения и их свойства

§2.1. Соответствия, отображения, функции

Определение 2.1.1. Пусть X и Y – два непустых множества. Если определен способ сопоставления элементов Y элементам X, то говорят, что между множествами X и Y установлено *соответствие*. Если обозначить соответствие буквой q, то запись $q: X \to Y$ обозначает существование данного соответствия между множествами X и Y. При этом совершенно необязательно, чтобы в сопоставлении участвовали все элементы множеств X и Y. Для того чтобы задать соответствие между множествами X и Y, нужно задать множество $Q \subseteq X \times Y = \{ (x, y) \mid x \in X, y \in Y \}$, определяющее закон, по которому осуществляется соответствие, т. е. перечисляющий все пары (x, y), участвующие в сопоставлении.

Таким образом, соответствие, обозначаемое q, представляет собой тройку множеств:

$$q = (X, Y, Q),$$

в которой $Q \subseteq X \times Y$. В этом выражении первую компоненту X называют *областью отправления соответствия*, вторую компоненту Y – *областью прибытия соответствия*, третью компоненту Q – *графиком соответствия*.

Кроме рассмотренных множеств X, Y и Q с каждым соответствием q неразрывно связаны еще два множества: множество $D(q) = \{ x \in X \mid (x, y) \in Q \}$, называемое *областью определения соответствия*, которое состоит из всех элементов множества X, участвующих в сопоставлении, и множество $E(q) = \{ y \in Y \mid (x, y) \in Q \}$, называемое *областью значений соответствия*, которое состоит из всех элементов множества Y, участвующих в сопоставлении. Если $(x, y) \in Q$, то говорят, что *элемент y соответствует элементу x*. Геометрически этот факт удобно изображать стрелкой, направленной от x к y.

Множество всех $y \in E(q)$, соответствующих фиксированному элементу $x \in D(q)$, называется *образом x* в Y при соответствии q и обозначается $q(x)$. Множество всех $x \in D(q)$, которым соответствует фиксированный элемент $y \in E(q)$, называется *прообразом y* в X при соответствии q и обозначается $q^{-1}(y)$. Если $A \subseteq D(q)$, то *образом $q(A)$ множества A* называется объединение образов всех элементов из A. Аналогично определяется *прообраз $q^{-1}(B)$ множества B* для любого $B \subseteq E(q)$ как объединение прообразов всех элементов из B.

Определение 2.1.2. Если $D(q) = X$, то соответствие q называется *всюду определенным* (или *отображением X* в Y), в противном случае соответствие называется *частичным*. Если $E(q) = Y$, то соответствие q называется *сюръективным* (*сюръекцией*) на Y. Соответствие q называется *инъективным* (*инъекцией*), если любые различные x_1 и x_2 из $D(q)$ имеют различные образы и любые различные y_1 и y_2 из $E(q)$ имеют различные прообразы при соответствии q.

Два отображения p и q называются *равными* (обозначение $p = q$), если их области определения – одно и то же множество X, и для любого $x \in X$ выполняется $p(x) = q(x)$.

Отображение, для которого область определения и область прибытия являются одним и тем же множеством X, часто называют *преобразованием множества X*.

Определение 2.1.3. Соответствие q называется *функциональным* (или *однозначным*), если образом любого элемента $x \in D(q)$ является единственный элемент $y \in E(q)$, что обычно записывается как $q: x \mapsto y$ или $q(x) = y$. Соответствие q между множествами X и Y называется *взаимно однозначным* (или *биективным*, также *биекцией*, иногда *1-1 соответствием*), если оно всюду определено, сюръективно и инъективно. Однозначное отображение называется *функцией*. Функция называется *инъективной*, если различным x_1 и x_2 из X соответствуют различные y_1 и y_2 из Y, и *сюръективной*, если она сюръективна как соответствие. Функция называется *биективной*, если она одновременно инъективна и сюръективна.

Определение 2.1.4. Пусть $f: X \to Y$ – функция. Каждому элементу $x \in X$ функция f ставит в соответствие единственный элемент $y \in Y$, такой, что $f(x) = y$. При этом элемент x называется *аргументом функции*, y – *значением функции* на x. Если $E(f)$ состоит из единственного элемента, то f называется *функцией-константой*. *Тождественной функцией* на множестве X называется функция $e_X: X \to X$, такая, что $e_X(x) = x$ для любого $x \in X$. Если $X, Y \subseteq \mathbf{R}$, то функцию f называют *вещественной* (или *числовой*).

Определение 2.1.5. Если f – вещественная функция, то упорядоченные пары $(x, f(x))$ можно изобразить в виде точек на плоскости $\mathbf{R}^2$. Полная совокупность таких точек будет представлять собой *график функции f*.

Определение 2.1.6. Для каждого соответствия $q = (X, Y, Q)$ с $Q \subseteq X \times Y$ существует *обратное соответствие*, которое получится, если данное соответствие q рассматривать в обратном направлении, т. е. определять элементы $x \in X$, с которыми сопоставляются элементы $y \in Y$. Соответствие, обратное соответствию q, будем обозначать

$$q^{-1} = (Y, X, Q^{-1}),$$

где $Q^{-1} \subseteq Y \times X$.

Геометрическое представление обратного соответствия получается путем изменения направления стрелок в геометрическом представлении прямого соответствия. Отсюда следует, что обратным соответствием для обратного соответствия будет прямое соответствие:

$$(q^{-1})^{-1} = q.$$

В дальнейшем будем рассматривать только функциональные соответствия, которые также иногда для краткости будем называть функциями.

Перечислим основные способы задания функций:

1. Наиболее простой способ задания функций – это *табличный*. Таблицы при этом представляют собой конечные списки пар $(x, f(x))$. Однако таким способом могут быть заданы только функции, определенные на конечных множествах.

2. Другим не менее известным способом задания функций является *аналитический*, или *формула*, описывающая функцию с помощью суперпозиции других (исходных) функций. Если способ вычисления исходных функций известен, то формула задает процедуру вычисления данной функции как некоторую последовательность вычислений исходных функций.

Иногда для разных подмножеств множества X при задании функции приходится пользоваться различными формулами. Пусть $A_i \subset X$, где $1 \le i \le n$, $X = A_1 \cup \ldots \cup A_n$, $A_i \cap A_j = \varnothing$ при $i \ne j$. Обозначим через $f_i(x)$ формулу, определяющую y при $x \in A_i$, где $1 \le i \le n$. Тогда функция f, определенная на всем множестве X, задается так:

$$f(x) = \begin{cases} f_1(x) \text{ при } x \in A_1; \\ f_2(x) \text{ при } x \in A_2; \\ \quad \ldots \\ f_n(x) \text{ при } x \in A_n. \end{cases}$$

3. Если f – вещественная функция, то она может быть задана графически на плоскости $\mathbf{R}^2$, как сказано ранее в определении 2.1.5.

4. Вычисления функций по таблицам, формулам, а также с помощью графиков являются частными видами вычислительных процедур. Существуют вычислительные процедуры, не относящиеся к указанным трем видам. Среди них особенно следует выделить рекурсивные процедуры. *Рекурсивная процедура* задает функцию f, определенную на множестве $\mathbf{N}$ (или $\mathbf{Z}_{\ge 0}$), следующим образом: 1) задается значение $f(1)$ (или $f(0)$); 2) значение $f(n+1)$ определяется через суперпозицию $f(n)$ и других функций, считающихся известными. Простейшим примером рекурсивной процедуры является вычисление функции $n!$: 1) $0! = 1$; 2) $(n+1)! = n!(n+1)$. Для вычисления $(n+1)!$ при $n \in \mathbf{N}$ требуется $n-1$ умножений, т. е. число вычислительных шагов увеличивается с ростом аргумента.

Определение 2.1.7. Пусть даны две функции $f: X \to Y_1$ и $g: Y_2 \to Z$, $Y_1 \subseteq Y_2$. Функция $h: X \to Z$ называется *композицией функций* f и g (обозначение $h = g \circ f$ или $h = gf$), если h – последовательное применение функций f и g: $h(x) = g(f(x))$ для любого $x \in X$. Часто говорят, что функция h получена *подстановкой* f в g:

$$gf: x \mapsto z,\ z = gf(x) = g(f(x)),$$

$$gf: x \xrightarrow{f} y \xrightarrow{g} z.$$

Аналогично по индукции определяется композиция n функций для любого натурального числа $n \ge 2$.

Для обратной функции удобно использовать еще одно определение.

Определение 2.1.8. Пусть дана функция $f: X \to Y$. Функция $f^{-1}: Y \to X$ называется *обратной* для функции f, если $f^{-1}f = e_X$, а $ff^{-1} = e_Y$, где e_X и e_Y – тождественные функции на множествах X и Y соответственно.

Из определения обратной функции следует ее единственность, и уравнение $f(x) = y$ при каждом фиксированном $y \in Y$ имеет единственное решение $x \in X$.

При аналитическом задании функции f принято аргумент как прямой, так и обратной функции обозначать одной и той же буквой, например x. Поэтому для нахождения обратной функции следует уравнение $f(x) = y$ разрешить (если это возможно) относительно x и поменять обозначения, заменив x на y и y на x. При этом формула для обратной функции запишется в виде $y = f^{-1}(x)$.

Теорема 2.1.1 (критерий существования обратной функции). *Для функции $f: X \to Y$ существует обратная функция тогда и только тогда, когда f – биекция.*

Определение 2.1.9. Пусть $f: X \to Y$ – произвольная функция, $A \subset X$ – произвольное непустое собственное подмножество X. *Сужением функции f на множество A* называют функцию $f_A: A \to Y$, такую, что $f_A(x) = f(x)$, $\forall\, x \in A$. График Q_{f_A} состоит из тех и только тех пар (x, y) графика Q_f функции f, в которых $x \in A$, а значит, $(x, y) \in A \times Y$. Таким образом, $Q_{f_A} = Q_f \cap A \times Y$.

Может так случиться, что сама функция, заданная на множестве X, не имеет обратной, но сужение этой функции на некоторое подмножество множества X, на котором она инъективна, уже имеет обратную функцию, определенную на области значений исходной функции.

Свойства функций и их композиций:

1. Композиция сюръективных функций сюръективна.

2. Композиция инъективных функций инъективна.

3. Композиция биективных функций биективна.

4. Композиция функций в общем случае некоммутативна.

5. Композиция функций ассоциативна.

6. Относительно операции композиции функций, являющихся преобразованиями одного множества X, имеется нейтральный элемент – функция e_X.

7. Функция, обратная биекции, сама является биекцией.

Теорема 2.1.2. *Пусть A – конечное множество. Функция $f: A \to A$ – сюръекция тогда и только тогда, когда f – инъекция.*

Примеры

1. Перечислить в виде подмножеств $X \times Y$ графики всех соответствий между множествами $X = \{1, 2\}$ и $Y = \{3, 5\}$. Какие из соответствий являются отображениями, сюръективными, инъективными, функциональными? Какие из отображений являются функциями? Указать все инъективные, сюръективные и биективные функции.

$X \times Y = \{(1, 3), (1, 5), (2, 3), (2, 5)\}$. Это множество дает возможность получить $2^4 = 16$ различных соответствий. Графики соответствий: $Q_0 = \{(\,)\} = \varnothing$, $Q_1 = \{(1, 3)\}$, $Q_2 = \{(1, 5)\}$, $Q_3 = \{(2, 3)\}$, $Q_4 = \{(2, 5)\}$, $Q_5 = \{(1, 3), (1, 5)\}$, $Q_6 = \{(1, 3), (2, 3)\}$, $Q_7 = \{(1, 3), (2, 5)\}$, $Q_8 = \{(1, 5), (2, 3)\}$, $Q_9 = \{(1, 5), (2, 5)\}$, $Q_{10} = \{(2, 3), (2, 5)\}$, $Q_{11} = \{(1, 3), (1, 5), (2, 3)\}$, $Q_{12} = \{(1, 3), (1, 5), (2, 5)\}$, $Q_{13} = \{(1, 3), (2, 3), (2, 5)\}$, $Q_{14} = \{(1, 5), (2, 3), (2, 5)\}$, $Q_{15} = \{(1, 3), (1, 5), (2, 3), (2, 5)\} = X \times Y$. Соответствие с графиком Q_i обозначим q_i, где $0 \le i \le 15$.

Отображениями являются соответствия q_6–q_9, q_{11}–q_{15}, поскольку $D(q_i) = X$ при $6 \le i \le 9$ и $11 \le i \le 15$. Сюръективными соответствиями являются q_5, q_7, q_8,

$q_{10}-q_{15}$, т. к. $E(q_i) = Y$ при $i = 5,\ 7,\ 8$ и $10 \le i \le 15$. Инъективные соответствия согласно определению 2.1.2: $q_1-q_4,\ q_7,\ q_8$. Функциональными соответствиями являются $q_1-q_4,\ q_6-q_9$, поскольку только они однозначны. Функциями являются q_6-q_9, поскольку только они являются функциональными отображениями. Инъективными, сюръективными и биективными функциями согласно определению 2.1.3 являются q_7 и q_8.

2. Представить вещественную функцию $f(x) = \left(1 + (x/(1-x))^2\right)^{1/2}$ в виде композиции элементарных функций, указав области определения и значений всех элементарных функций и их последовательных композиций.

$f_1(x) = x/(1-x),\ D(f_1) = \mathbf{R}\backslash\{1\},\ E(f_1) = \mathbf{R}\backslash\{-1\}$, т. к. уравнение $x/(1-x) = y$ разрешимо относительно x и $x = y/(1+y)$ для любого $y \in \mathbf{R}\backslash\{-1\}$.

$$f_2(x) = x^2,\ D(f_2) = \mathbf{R},\ E(f_1) \subset D(f_2),\ E(f_2) = \mathbf{R}_{\ge 0},\ E(f_2 f_1) = \mathbf{R}_{\ge 0}.$$

$$f_3(x) = 1 + x,\ D(f_3) = \mathbf{R},\ E(f_2 f_1) \subset D(f_3),\ E(f_3) = \mathbf{R},\ E(f_3 f_2 f_1) = \mathbf{R}_{\ge 1}.$$

$$f_4(x) = x^{1/2},\ D(f_4) = \mathbf{R}_{\ge 0},\ E(f_3 f_2 f_1) \subset D(f_4),\ E(f_4) = \mathbf{R}_{\ge 0},\ E(f_4 f_3 f_2 f_1) = \mathbf{R}_{\ge 1}.$$

$$f(x) = f_4\big(f_3(f_2(f_1(x)))\big) = f_4 f_3 f_2 f_1(x),\ D(f) = D(f_1) = \mathbf{R}\backslash\{1\},\ E(f) = \mathbf{R}_{\ge 1}.$$

3. Даны вещественные функции $f(x) = \sin x$ и $g(x) = \sqrt{x^2 - 5x + 9}$. Доказать, что композиция функций f и g некоммутативна.

$D(f) = \mathbf{R}$. Поскольку дискриминант $D = 25 - 36 = -11 < 0$, то $x^2 - 5x + 9 > 0$ при всех $x \in \mathbf{R}$ и функция g всюду на $\mathbf{R}$ определена. Значит, $D(g) = \mathbf{R}$ также. Построим композиции функций gf и fg. Очевидно, что $D(gf) = D(fg) = \mathbf{R}$. Тогда

$gf(x) = \sqrt{\sin^2 x - 5\sin x + 9}$, при $x = 0$ имеем $gf(0) = 3$;

$fg(x) = \sin\sqrt{x^2 - 5x + 9}$, при $x = 0$ имеем $fg(0) = \sin 3 \ne 3$, т. к. $E(f) = [-1;\ 1]$.

Итак, $gf \ne fg$.

4. Заданы три вещественные функции: $f(x) = 2x - 3,\ g(x) = x^3 - 8,\ h(x) = 2^{x^2+16x}$. Требуется:

1) указать области определения функций f, g, h и найти формулы композиций $fgh(x)$, $hfg(x)$, $ffg(x)$, указав их области определения;

2) исследовать функции f, g, h на инъективность в области определения, сюръективность на $\mathbf{R}$, биективность на $\mathbf{R}$;

3) найти обратные функции для f, g, h или обратные функции для их инъективных сужений на подмножества $D(f)$, $D(g)$, $D(h)$ соответственно. Найти области определения и области значений обратных функций.

Решение:

1) $D(f) = D(g) = D(h) = \mathbf{R}$, поэтому все три указанные композиции функций могут быть построены и определены на $\mathbf{R}$:

$$fgh(x) = 2\big(gh(x)\big) - 3 = 2\left(\left(2^{x^2+16x}\right)^3 - 8\right) - 3 = 2^{3x^2+48x+1} - 19;$$

$$hfg(x) = 2^{(fg(x))^2 + 16\,fg(x)} = 2^{\left(2x^3-19\right)^2 + 16\left(2x^3-19\right)} = 2^{4x^6 - 44x^3 + 57};$$

$$ffg(x) = 2\big(fg(x)\big) - 3 = 2\left(2x^3 - 19\right) - 3 = 4x^3 - 41.$$

2) Пусть $x_1, x_2 \in \mathbf{R}$, $x_1 \ne x_2$, тогда $2x_1 - 3 \ne 2x_2 - 3$, иначе приходим к противоречию. Следовательно, f – инъекция на $\mathbf{R}$. Уравнение $2x - 3 = y$ разрешимо

относительно x, и $x = (y+3)/2 = f^{-1}(y)$ для любого $y \in \mathbf{R}$. Значит, f – сюръекция на $\mathbf{R}$. Итак, f – биекция на $\mathbf{R}$.

Производная $g'(x) = 3x^2 > 0$ для всех $x \in \mathbf{R}\backslash\{0\}$ и $g'(x) = 0$ при $x = 0$, значит, g является строго возрастающей функцией на $\mathbf{R}$. Поэтому g инъективна на $\mathbf{R}$. Функция g непрерывна на $\mathbf{R}$, $\lim\limits_{x\to-\infty} g(x) = -\infty$, $\lim\limits_{x\to+\infty} g(x) = +\infty$. Поэтому $E(g) = \mathbf{R}$ и g является сюръекцией на $\mathbf{R}$. Таким образом, g – биекция на $\mathbf{R}$.

Так как, например, $h(0) = 2^0 = 1$ и $h(-16) = 2^0 = 1$, то h не является инъективной функцией на $\mathbf{R}$. Поскольку $2^{x^2+16x} > 0$ при всех $x \in \mathbf{R}$, то $E(h) \subset \mathbf{R}_{>0}$, поэтому $E(h) \neq \mathbf{R}$ и h не является сюръективной функцией на $\mathbf{R}$. Итак, h не является биекцией на $\mathbf{R}$.

3) $2x - 3 = y$, откуда $x = (y+3)/2$ для любого $y \in \mathbf{R}$, как уже указывалось в п. 2 решения данного примера. Поэтому $f^{-1}(x) = (x+3)/2$, $D(f^{-1}) = E(f^{-1}) = \mathbf{R}$.

$x^3 - 8 = y$, откуда $x = \sqrt[3]{y+8}$ – единственное решение в $\mathbf{R}$ для любого $y \in \mathbf{R}$. Поэтому $g^{-1}(x) = \sqrt[3]{x+8}$, $D(g^{-1}) = E(g^{-1}) = \mathbf{R}$.

$2^{x^2+16x} = y$, откуда $x^2 + 16x = \log_2 y$. Имеем $D/4 = 64 + \log_2 y \geq 0$ при $y \geq 2^{-64}$, поэтому $E(h) = D(h^{-1}) = [2^{-64}; +\infty)$ и $x_{1,2} = -8 \pm \sqrt{\log_2 y + 64}$. Отображение $h^{-1}(x) = -8 \pm \sqrt{\log_2 x + 64}$ нефункционально, т. к. каждому $x \in (2^{-64}; +\infty)$ ставит в соответствие два различных значения. Но отображения $h_1^{-1}(x) = -8 + \sqrt{\log_2 x + 64}$ и $h_2^{-1}(x) = -8 - \sqrt{\log_2 x + 64}$ где $D(h_1^{-1}) = D(h_2^{-1}) = [2^{-64}; +\infty)$, являются функциями, обратными соответственно сужениям функции h на множества $[-8; +\infty) = D(h_1) = E(h_1^{-1})$ и $(-\infty; -8] = D(h_2) = E(h_2^{-1})$.

5. Множество n-мерных векторов с компонентами из множества K обозначим $V_n(K)$, множество квадратных матриц порядка n с элементами из множества K обозначим $M_n(K)$. Дана функция $f: V_3(\mathbf{Z}/26\mathbf{Z}) \to V_3(\mathbf{Z}/26\mathbf{Z})$, где $f(\boldsymbol{c}) = A\boldsymbol{c}$ для всех $\boldsymbol{c} \in V_3(\mathbf{Z}/26\mathbf{Z})$, $A = \begin{pmatrix} \overline{11} & \overline{2} & \overline{19} \\ \overline{5} & \overline{23} & \overline{25} \\ \overline{22} & \overline{7} & \overline{1} \end{pmatrix} \in M_3(\mathbf{Z}/26\mathbf{Z})$. Обратима ли функция f? В случае положительного ответа найти обратную функцию f^{-1}.

Для упрощения вычислений матрица A может быть представлена в виде

$$A = \begin{pmatrix} \overline{11} & \overline{2} & \overline{-7} \\ \overline{5} & \overline{-3} & \overline{-1} \\ \overline{-4} & \overline{7} & \overline{1} \end{pmatrix}.$$

Если f^{-1} существует, то $f^{-1}: V_3(\mathbf{Z}/26\mathbf{Z}) \to V_3(\mathbf{Z}/26\mathbf{Z})$, где $f^{-1}(\boldsymbol{c}) = A^{-1}\boldsymbol{c}$. Таким образом, функция обратима тогда и только тогда, когда существует обратная матрица $A^{-1} \in M_3(\mathbf{Z}/26\mathbf{Z})$, для чего необходимо и достаточно, чтобы определитель матрицы $\det(A)$ был обратимым классом вычетов в $\mathbf{Z}/26\mathbf{Z}$.

Вычислим $\det(A)$ по правилу «треугольников»:

$$\overline{11}\cdot\overline{(-3)}\cdot\overline{1}+\overline{5}\cdot\overline{7}\cdot\overline{(-7)}+\overline{2}\cdot\overline{(-1)}\cdot\overline{(-4)}-\overline{(-7)}\cdot\overline{(-3)}\cdot\overline{(-4)}-\overline{(-1)}\cdot\overline{7}\cdot\overline{11}-\overline{5}\cdot\overline{2}\cdot\overline{1}=$$
$$=\overline{-33}-\overline{245}+\overline{8}+\overline{84}+\overline{77}-\overline{10}=\overline{-119}=\overline{11}.$$

Поскольку НОД$(11, 26) = 1$, то по теореме 1.4.1 $\det(A)=\overline{11}$ обратим в $\mathbf{Z}/26\mathbf{Z}$. Вычислим $\det(A)^{-1}=\det(A^{-1})$, используя соотношение Безу для чисел 1, 11 и 26 и расширенный алгоритм Евклида:

$$r_{-1}=26,\ u_{-1}=0,\ v_{-1}=1;\ r_0=11,\ u_0=1,\ v_0=0;$$
$$q_1=2,\ u_1=u_{-1}-u_0q_1=-2,\ v_1=v_{-1}-v_0q_1=1\Rightarrow r_1=4=11\cdot(-2)+26;$$
$$q_2=2,\ u_2=u_0-u_1q_2=5,\ v_2=v_0-v_1q_2=-2\Rightarrow r_2=3=11\cdot5+26\cdot(-2);$$
$$q_3=1,\ u_3=u_1-u_2q_3=-7,\ v_3=v_1-v_2q_3=3\Rightarrow r_3=1=11\cdot(-7)+26\cdot3.$$

Тогда $11\cdot(-7)\equiv1\ (\mathrm{mod}\ 26)$ и $\det(A)^{-1}=\overline{11}^{-1}=\overline{-7}$. Итак, функция f^{-1} существует и имеет указанный выше вид.

Алгебраическое дополнение к элементу a_{ij} матрицы A обозначим A_{ij}. Тогда $A^{-1}=\det(A)^{-1}\begin{pmatrix}A_{11}&A_{21}&A_{31}\\A_{12}&A_{22}&A_{32}\\A_{13}&A_{23}&A_{33}\end{pmatrix}$. Вычислим матрицу A^{-1}:

$$A^{-1}=\overline{-7}\begin{pmatrix}\begin{vmatrix}\overline{-3}&\overline{-1}\\\overline{7}&\overline{1}\end{vmatrix}&-\begin{vmatrix}\overline{2}&\overline{-7}\\\overline{7}&\overline{1}\end{vmatrix}&\begin{vmatrix}\overline{2}&\overline{-7}\\\overline{-3}&\overline{-1}\end{vmatrix}\\-\begin{vmatrix}\overline{5}&\overline{-1}\\\overline{-4}&\overline{1}\end{vmatrix}&\begin{vmatrix}\overline{11}&\overline{-7}\\\overline{-4}&\overline{1}\end{vmatrix}&-\begin{vmatrix}\overline{11}&\overline{-7}\\\overline{5}&\overline{-1}\end{vmatrix}\\\begin{vmatrix}\overline{5}&\overline{-3}\\\overline{-4}&\overline{7}\end{vmatrix}&-\begin{vmatrix}\overline{11}&\overline{2}\\\overline{-4}&\overline{7}\end{vmatrix}&\begin{vmatrix}\overline{11}&\overline{2}\\\overline{5}&\overline{-3}\end{vmatrix}\end{pmatrix}=\overline{-7}\begin{pmatrix}\overline{-3+7}&-\overline{(2+49)}&\overline{-2-21}\\-\overline{(5-4)}&\overline{11-28}&-\overline{(-11+35)}\\\overline{35-12}&-\overline{(77+8)}&\overline{-33-10}\end{pmatrix}=$$
$$=\overline{-7}\begin{pmatrix}\overline{4}&\overline{1}&\overline{3}\\\overline{-1}&\overline{9}&\overline{2}\\\overline{-3}&\overline{-7}&\overline{9}\end{pmatrix}=\begin{pmatrix}\overline{-2}&\overline{-7}&\overline{-21}\\\overline{7}&\overline{-11}&\overline{-14}\\\overline{21}&\overline{23}&\overline{-11}\end{pmatrix}=\begin{pmatrix}\overline{24}&\overline{19}&\overline{5}\\\overline{7}&\overline{15}&\overline{12}\\\overline{21}&\overline{23}&\overline{15}\end{pmatrix}.$$

Задачи

1. Перечислить в виде подмножеств $X\times Y$ графики всех соответствий между множествами X и Y. Какие из соответствий являются отображениями, сюръективными, инъективными, функциональными? Какие из отображений являются функциями? Указать все инъективные, сюръективные и биективные функции:

а) $X=\{1, 2\}$, $Y=\{3\}$; **б)** $X=\{1\}$, $Y=\{3, 4\}$.

2. Представить вещественную функцию $f(x)=\left(1-e^{2x}\right)^3$ в виде композиции элементарных функций.

3. Даны вещественные функции $f(x)=\log_2 x$ и $g(x)=\log_3 x$. Доказать, что композиция функций f и g некоммутативна.

4. Заданы три вещественные функции: $f(x)=2x^9-7$, $g(x)=-5\mathrm{arctg}(4x)+2$, $h(x)=e^{5^x}-17$. Требуется:

1) указать области определения функций f, g, h и найти формулы композиций $fgh(x)$, $hfg(x)$, $ffg(x)$, указав их области определения;

2) исследовать функции f, g, h на инъективность в области определения, сюръективность на **R**, биективность на **R**;

3) найти обратные функции для f, g, h или обратные функции для их инъективных сужений на подмножества $D(f)$, $D(g)$, $D(h)$ соответственно. Найти области определения и области значений обратных функций.

5. Дана функция $f: V_3(\mathbf{Z}/28\mathbf{Z}) \to V_3(\mathbf{Z}/28\mathbf{Z})$, где $f(\boldsymbol{c}) = A\boldsymbol{c}$, $\forall\, \boldsymbol{c} \in V_3(\mathbf{Z}/28\mathbf{Z})$, $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{4} & \overline{5} & \overline{6} \\ \overline{7} & \overline{8} & \overline{0} \end{pmatrix} \in M_3(\mathbf{Z}/28\mathbf{Z})$. Обратима ли функция f? В случае положительного ответа найти обратную функцию f^{-1} и обратную матрицу A^{-1}.

Ответы

1. а) $Q_0 = \{(\,)\} = \varnothing$, $Q_1 = \{(1, 3)\}$, $Q_2 = \{(2, 3)\}$, $Q_3 = \{(1, 3), (2, 3)\}$, q_1, q_2 – сюръективные, инъективные, функциональные соответствия, q_3 – сюръективная функция; **б)** $Q_0 = \{(\,)\} = \varnothing$, $Q_1 = \{(1, 3)\}$, $Q_2 = \{(1, 4)\}$, $Q_3 = \{(1, 3), (1, 4)\}$, q_1, q_2 – инъективные функции, q_3 – сюръективное отображение. **2.** $f(x) = f_4 f_3 f_2 f_1(x)$, где $f_1(x) = 2x$ $(f_1(x) = e^x)$, $f_2(x) = e^x$ $(f_2(x) = x^2)$, $f_3(x) = 1 - x$, $f_4(x) = x^3$. **4. 1)** $D(f) = D(g) = D(h) = \mathbf{R}$, $D(fgh) = D(hfg) = D(ffg) = \mathbf{R}$, $fgh(x) = 2\left(-5\operatorname{arctg}\left(4e^{5^x} - 68\right) + 2\right)^9 - 7$, $hfg(x) = e^{5^{2\left(-5\operatorname{arctg}(4x) + 2\right)^9 - 7}} - 17$, $ffg(x) = 2\left(2(-5\operatorname{arctg}(4x) + 2)^9 - 7\right)^9 - 7$; **2)** f – биекция на **R**, g, h – инъекции, не сюръекции, не биекции на **R**; **3)** $f^{-1}(x) = \sqrt[9]{(x+7)/2}$, $D(f^{-1}) = E(f^{-1}) = \mathbf{R}$, $g^{-1}(x) = \frac{1}{4}\operatorname{tg}((2-x)/5)$, $D(g^{-1}) = (-5\pi/2 + 2;\, 5\pi/2 + 2)$, $E(g^{-1}) = \mathbf{R}$, $h^{-1}(x) = \log_5(\ln(x+17))$, $D(h^{-1}) = (-16; +\infty)$, $E(h^{-1}) = \mathbf{R}$. **5.** $f^{-1}: V_3(\mathbf{Z}/28\mathbf{Z}) \to V_3(\mathbf{Z}/28\mathbf{Z})$, где $f^{-1}(\boldsymbol{c}) = A^{-1}\boldsymbol{c}$, $\det(A) = \det(A^{-1}) = \overline{-1}$, $A^{-1} = \begin{pmatrix} \overline{20} & \overline{4} & \overline{3} \\ \overline{14} & \overline{21} & \overline{22} \\ \overline{3} & \overline{22} & \overline{3} \end{pmatrix} \in M_3(\mathbf{Z}/28\mathbf{Z})$.

§2.2. Взаимно однозначное соответствие. Мощность множества

Определение 2.2.1. *Взаимно однозначным соответствием* между двумя непустыми множествами A и B называется такое правило (или закон) f, по которому каждому элементу $a \in A$ сопоставляется единственный элемент $f(a) \in B$ и для любого элемента $b \in B$ существует единственный элемент $a \in A$, такой, что $f(a) = b$, другими словами, функция $f: A \to B$ является биекцией.

Определение 2.2.2. Множества A и B называются *равномощными* (обозначение $A \leftrightarrow B$), если между ними можно установить взаимно однозначное соответствие.

Очевидно, что если множество A равномощно B, а B равномощно C, то A равномощно C, т. е. $A \leftrightarrow B \;\&\; B \leftrightarrow C \Rightarrow A \leftrightarrow C$, – свойство транзитивности.

Определение 2.2.3. Число элементов в конечном множестве A называется *мощностью* A и часто обозначается $|A|$. Пустое множество, т. е. не содержащее элементов, относят к конечным, оно является множеством мощности 0: $|\varnothing| = 0$.

Теорема 2.2.1. *Между непустыми конечными множествами A и B существует взаимно однозначное соответствие тогда и только тогда, когда* $|A| = |B|$.

Теорема 2.2.2. *Общее число взаимно однозначных соответствий для двух n-элементных множеств равно* $n!$.

Теорема 2.2.3. *Пусть* $A_1, A_2, \ldots, A_n$ *– конечные множества и* $|A_i| = m_i$, $i = \overline{1, n}$, *причем* $A_i \cap A_j = \varnothing$ *при* $i \neq j$. *Тогда мощность множества* $A_1 \cup A_2 \cup \ldots \cup A_n$ *равна сумме мощностей множеств* $A_1, A_2, \ldots, A_n$:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = m_1 + m_2 + \ldots + m_n.$$

Теорема 2.2.4. *Пусть* $A_1, A_2, \ldots, A_n$ *– конечные множества и* $|A_i| = m_i$, $i = \overline{1, n}$. *Тогда мощность множества* $A_1 \times A_2 \times \ldots \times A_n = \{ (a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = \overline{1, n} \}$ *равна произведению мощностей множеств* $A_1, A_2, \ldots, A_n$:

$$|A_1 \times A_2 \times \ldots \times A_n| = m_1 m_2 \ldots m_n.$$

Если $A_i = A$, $i = \overline{1, n}$, то $\underbrace{A \times A \times \ldots \times A}_{n} = A^n = \{ (a_1, a_2, \ldots, a_n) \mid a_i \in A, i = \overline{1, n} \}$.

Следствие. $|A^n| = |A|^n$ *для любого конечного множества A и любого* $n \in \mathbf{N}$.

Определение 2.2.4. Пусть A – некоторое множество. *Множеством-степенью*, или *булеаном*, A называется множество $P(A) = \{X \mid X \subseteq A\}$, состоящее из всех подмножеств множества A.

Теорема 2.2.5. *Для любого конечного множества A, где* $|A| = n \in \mathbf{Z}_{\geq 0}$, *число всех подмножеств A равно* 2^n, *т. е.* $|P(A)| = 2^n$.

Число всех k-элементных подмножеств n-элементного множества A, где $n \in \mathbf{Z}_{\geq 0}$, $0 \leq k \leq n$, равно числу сочетаний из n элементов по k: $C_n^k = \dfrac{n!}{k!(n-k)!}$.

Определение 2.2.5. Множество, равномощное множеству натуральных чисел **N**, называется *счетным*.

Любое бесконечное подмножество множества **N** счетно. Счетным является множество **Z**. Это можно установить, рассмотрев взаимно однозначное соответствие f: $\mathbf{Z} \to \mathbf{N}$, представленное на рис. 2.2.1.

Z:	…	$-n$	…	-4	-3	-2	-1	0	1	2	3	4	…	n	…
		↓		↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	
N:	…	$2n+1$	…	9	7	5	3	1	2	4	6	8	…	$2n$	…

Рис. 2.2.1

$$f(z) = \begin{cases} 2z \text{ при } z \in \mathbf{N}; \\ 2|z| + 1 \text{ при } z \in \mathbf{Z}_{\leq 0}. \end{cases}$$

Счетным является также и множество **Q**. Объединение конечного числа счетных множеств, объединение счетного множества конечных множеств и объединение счетного множества счетных множеств счетны.

Определение 2.2.6. Если бесконечное множество не равномощно множеству **N**, то такое множество называется *несчетным*.

Теорема 2.2.6 (Г. Кантор). *Множество всех действительных чисел интервала* (0; 1) *несчетно*.

Определение 2.2.7. Мощность множества всех действительных чисел интервала (0; 1) называется *континуумом*, а множества такой мощности – *континуальными*.

Интервал (0; 1) может быть приведен во взаимно однозначное соответствие с полуинтервалами [0; 1) (рис. 2.2.2) и (0; 1], отрезком [0; 1] (рис. 2.2.3), а также множествами $(a; b)$, $(a; b]$, $[a; b)$, $[a; b]$, где $a, b \in \mathbf{R}$, $a < b$, и всем множеством **R**.

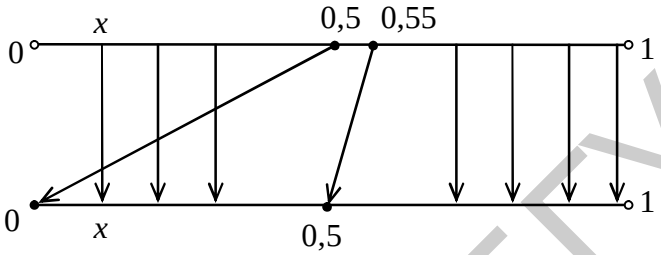

Рис. 2.2.2

$$f\colon (0;\,1) \to [0;\,1),\ \text{где}\ f(x) = \begin{cases} x \ \text{ при } \ x \neq 0,\underbrace{5\ldots5}_{n},\ n \in \mathbf{N}; \\ 0 \ \text{ при } \ x = 0{,}5; \\ 0,\underbrace{5\ldots5}_{n} \ \text{ при } \ x = 0,\underbrace{5\ldots5}_{n+1},\ n \in \mathbf{N}. \end{cases}$$

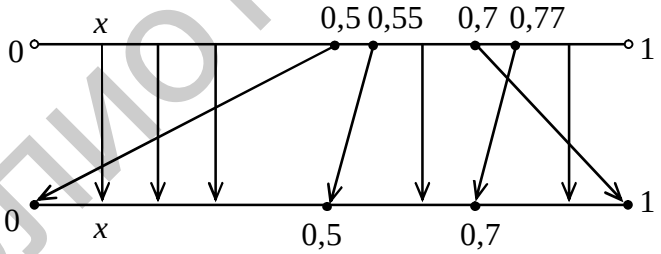

Рис. 2.2.3

$$f\colon (0;\,1) \to [0;\,1],\ \text{где}\ f(x) = \begin{cases} x \ \text{ при } \ x \neq 0,\underbrace{5\ldots5}_{n},\ x \neq 0,\underbrace{7\ldots7}_{n},\ n \in \mathbf{N}; \\ 0 \ \text{ при } \ x = 0{,}5; \\ 1 \ \text{ при } \ x = 0{,}7; \\ 0,\underbrace{5\ldots5}_{n} \ \text{ при } \ x = 0,\underbrace{5\ldots5}_{n+1},\ n \in \mathbf{N}; \\ 0,\underbrace{7\ldots7}_{n} \ \text{ при } \ x = 0,\underbrace{7\ldots7}_{n+1},\ n \in \mathbf{N}. \end{cases}$$

В общем случае взаимно однозначное соответствие $f\colon (c; d) \to (a; b)$ для произвольных $a, b, c, d \in \mathbf{R}$, таких, что $a < b$, $c < d$, задается аналитически следующим образом:

$$f(x) = \frac{b-a}{d-c}(x-c) + a, \ \forall\ x \in (c; d). \qquad (2.2.1)$$

Значит, функция $g\colon (0; 1) \to \mathbf{R}$, где $g(x) = \operatorname{tg}(\pi x - \pi/2)$, задает взаимно однозначное соответствие между множествами (0; 1) и $\mathbf{R}$.

Примерами континуальных множеств являются $\mathbf{R}^2$ и вообще $\mathbf{R}^n$ для любого $n \in \mathbf{N}$.

Множество всех подмножеств счетного множества континуально. Вообще для множества любой мощности его булеан имеет более высокую мощность. Поэтому не существует множества максимальной мощности.

Примеры

1. Показать, что множества $\mathbf{R}^2$ и $A \times B$, где $A = \{(x, y) \in \mathbf{R}^2 \mid 2x + y = 1\}$, $B = \{(x, y) \in \mathbf{R}^2 \mid x - y = 0\}$, равномощны.

Нетрудно видеть, что $\mathbf{R}^2$ равномощно множеству всех точек на действительной плоскости, A равномощно множеству всех точек прямой $2x + y = 1$, B – множеству всех точек прямой $x - y = 0$ на действительной плоскости (рис. 2.2.4). Поскольку коэффициенты при x и y в уравнениях двух данных прямых непропорциональны, прямые пересекаются на плоскости в единственной точке с координатами (1/3, 1/3).

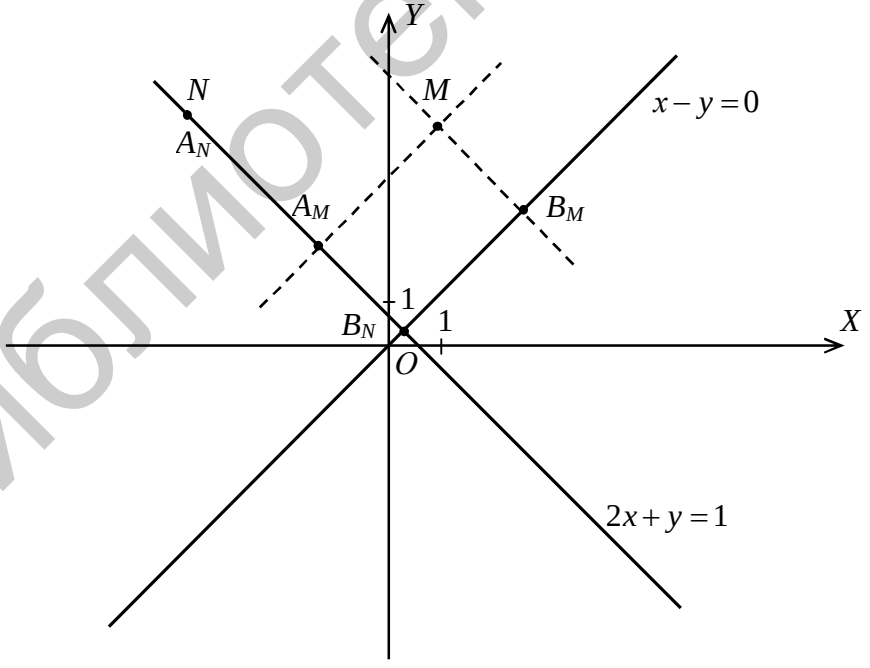

Рис. 2.2.4

Для доказательства равномощности $\mathbf{R}^2$ и $A \times B$ достаточно показать равномощность множеств всех точек действительной плоскости и всех упорядоченных пар точек на прямых $2x + y = 1$ и $x - y = 0$.

Каждой точке M на плоскости поставим в соответствие упорядоченную пару точек (A_M, B_M) на прямых $2x+y=1$ и $x-y=0$, являющихся точками пересечения этих прямых с прямыми, проходящими через данную точку и параллельными $x-y=0$ и $2x+y=1$ соответственно. Если точка N принадлежит прямой $2x+y=1$ либо $x-y=0$, то первым (вторым) элементом пары точек на прямых будет сама данная точка, а вторым (первым) элементом пары – точка (1/3, 1/3) (см. рис. 2.2.4).

Согласно утверждениям планиметрии данное правило задает взаимно однозначное соответствие между множеством всех точек на действительной плоскости $(\mathbf{R}^2)$ и множеством всех упорядоченных пар точек на прямых $2x+y=1$ и $x-y=0$ ($A\times B$).

2. Пусть A и B – конечные множества. Доказать утверждения:

1) $|A\cap B|=|A|-|A\setminus B|=|B|-|B\setminus A|$;

2) $|A\cup B|=|A|+|B|-|A\cap B|$;

3) $|A\Delta B|=|A|+|B|-2|A\cap B|$, здесь $A\Delta B=A\setminus B\cup B\setminus A$ – симметрическая разность множеств A и B.

Доказательство:

1) поскольку $A=(A\cap B)\cup(A\setminus B)$ и $(A\cap B)\cap(A\setminus B)=\varnothing$, то согласно теореме 2.2.3 получаем, что $|A|=|A\cap B|+|A\setminus B|$, откуда $|A\cap B|=|A|-|A\setminus B|$. Аналогично доказывается, что $|A\cap B|=|B|-|B\setminus A|$;

2) так как $A\cup B=A\setminus B\cup B\setminus A\cup(A\cap B)$ и множества в правой части попарно не пересекаются, то $|A\cup B|=|A\setminus B|+|B\setminus A|+|A\cap B|$ согласно теореме 2.2.3. Согласно п. 1 данного примера имеем $|A\setminus B|=|A|-|A\cap B|$ и $|B\setminus A|=|B|-|A\cap B|$, следовательно,

$$|A\cup B|=|A|-|A\cap B|+|B|-|A\cap B|+|A\cap B|=|A|+|B|-|A\cap B|;$$

3) так как $A\Delta B=A\setminus B\cup B\setminus A$ и $(A\setminus B)\cap(B\setminus A)=\varnothing$, то согласно теореме 2.2.3 имеем $|A\Delta B|=|A\setminus B|+|B\setminus A|$, откуда согласно п. 1 данного примера получаем

$$|A\Delta B|=|A\setminus B|+|B\setminus A|=|A|-|A\cap B|+|B|-|A\cap B|=|A|+|B|-2|A\cap B|.$$

3. Доказать, что множество $\mathbf{N}^2$ счетно.

$\mathbf{N}^2=\{(m, n)\mid m, n\in\mathbf{N}\}$. Разобьем $\mathbf{N}^2$ на классы. К первому классу N_2 отнесем все пары чисел с минимальной суммой, равной 2. Таким образом, $N_2=\{(1, 1)\}$. Ко второму классу N_3 отнесем все пары чисел с суммой 3: $N_3=\{(1, 2), (2, 1)\}$. Тогда $N_4=\{(1, 3), (2, 2), (3, 1)\}$. В общем случае $N_i=\{(1, i-1),\ldots, (i-1, 1)\}$, $i=2, 3, \ldots$. Каждый класс N_i содержит ровно $i-1$ пар. Упорядочим классы N_i по возрастанию индексов i, а пары внутри класса – по возрастанию первого элемента и занумеруем получившуюся последовательность пар номерами 1, 2, 3, … . Легко видеть, что если $m+n=i+1$, то пара (m, n) получит номер $1+\ldots+(i-1)+m=i(i-1)/2+m$. Эта нумерация задает взаимно однозначное соответствие между $\mathbf{N}^2$ и $\mathbf{N}$, что доказывает счетность $\mathbf{N}^2$.

4. Доказать, что при фиксированном $b\in\mathbf{R}_{>0}$ бесконечное множество равносторонних треугольников, в котором вершинами каждого треугольника являются середины сторон уже построенного треугольника (рис. 2.2.5), счетно.

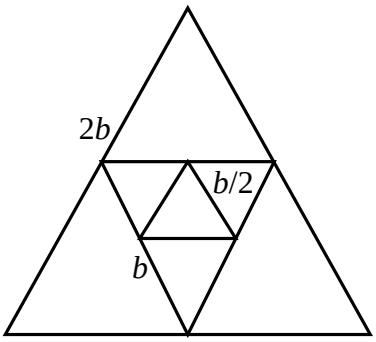

Рис. 2.2.5

Каждому равностороннему треугольнику поставим в соответствие длину его стороны. Если длина стороны фиксированного треугольника равна b, то длина стороны предыдущего треугольника равна $2b$, а последующего – $b/2$. Итак, существует взаимно однозначное соответствие между данным бесконечным множеством равносторонних треугольников и множеством чисел $T_b = \{\, 2^z b \mid z \in \mathbf{Z} \,\}$.

Покажем, что $T_b \leftrightarrow \mathbf{N}$. Для этого рассмотрим взаимно однозначное соответствие $f\colon T_b \to \mathbf{N}$, представленное на рис. 2.2.6.

$$\begin{array}{l} T_b\colon \ldots\ 2^{-n}b\ \ldots\ 2^{-2}b\ \ 2^{-1}b\ \ b\ \ 2b\ \ 2^2 b\ \ldots\ 2^n b\ \ldots \\ \qquad\quad\ \downarrow \qquad\ \downarrow\ \ \downarrow\ \ \downarrow\ \ \downarrow\ \ \downarrow \qquad\ \downarrow \\ \mathbf{N}\colon \ldots\ 2n+1\ \ \ldots\ \ 5\ \ \ 3\ \ \ 1\ \ \ 2\ \ \ 4\ \ \ldots\ \ 2n\ \ldots \end{array}$$

Рис. 2.2.6

$$f\left(2^z b\right) = \begin{cases} 2z \text{ при } z \in \mathbf{N}; \\ 2|\, z \,| + 1 \text{ при } z \in \mathbf{Z}_{\le 0}. \end{cases}$$

Можно было также показать, что $T_b \leftrightarrow \mathbf{Z}$, построив взаимно однозначное соответствие $g\colon T_b \to \mathbf{Z}$, где $g\left(2^z b\right) = z$ для любого $z \in \mathbf{Z}$. Как известно, $\mathbf{Z}$ счетно.

5. Доказать, что множество всех точек гиперболы $y = 1/x$ (рис. 2.2.7) на действительной плоскости $\mathbf{R}^2$ имеет мощность континуума.

Множество всех точек данной гиперболы равномощно следующему множеству: $\Gamma = \{\, (x,\, 1/x) \mid x \in \mathbf{R} \backslash \{0\} \,\}$. Установим взаимно однозначное соответствие между множествами Γ и $\mathbf{R}$. Положим

$$f\left((x,\, 1/x)\right) = \begin{cases} x \text{ при } x \in \mathbf{R} \backslash \mathbf{Z}_{\ge 0}; \\ x - 1 \text{ при } x \in \mathbf{N}. \end{cases}$$

Функция $f\colon \Gamma \to \mathbf{R}$ действительно является взаимно однозначным соответствием. Графическая иллюстрация представлена на рис. 2.2.7. Итак, $\Gamma \leftrightarrow \mathbf{R}$. Поскольку $\mathbf{R}$ – континуальное множество, Γ – также континуальное множество.

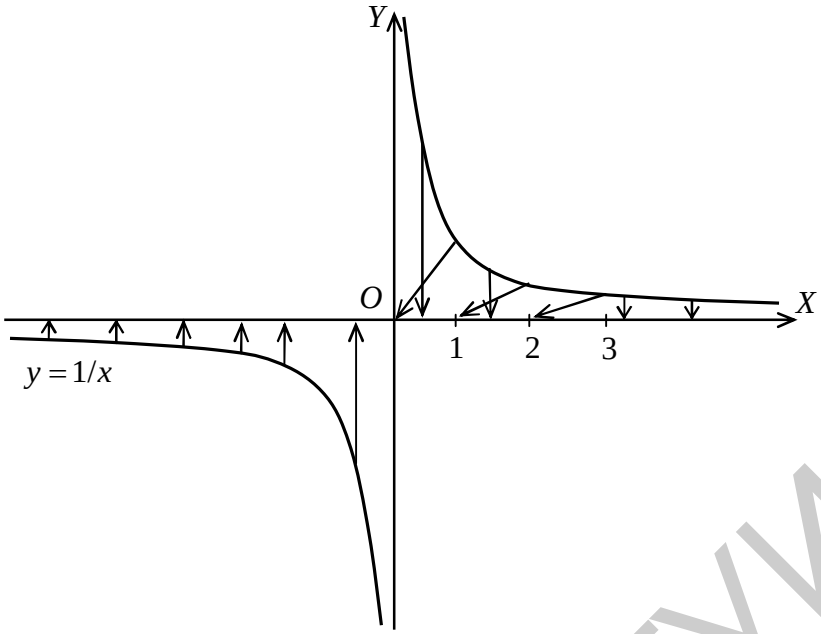

Рис. 2.2.7

6. Доказать равномощность множеств X и Y, построив взаимно однозначные соответствия между ними:

а) $X = [-3; 2]$, $Y = [-5; 1] \cup [7; 8]$.

Представим первое множество в виде $X = [-3; 1] \cup (1; 2]$. Тогда функция

$$g(x) = \frac{1+5}{1+3}(x+3) - 5 = \frac{3}{2}x - \frac{1}{2},\ \forall\, x \in [-3; 1],$$

полученная по формуле (2.2.1), задает взаимно однозначное соответствие между множествами $[-3; 1]$ и $[-5; 1]$. Также линейная функция h_1, построенная согласно (2.2.1), задает взаимно однозначное соответствие между $(1; 2]$ и $(7; 8]$:

$$h_1(x) = \frac{8-7}{2-1}(x-1) + 7 = x + 6,\ \forall\, x \in (1; 2].$$

Функция h, построенная при помощи h_1 и одной последовательности сдвигов, задает взаимно однозначное соответствие между $(1; 2]$ и $[7; 8]$:

$$h(x) = \begin{cases} h_1(x) \text{ при } x \in (1; 2],\ x \neq 1,\underbrace{5\ldots5}_{n},\ n \in \mathbf{N}; \\ 7 \text{ при } x = 1{,}5; \\ 7,\underbrace{5\ldots5}_{n} \text{ при } x = 1,\underbrace{5\ldots5}_{n+1},\ n \in \mathbf{N}. \end{cases}$$

$$f(x) = \begin{cases} g(x) \text{ при } x \in [-3; 1]; \\ h(x) \text{ при } x \in (1; 2]. \end{cases}$$

Функция $f\colon X \to Y$ является биекцией, поэтому $X \leftrightarrow Y$.

б) $X = [3; 5]$, $Y = [-7; 12] \cup \{13\}$.

$[3; 5] \leftrightarrow [-7; 12]$, т. к. функция g, построенная в соответствии с (2.2.1), биективна:

$$g(x)=\frac{12+7}{5-3}(x-3)-7=\frac{19}{2}x-\frac{71}{2},\ \forall\, x\in[3;\,5].$$

$$f(x)=\begin{cases} g(x) \text{ при } x\in[3;\,5],\ x\neq 3,\underbrace{5\ldots5}_{n},\ n\in\mathbf{N};\\ 13 \text{ при } x=3{,}5;\\ g(3,\underbrace{5\ldots5}_{n}) \text{ при } x=3,\underbrace{5\ldots5}_{n+1},\ n\in\mathbf{N}. \end{cases}$$

Функция f, построенная при помощи g и одной последовательности сдвигов, задает взаимно однозначное соответствие между X и Y, поэтому $X\leftrightarrow Y$.

в) $X=[-2;\,4]$, $Y=[-2;\,1]\cup\{3\}\cup\{4\}$.

$[-2;\,4]\leftrightarrow[-2;\,1]$, т. к. функция g, построенная согласно (2.2.1), биективна:

$$g(x)=\frac{1+2}{4+2}(x+2)-2=\frac{1}{2}x-1,\ \forall\, x\in[-2;\,4].$$

Тогда функция f, построенная при помощи g и двух непересекающихся последовательностей сдвигов, задает взаимно однозначное соответствие между X и Y:

$$f(x)=\begin{cases} g(x) \text{ при } x\in[-2;\,4],\ x\neq 1,\underbrace{5\ldots5}_{n},\ x\neq 2,\underbrace{7\ldots7}_{n},\ n\in\mathbf{N};\\ 3 \text{ при } x=1{,}5;\\ 4 \text{ при } x=2{,}7;\\ g(1,\underbrace{5\ldots5}_{n}) \text{ при } x=1,\underbrace{5\ldots5}_{n+1},\ n\in\mathbf{N};\\ g(2,\underbrace{7\ldots7}_{n}) \text{ при } x=2,\underbrace{7\ldots7}_{n+1},\ n\in\mathbf{N}. \end{cases}$$

Таким образом, $X\leftrightarrow Y$.

г) $X=[-3;\,2]$, $Y=\mathbf{R}$.

$(-3;\,2)\leftrightarrow(-\pi/2;\,\pi/2)$, т. к. функция g_1, построенная согласно (2.2.1), биективна:

$$g_1(x)=\frac{\pi/2+\pi/2}{2+3}(x+3)-\pi/2=\frac{\pi}{5}x+\frac{\pi}{10},\ \forall\, x\in(-3;\,2).$$

$$g(x)=\begin{cases} g_1(x) \text{ при } x\in(-3;\,2),\ x\neq g_1^{-1}(0,\underbrace{4\ldots4}_{n}),\ x\neq g_1^{-1}(0,\underbrace{8\ldots8}_{n}),\ n\in\mathbf{N};\\ 0{,}4 \text{ при } x=-3;\\ 0{,}8 \text{ при } x=2;\\ 0,\underbrace{4\ldots4}_{n+1} \text{ при } x=g_1^{-1}(0,\underbrace{4\ldots4}_{n}),\ n\in\mathbf{N};\\ 0,\underbrace{8\ldots8}_{n+1} \text{ при } x=g_1^{-1}(0,\underbrace{8\ldots8}_{n}),\ n\in\mathbf{N}. \end{cases}$$

Функция g, построенная при помощи g_1 и двух непересекающихся последовательностей сдвигов, задает взаимно однозначное соответствие между $[-3;\,2]$ и $(-\pi/2;\,\pi/2)$. Функция $f\colon(-\pi/2;\,\pi/2)\to\mathbf{R}$, где $f(x)=\operatorname{tg}x$, является биективной, поэтому $(-\pi/2;\,\pi/2)\leftrightarrow\mathbf{R}$. Таким образом, $X\leftrightarrow Y$, т. к. взаимно однозначное соответствие задается функцией $fg\colon X\to Y$.

Задачи

1. Определить, задает ли функция f взаимно однозначное соответствие между множествами:

а) $X = \{$множество всех студентов в аудитории$\}$, $Y = \{ y \in \mathbf{R} \mid 1{,}5 \le y \le 2 \}$, где функция $f\colon X \to Y$ ставит в соответствие каждому человеку его рост в метрах;

б) $X = Y = \mathbf{R}$, $f\colon X \to Y$, где $f(x) = \sin x$. В случае отрицательного ответа установить, как нужно изменить множества, чтобы данная функция f задавала взаимно однозначное соответствие между ними.

2. Показать, что множество всех положительных вещественных чисел континуально. Указание: $\mathbf{R}$ – континуальное множество, построить биективную функцию $f\colon \mathbf{R} \to \mathbf{R}_{>0}$ или $f^{-1}\colon \mathbf{R}_{>0} \to \mathbf{R}$.

3. Доказать равномощность множеств X и Y, построив взаимно однозначные соответствия между ними:

а) $X = 3\mathbf{Z} = \{ 3z \mid z \in \mathbf{Z} \}$, $Y = \mathbf{Z}_{\ge -1}$. Указание: использовать метод доказательства счетности $\mathbf{Z}$ и метод решения примера 4;

б) $X = (-8;\, 5]$, $Y = (0;\, 1] \cup [3;\, 7]$. Указание: использовать метод решения примера 6, а;

в) $X = [4;\, 9] \cup \{10\}$, $Y = \mathbf{R}$. Указание: использовать метод решения примера 6, г.

4. Доказать, что равномощны множества $\mathbf{C}\backslash\{0\}$ и $(0;\, +\infty) \times (-2\pi;\, \pi)$. Указание: доказать, что $(-2\pi;\, \pi) \leftrightarrow [0;\, 2\pi)$, и воспользоваться тригонометрической или показательной формой записи комплексных чисел.

Ответы

1. а) нет, т. к. функция f несюръективна и не всегда инъективна; **б)** нет, т. к. функция f несюръективна и неинъективна; на X функция f должна быть строго монотонна, а Y должно быть областью значений f, заданной на X, например $X = [-\pi/2;\, \pi/2]$, $Y = [-1;\, 1]$.

§2.3. Классические шифры

Шифрование – это частный случай кодирования, преобразование сообщений в формулы, которые обеспечивают защиту информации от несанкционированного доступа.

Определение 2.3.1. *Криптографические преобразования шифрования* (*зашифровывания*) и *расшифровывания* определяются как взаимно обратные функции:

$$f_L(A) = B,\ g_L(B) = A,$$

где L – *ключ* – параметр шифра, определяющий выбор конкретного преобразования, известный отправителю и адресату;

A и B – соответственно исходное и закодированное сообщение, или *открытый текст* и *шифртекст* (*криптограмма*).

Совокупность преобразований f_L и набор ключей, которым они соответствуют, будем называть *шифром*. *Классическими шифрами* принято называть симметричные блочные шифры, т. е. те, которые для шифрования и расшифровывания используют один и тот же ключ и шифруют информацию блоками.

Определение 2.3.2. Получение открытого сообщения без заранее известного ключа по шифрованному называется *дешифрованием*, или *вскрытием шифра*, в отличие от процесса *расшифровывания*, когда ключ известен. Под *стойкостью шифра*, как правило, понимается способность противостоять попыткам произвести его вскрытие.

Определение 2.3.3. *Шифрами замены* называют такие шифры, преобразования из которых приводят к замене каждого символа открытого сообщения на другие символы – *шифробозначения*, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения. *Шифрами перестановки* называют такие шифры, преобразования из которых приводят к изменению только порядка следования символов исходного сообщения.

Шифры замены

Шифр простой однобуквенной замены. Рассмотрим на примере русского алфавита следующую таблицу (табл. 2.3.1).

Таблица 2.3.1

А	Б	В	Г	Д	…	Э	Ю	Я
f(А)	f(Б)	f(В)	f(Г)	f(Д)	…	f(Э)	f(Ю)	f(Я)

Вторая строка в табл. 2.3.1 представляет собой перестановку букв алфавита первой строки. При зашифровывании и расшифровывании надо помнить вторую строку, т. е. ключ. Обычно ее запомнить сложно, поэтому всегда пытались придумать какое-либо правило.

Одним из древнейших шифров, известных истории, был *шифр Цезаря*, для которого вторая строка в табл. 2.3.1 является первой строкой, циклически сдвинутой на определенное число позиций, т. е. последовательностью, записанной в алфавитном порядке, но начинающейся не с буквы «А». Главное, чтобы тот, кому посылается зашифрованное сообщение, знал эту величину сдвига. Итак, чтобы запомнить ключ, надо знать первую букву второй строки табл. 2.3.1. Однако такой шифр обладает большим недостатком: число различных ключей на 1 меньше числа букв в алфавите. Перебрав эти варианты, можно однозначно восстановить отправленное сообщение.

Шифры перестановки

Шифры перестановки изменяют только порядок следования символов текста, но не изменяют их самих. Поэтому для расшифровывания нужно знать *подстановку* – биекцию множества символов сообщения, задающую преобразование. Всего существует $n!$ подстановок на n-элементном множестве (теорема 2.2.2). С увеличением числа n значение $n!$ растет очень быстро.

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Рассмотрим некоторые из них подробнее.

1. Одним из самых первых шифровальных приспособлений был жезл («сцита́ла»), применявшийся еще в древней Греции во времена войны Спарты

против Афин в V в. до н. э. Жезл имел форму цилиндра, на который виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль его оси записывался необходимый для передачи текст. Лента разматывалась, и получалось (для непосвященных), что поперек нее в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату, который, имея цилиндр точно такого же диаметра, наматывал ленту на него и прочитывал сообщение вдоль оси. Ясно, что такой способ шифрования осуществляет перестановку местами букв сообщения.

Шифр «сцитала» реализует не более n перестановок, где n – длина сообщения. Действительно, этот шифр, как нетрудно видеть, эквивалентен следующему шифру *маршрутной перестановки*: в таблицу, состоящую из m столбцов, построчно записывают сообщение, после чего выписывают буквы по столбцам. Число задействованных столбцов таблицы не может превосходить длины сообщения. Имеются еще и чисто физические ограничения, накладываемые реализацией шифра «сцитала». Естественно предположить, что диаметр жезла не должен превосходить 10 см. Тогда при высоте строки в 1 см на одном витке такого жезла уместится не более 32 букв ($10\pi < 32$). Таким образом, число перестановок, реализуемых «сциталой», вряд ли превосходит 32.

2. Шифр «поворотная решетка». Данный способ шифрования также носит название «сетки (решетки) Кардано». Для использования такого шифра изготавливается трафарет из прямоугольного листа клетчатой бумаги размером $2m \times 2k$ клеток. В трафарете вырезано mk клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа. Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке. Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Число возможных трафаретов, т. е. количество ключей шифра «поворотной решетки», составляет $T = 4^{mk}$. Этот шифр предназначен для сообщений длиной $n = 4mk$.

3. Широко распространена разновидность шифра маршрутной перестановки, называемая «вертикальной перестановкой». Здесь снова используется прямоугольник, в который сообщение вписывается обычным способом (по строкам слева направо). Для получения горизонтальной криптограммы по строкам слева направо выписываются буквы, записанные по вертикали в столбцах, а столбцы при этом берутся в порядке, определяемом ключом.

Число ключей шифра «вертикальной перестановки» не более $m!$, где m – число столбцов таблицы. Как правило, m гораздо меньше, чем длина текста n (сообщение укладывается в несколько строк по m букв), а значит, и $m!$ много меньше $n!$. В случае когда ключ «вертикальной перестановки» не рекомендуется записывать, его можно извлекать из какого-то легко запоминающегося слова

или предложения, содержащего m букв. Наиболее распространенный способ состоит в том, чтобы приписывать буквам числа в соответствии с обычным алфавитным порядком букв. Например, пусть ключевым словом будет «перестановка». Присутствующая в нем первая буква «А» получает номер 1. Если какая-то буква входит в ключевое слово несколько раз, то ее появления нумеруются последовательно слева направо. Поэтому второе вхождение буквы «А» получает номер 2. Поскольку буквы «Б» в этом слове нет, то буква «В» получает номер 3 и т. д. Процесс продолжается до тех пор, пока все буквы не получат номера. Таким образом, мы получаем ключ в соответствии с табл. 2.3.2.

Таблица 2.3.2

Исходный номер столбца											
1	2	3	4	5	6	7	8	9	10	11	12
П	Е	Р	Е	С	Т	А	Н	О	В	К	А
9	4	10	5	11	12	1	7	8	3	6	2
Номер столбца после перестановки											

Данный ключ определяет перестановку столбцов: $1 \mapsto 9,\ 2 \mapsto 4,\ 3 \mapsto 10,\ 4 \mapsto 5,\ 5 \mapsto 11,\ 6 \mapsto 12,\ 7 \mapsto 1,\ 8 \mapsto 7,\ 9 \mapsto 8,\ 10 \mapsto 3,\ 11 \mapsto 6,\ 12 \mapsto 2$. Получатель сообщения должен выполнить обратную перестановку строк: $1 \mapsto 7,\ 2 \mapsto 12,\ 3 \mapsto 10,\ 4 \mapsto 2,\ 5 \mapsto 4,\ 6 \mapsto 11,\ 7 \mapsto 8,\ 8 \mapsto 9,\ 9 \mapsto 1,\ 10 \mapsto 3,\ 11 \mapsto 5,\ 12 \mapsto 6$, затем прочитать текст по столбцам сверху вниз в порядке их следования или транспонировать матрицу и прочитать текст по строкам слева направо в порядке их следования.

Шифр Виженера

Шифр Виженера относится к *многоалфавитным шифрам замены*. В европейских странах многоалфавитные шифры были изобретены в эпоху Возрождения, когда развитие торговли потребовало надежных способов защиты информации.

Дополним естественный порядок букв в алфавите. Будем считать, что за последней буквой алфавита следует его первая буква. Расположим буквы на окружности в естественном порядке по часовой стрелке. Тогда значения относительных порядковых номеров (относительно фиксированной буквы) букв алфавита из n элементов совпадают со значениями всевозможных остатков от деления целых чисел на натуральное число n.

Определение 2.3.4. Число $D(N_1, N_2)$, равное порядковому номеру буквы с естественным номером N_1 относительно буквы с порядковым номером N_2 в алфавите, называется *знаком гаммы*.

Остаток от деления целого числа N на $n \in \mathbf{N}$ обозначим $r_n(N)$. Таким образом, $D(N_1, N_2) = r_n(N_1 - N_2)$, где n – число букв в алфавите.

Для шифра Виженера характерно то, что буквы открытого текста, зашифрованные одним и тем же знаком гаммы, по сути, зашифрованы одним и тем же шифром простой замены. Например, в *ключевой таблице* шифра простой замены при знаке гаммы, равном 1, для русского алфавита (см. табл. 2.3.1) вторая

строка получена из первой циклическим сдвигом на одну позицию, т. е. начинается буквой «Б» и заканчивается буквой «А».

Вторую строку ключевой таблицы называют *алфавитом шифрования, соответствующим данному знаку гаммы*. Поскольку в шифре Виженера возможны все значения гаммы от 0 до $n-1$, то данный шифр можно рассматривать как n-алфавитный шифр замены. Если каждому из этих алфавитов поставить в соответствие его первую букву, то каждый знак гаммы можно заменить порядковым номером этой буквы в исходном алфавите. В этом случае ключ рассматриваемого шифра можно взаимно однозначно заменить соответствующим словом в этом же алфавите. *Таблица Виженера* состоит из списка n алфавитов шифрования, расположенных горизонтально. Каждый алфавит циклически сдвинут относительно находящегося над ним на одну букву влево.

Способ зашифровывания с помощью таблиц Виженера заключается в том, что первый из алфавитов соответствует исходному алфавиту открытого текста, а букве ключевого слова соответствует алфавит шифрования из данного списка, начинающийся с этой буквы. Буква зашифрованного текста находится в алфавите шифрования на месте, соответствующем данной букве открытого текста. Таким образом, шифр Цезаря – частный случай шифра Виженера, соответствующий ключевой последовательности, состоящей из одной буквы. Например:

УНИВЕРСИТЕТ – открытый текст;

ВЛТВЛТВЛТВЛ – периодическая ключевая последовательность;

ХЧЫДРВУУДЗЭ – зашифрованный текст.

Здесь русский алфавит состоит из 30 букв (без «Ё», «Й», «Ъ»), период ключевой последовательности равен 3.

Простота построения таблиц Виженера делает эту систему привлекательной для практического использования. В качестве ключа может быть использован текст самого сообщения или же зашифрованный текст. Такой шифр носит название *самоключа*. Первая идея вскрытия зашифрованного текста при таком методе шифрования состоит в использовании *вероятного слова*, т. е. слова, которое с большой вероятностью может содержаться в данном открытом тексте или в ключевой последовательности. Вторая идея дешифрования основана на том, что буквы открытого сообщения находятся в тексте на вполне определенных позициях. Если разность номеров их позиций окажется кратной периоду ключевой последовательности, то стоящие на этих позициях буквы будут зашифрованы одним и тем же знаком гаммы. Это означает, что определенные части открытого текста окажутся зашифрованными шифром Цезаря. Эту идею можно использовать для определения периода ключевой последовательности.

Примеры

1. Зашифровывание фразы на латинском языке осуществляется в два этапа. На первом этапе каждая буква текста заменяется на следующую за ней в алфавитном порядке («Z» заменяется на «A»). На втором этапе применяется шифр простой замены с неизвестным ключом. Его применение заключается в замене каждой буквы текста буквой того же алфавита, при этом разные буквы заменяются разными буквами. Ключом такого шифра является таблица, в которой

указано, какой буквой надо заменить каждую букву алфавита. По данному шифртексту

OSZKX FXRF YOQKSZ RAYFK

требуется восстановить отправленное сообщение, если известно, что для использованного (неизвестного) ключа результат шифрования не зависит от порядка выполнения указанных этапов при любом отправленном сообщении. Пробелы разделяют слова, при зашифровывании пробел остается пробелом. Известно также, что в результате зашифровывания «A» $\mapsto$ «F».

Занумеруем от 0 до 23 буквы латинского алфавита, состоящего из 24 букв, как указано в табл. 2.3.3.

Таблица 2.3.3

Латинский алфавит																						
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Порядковые номера букв																							

Пусть x – некоторое число от 0 до 23, $f(x)$ – число, в которое переходит x на втором этапе. Тогда перестановочность этапов можно записать в виде равенства $f(x+1)=f(x)+1$, т. е. $f(x+1)-f(x)=1$. Значит, соседние числа x и $x+1$ на втором этапе переходят в соседние числа $f(x)$ и $f(x)+1$ соответственно, отсюда следует, что второй этап – тоже циклический сдвиг. Последовательное применение двух циклических сдвигов – также циклический сдвиг. Итак, мы имеем классический шифр Цезаря. Остается рассмотреть 23 варианта различных сдвигов. Но поскольку в условии указано, что в результате зашифровывания «A» $\mapsto$ «F», то получаем, что зашифровывание представляет собой циклический сдвиг на 5 позиций вправо. Осложнения, связанные с переходом «Z» в «A», устраняются либо переходом к остаткам при делении на 24, либо выписыванием после буквы «Z» второй раз алфавита A, B,…, Z, т. е. операции выполняются в $\mathbf{Z}/24\mathbf{Z}$. Итак, для расшифровывания фразы нужно каждую букву полученного сообщения сдвинуть циклически на 5 позиций влево, а пробелы оставить на месте.

Итак, получаем следующее исходное сообщение:

INTER ARMA SILENT MUSAE

(и́нтэр а́рма си́лент му́зэ – «когда гремит оружие, музы молчат»).

2. Пусть x_1, x_2 – корни многочлена x^2+3x+1. К порядковому номеру каждой буквы (от 0 до 32) в стандартном русском алфавите (33 буквы) прибавляется по модулю 33 значение многочлена $f(x)=x^6+3x^5+x^4+x^3+4x^2+4x+3$, вычисленное либо при $x=x_1$, либо при $x=x_2$ (в неизвестном порядке), и получается порядковый номер буквы шифртекста в том же алфавите. Нужно расшифровать или дешифровать сообщение

ФВМЁЖТИВФЮ.

Занумеруем буквы русского алфавита от 0 до 32. Все операции будут выполняться в $\mathbf{Z}/33\mathbf{Z}$. Легко видеть, что $f(x)=(x^2+3x+1)(x^4+x+1)+2$. Отсюда

$f(x_1) = f(x_2) = 2$, где x_1, x_2 – корни $x^2 + 3x + 1$. Итак, мы имеем классический шифр Цезаря с циклическим сдвигом на 2 позиции вправо. Для расшифровывания сообщения нужно каждую букву циклически сдвинуть на 2 позиции влево (табл. 2.3.4).

Таблица 2.3.4

Буква шифртекста	Ф	В	М	Ё	Ж	Т	И	В	Ф	Ю
Номер буквы шифртекста	21	2	13	6	7	19	9	2	21	31
Номер буквы открытого текста	19	0	11	4	5	17	7	0	19	29
Буква открытого текста	Т	А	К	Д	Е	Р	Ж	А	Т	Ь

Исходное сообщение:

ТАКДЕРЖАТЬ.

3. Зашифровывание сообщения на русском языке в алфавите из 30 букв (без букв «Ё», «Й», «Ъ») осуществляется при помощи шифра Виженера. Пусть сообщение состоит из *m* букв. Выбирается ключ *K* – некоторая последовательность из *m* букв приведенного выше алфавита. Зашифровывание каждой буквы сообщения состоит в сложении ее порядкового номера (от 0 до 29) с порядковым номером соответствующей буквы ключевой последовательности и замене на букву алфавита, номер которой совпадает с остатком от деления на 30 полученной суммы.

Известно, что ключевая последовательность не содержит никаких букв, кроме «Б», «В», «Г». Требуется дешифровать шифртекст

РБЫНПТСИТСРРЕЗОХ.

Каждая буква зашифрованного сообщения расшифровывается в трех вариантах, предполагается, что соответствующая буква ключевой последовательности есть «Б», «В» или «Г» (табл. 2.3.5).

Таблица 2.3.5

Буква шифртекста	Р	Б	Ы	Н	П	Т	С	И	Т	С	Р	Р	Е	З	О	Х
Вариант «Б»	П	А	Щ	М	О	С	Р	З	С	Р	П	П	Д	Ж	Н	Ф
Вариант «В»	О	Я	Ш	Л	Н	Р	П	Ж	Р	П	О	О	Г	Е	М	У
Вариант «Г»	Н	Ю	Ч	К	М	П	О	Е	П	О	Н	Н	В	Д	Л	Т

Выбирая из каждой колонки в табл. 2.3.5 ровно по одной букве, находим осмысленное сообщение «НАШКОРРЕСПОНДЕНТ», которое и является искомым. При этом ключевая последовательность «ГБВГБВБГБВВГБВБГ» не является периодической.

Можно было найти также «НАШМОРОЗПОНОГЕМУ». Если предположить искажение в зашифрованном сообщении (в качестве 11-й буквы была бы принята не «Р», а «П»), то получим «НАШМОРОЗПОМОГЕМУ». Вообще число всех различных вариантов сообщений без ограничений на осмысленность равно 3^{16}, или 43046721, т. е. более 40 млн.

Таким образом, исходным является сообщение

НАШКОРРЕСПОНДЕНТ.

Задачи

1. Подобрав ленту (полоску бумаги) соответствующей длины и ширины и цилиндр соответствующего диаметра, составить, зашифровать и расшифровать текст из 32 букв, применяя шифр «сцитала».

2. Изготовив трафарет из прямоугольного листа клетчатой бумаги размером 8×6 клеток и вырезав в трафарете 12 клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывали бы всю площадь листа, составить, зашифровать и расшифровать текст из 48 букв, применяя шифр «поворотная решетка».

3. Составив текст из 80 букв и ключевое слово из 10 букв, зашифровать и расшифровать текст с помощью шифра «вертикальная перестановка».

4. Зашифровывание сообщения на русском языке в алфавите из 31 буквы (без букв «Ё», «Й», «Ъ» и с добавлением в конце алфавита знака пробел « ») осуществляется при помощи шифра Виженера. Дешифровать криптограмму «РБЫВЛРУСЗФРРРРЕЗРУ», если известно, что ключевая последовательность не содержит никаких букв, кроме «Б», «В», «Г», имеет период 3 и на любом отрезке длиной 3 все буквы различны. Указание: использовать метод решения примера 3, причем количество всех различных вариантов ключевых периодических последовательностей здесь равно $3! = 6$.

Ответы

4. «НАШ КОРРЕСПОНДЕНТ», ключевая последовательность – «ГБВ».

Глава 3. Элементы теории групп

§3.1. Понятие алгебраической системы. Группы и их свойства. Подгруппы

Определение 3.1.1. Пусть X – непустое множество. *Бинарной алгебраической операцией* на множестве X называется всякое правило f, по которому каждой упорядоченной паре (x, y) элементов $x, y \in X$ ставится в соответствие один вполне определенный элемент z из X. Таким образом, бинарная алгебраическая операция – это функция $f: X^2 \to X$, где $f: (x, y) \mapsto z$.

Аналогично можно определить n-арную алгебраическую операцию для любого $n \in \mathbf{N}$. В дальнейшем будем рассматривать только бинарные алгебраические операции. Обычно для обозначения операций используются знаки $*$, $\times$, $\bullet$, $\circ$, $+$ и т. п. Воспользуемся первым из обозначений, тогда в определении 3.1.1 $z = x * y$.

Определение 3.1.2. Если на множестве X задана одна или несколько алгебраических операций, то говорят, что X есть *алгебраическая система с данными операциями*. Алгебраические системы различают по количеству и свойствам операций. Алгебраическая система $(X, *)$ на множестве X с одной бинарной алгебраической операцией $*$ называется *группоидом*. Если у группоида $(X, *)$ операция $*$ ассоциативна: $a * (b * c) = (a * b) * c$ для любых $a, b, c \in X$, то такую алгебраическую систему называют *полугруппой*. *Моноидом* $(X, *)$ называют полугруппу с *единицей*, или *нейтральным элементом*, т. е. таким элементом $e \in X$, что $e * a = a * e = a$ для каждого $a \in X$. Моноид $(X, *)$, у которого каждый элемент обратим, т. е. для всякого $a \in X$ существует *обратный элемент* $a^{-1} \in X$, такой, что $a * a^{-1} = a^{-1} * a = e$, называется *группой*.

Из определения 3.1.2 нейтрального элемента следует его единственность в моноиде. Из ассоциативности операции $*$ и определения 3.1.2 следует, что обратный элемент в группе $(X, *)$ – единственный для каждого $x \in X$. Из определения 3.1.2 вытекает следующее независимое определение группы.

Определение 3.1.3. *Группой* называется непустое множество G с определенной на нем бинарной алгебраической операцией $\bullet$, которая обладает следующими свойствами:

1) ассоциативности – $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ для любых $a, b, c \in G$;

2) существования нейтрального элемента, т. е. такого элемента $e \in G$, что $a \bullet e = e \bullet a = a$ для каждого $a \in G$;

3) наличия для каждого элемента $a \in G$ обратного, т. е. такого элемента $a^{-1} \in G$, что $a \bullet a^{-1} = a^{-1} \bullet a = e$.

Знак «$\bullet$» групповой операции, как и знак умножения, в записи можно опускать для сокращения.

Определение 3.1.4. *Абелевой*, или *коммутативной*, называется группа $(G, \bullet)$ со свойством $a \bullet b = b \bullet a$ для произвольных $a, b \in G$. В противном случае группа называется *неабелевой*, или *некоммутативной*.

Определение 3.1.5. Группа относительно операции сложения называется *аддитивной группой*. Нейтральный элемент аддитивной группы называют *нулем* и обозначают символом 0, а обратный элемент для элемента a – *противоположным* и обозначают $-a$. Группа относительно операции умножения называется *мультипликативной группой*. Нейтральный элемент мультипликативной группы называют *единицей* и часто обозначают символом 1, а обратный элемент для элемента a обозначают a^{-1}.

Пусть K – одно из множеств $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ или $\mathbf{Z}/k\mathbf{Z}$ при любом $k \in \mathbf{N}$. *Полной линейной группой* $GL_n(K)$ (англ. *general linear group* – полная линейная группа) называется группа всех квадратных матриц порядка $n \in \mathbf{N}$ с элементами из K и ненулевыми определителями (или обратимыми определителями в случае $\mathbf{Z}/k\mathbf{Z}$) относительно операции матричного умножения. Группа $GL_n(K)$ является неабелевой мультипликативной группой при $n \geq 2$ и $k \geq 2$, т. к. произведение матриц некоммутативно в общем случае.

Определение 3.1.6. Группа $(G, \bullet)$ называется *конечной*, если G – конечное множество, в противном случае – *бесконечной*. *Порядком* конечной группы $|G|$ называется мощность множества G.

Алгебраическая операция в конечной группе может быть задана таблицей Кэли.

Определение 3.1.7. *Подгруппа* группы $(G, \bullet)$ – это непустое подмножество H множества G, которое в свою очередь является группой относительно той же бинарной алгебраической операции. Этот факт обозначают так: $H \leq G$ или $H < G$, если $H \subset G$.

Теорема 3.1.1 (критерий подгруппы). *Непустое подмножество H группы $(G, \bullet)$ является подгруппой тогда и только тогда, когда для произвольных $a, b \in H$ выполняется условие $a \bullet b^{-1} \in H$.*

Очевидно, что $G \leq G$ для произвольной группы $(G, \bullet)$, а также подмножество $\{e\}$, состоящее из одного нейтрального элемента e этой группы, является подгруппой.

Определение 3.1.8. Подгруппа H группы G называется *собственной* (или *нетривиальной*), если $H \neq G$ и $H \neq \{e\}$.

Пусть K – одно из множеств $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ или $\mathbf{Z}/k\mathbf{Z}$ при любом $k \in \mathbf{N}$. *Специальной линейной группой* $SL_n(K)$ (англ. *special linear group* – специальная линейная группа) называется группа всех квадратных матриц порядка $n \in \mathbf{N}$ с элементами из K и определителем, равным 1 $\left(\text{или } \bar{1} \text{ в случае } \mathbf{Z}/k\mathbf{Z}\right)$, относительно операции матричного умножения. С помощью критерия подгруппы легко убедиться в том, что $SL_n(K) < GL_n(K)$ при $K \neq \mathbf{Z}$, $K \neq \mathbf{Z}/\mathbf{Z}$ и $K \neq \mathbf{Z}/2\mathbf{Z}$, но $SL_n(\mathbf{Z}) < GL_n(\mathbf{Q})$ и $SL_n(\mathbf{Z}/k\mathbf{Z}) = GL_n(\mathbf{Z}/k\mathbf{Z})$ при $k \leq 2$.

Теорема 3.1.2. *Пусть a – любой фиксированный элемент произвольной группы G, $H = \{a^z \mid z \in \mathbf{Z}\}$ – множество всевозможных целых степеней элемента a. Тогда H – подгруппа группы G, причем абелева.*

Определение 3.1.9. Подгруппа H из теоремы 3.1.2 называется *циклической подгруппой, порожденной элементом a*, и обозначается $< a >$. Если найдется $b \in G$, такой, что $G = < b >$, то такую группу называют *циклической*, а b – ее *образующим элементом*.

Определение 3.1.10. Пусть e – нейтральный элемент группы. Элемент группы a называется *элементом бесконечного порядка*, если $a^k \neq e$ для любого $k \in \mathbf{N}$. Элемент a называется *элементом конечного порядка* $n \in \mathbf{N}$, если $a^n = e$, но $a^k \neq e$ для любого $k \in \mathbf{N}_{<n}$. Будем обозначать $\mathrm{ord}(a)$ порядок элемента a (англ. *order* – порядок). Очевидно, что в любой группе $\mathrm{ord}(e) = 1$.

Теорема 3.1.3. *Пусть элемент $a \in G$ обладает свойством* $\mathrm{ord}(a) = n$ *для некоторого $n \in \mathbf{N}$. Тогда $< a > = \{a, a^2, \ldots, a^n = e\}$ – циклическая подгруппа группы G, имеющая порядок n.*

Теорема 3.1.4. *Всякая подгруппа циклической группы является циклической.*

Примеры

1. Какую алгебраическую систему (группоид, полугруппу, моноид, группу) образует заданное множество относительно указанной операции? Определить, является ли алгебраическая система абелевой:

а) $T = \left\{ \dfrac{m}{2^k} \;\middle|\; m \in \mathbf{Z},\ k \in \mathbf{Z}_{\geq 0} \right\}$ относительно обычной операции сложения в $\mathbf{Q}$.

$T = \left\{ \dfrac{m}{2^k} \;\middle|\; m \in \mathbf{Z},\ k \in \mathbf{Z}_{\geq 0} \right\} \subset \mathbf{Q}$. Алгебраическая система $(\mathbf{Q}, +)$, как несложно проверить, – абелева группа. Проверим по критерию подгруппы (теорема 3.1.1) для аддитивной группы, будет ли $(T, +)$ подгруппой $(\mathbf{Q}, +)$.

Рассмотрим произвольные $m_1, m_2 \in \mathbf{Z}$, $k_1, k_2 \in \mathbf{Z}_{\geq 0}$. Пусть $k_{\max} = \max\{k_1, k_2\}$. Тогда

$$\frac{m_1}{2^{k_1}} - \frac{m_2}{2^{k_2}} = \frac{2^{k_{\max} - k_1} m_1 - 2^{k_{\max} - k_2} m_2}{2^{k_{\max}}} \in T,$$

т. к. $2^{k_{\max} - k_1} m_1 - 2^{k_{\max} - k_2} m_2 \in \mathbf{Z}$, $k_{\max} \in \mathbf{Z}_{\geq 0}$.

Итак, $T < \mathbf{Q} \Rightarrow (T, +)$ – абелева группа, как подгруппа абелевой группы. Доказательство можно было также провести, непосредственно проверив определения 3.1.1–3.1.4.

б) Булеан $P(V)$, где $V \neq \varnothing$, относительно операции пересечения множеств.

Проверим определения 3.1.1–3.1.4:

1) $A \cap B \subseteq V$, $\forall A, B \subseteq V$, следовательно, определена бинарная алгебраическая операция на множестве $P(V)$;

2) $(A \cap B) \cap C = A \cap (B \cap C)$, $\forall A, B, C \subseteq V$, – операция ассоциативна;

3) $A \cap V = V \cap A = V$, $\forall A \subseteq V$, значит, V – нейтральный элемент;

4) для любого ли $A \subseteq V$ найдется обратный элемент $A^{-1} \subseteq V$ со свойством $A \cap A^{-1} = A^{-1} \cap A = V$? Но если $A \subset V$, т. е. $A \neq V$, то $A \cap B \subseteq A \subset V$ и $A \cap B \neq V$, $\forall\, B \subseteq V$, значит, нет обратных элементов у элементов из $P(V)$, отличных от V;

5) $A \cap B = B \cap A$, $\forall\, A, B \subseteq V$, – операция коммутативна.

Итак, $(P(V), \cap)$ – абелев моноид, но не группа.

2. Пусть $(G, \bullet)$ – группа. Доказать, что если $a^2 = a \bullet a = e$ для любого $a \in G$, то G – абелева группа.

Рассмотрим произвольные $a, b \in G$. Тогда

$$(a \bullet b) \bullet (b \bullet a) = a \bullet (b \bullet b) \bullet a = a \bullet e \bullet a = a \bullet a = e,$$
$$(b \bullet a) \bullet (a \bullet b) = b \bullet (a \bullet a) \bullet b = b \bullet e \bullet b = b \bullet b = e,$$

т. е. $(a \bullet b)^{-1} = b \bullet a$, но, с другой стороны, $(a \bullet b)^{-1} = a \bullet b$ по свойству данной группы. Итак, $a \bullet b = b \bullet a$ для любых $a, b \in G \Rightarrow G$ – абелева группа.

3. Установить, является ли H подгруппой группы G:

а) $(G, \bullet)$ – абелева группа, $H = \{ a^2 = a \bullet a \mid a \in G \}$.

Рассмотрим произвольные $a^2, b^2 \in H$. Тогда

$a^2 \bullet (b^2)^{-1} = (a \bullet a) \bullet (b \bullet b)^{-1} = (a \bullet a) \bullet (b^{-1} \bullet b^{-1}) = (a \bullet b^{-1}) \bullet (a \bullet b^{-1})$ – элемент H, поскольку $a \bullet b^{-1} \in G$.

Итак, по критерию подгруппы (теорема 3.1.1) H – подгруппа группы G.

б) $H_1 \leq G$, $H_2 \leq G$, $H = H_1 \backslash H_2$.

Пусть H_1, H_2 – подгруппы группы G, тогда $e \in H_1 \cap H_2$, где e – нейтральный элемент группы G. Но $e \notin H_1 \backslash H_2 \Rightarrow H_1 \backslash H_2$ – не подгруппа группы G, т. к. любая подгруппа содержит нейтральный элемент группы, который является также нейтральным элементом подгруппы.

в) $(G, \bullet)$ – группа, $H_1 \leq G$, $H_2 \leq G$, $H = \{ h_1 \bullet h_2 \mid h_1 \in H_1, h_2 \in H_2 \}$.

Для всех $h_1 \bullet h_2 \in H$ справедливо $(h_1 \bullet h_2)^{-1} = h_2^{-1} \bullet h_1^{-1}$, где $h_1^{-1} \in H_1$, $h_2^{-1} \in H_2$. Для любых $g_1, h_1 \in H_1$, $g_2, h_2 \in H_2$ имеем $g_1 \bullet h_1^{-1} \in H_1$, $g_2 \bullet h_2^{-1} \in H_2$ по теореме 3.1.1.

Если $(G, \bullet)$ – абелева группа, то $H \leq G$ согласно теореме 3.1.1, т. к. для любых $g_1 \bullet g_2$, $h_1 \bullet h_2 \in H$ выполняется

$$(g_1 \bullet g_2) \bullet (h_1 \bullet h_2)^{-1} = (g_1 \bullet g_2) \bullet (h_2^{-1} \bullet h_1^{-1}) = (g_1 \bullet h_1^{-1}) \bullet (g_2 \bullet h_2^{-1}) \in H.$$

Теперь рассмотрим пример неабелевой группы. Пусть

$$G = SL_2(\mathbf{R}),\ H_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \mathbf{R} \right\},\ H_2 = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \,\middle|\, b \in \mathbf{R} \right\}.$$

$$\begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 - a_2 \\ 0 & 1 \end{pmatrix} \in H_1,\ \forall\, a_1, a_2 \in \mathbf{R},\ \text{значит, } H_1 < G.$$

$$\begin{pmatrix} 1 & 0 \\ b_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b_2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ b_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b_2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b_1 - b_2 & 1 \end{pmatrix} \in H_2,\ \forall\, b_1, b_2 \in \mathbf{R},\ \text{значит, } H_2 < G.$$

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix} \,\middle|\, a, b \in \mathbf{R} \right\}.$$

Таким образом, у любой матрицы C из множества H элемент $c_{22} = 1$.

$$\begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ -b & ab+1 \end{pmatrix},$$

и если $H < G$, то должно быть $ab + 1 = 1$ для всех $a, b \in \mathbf{R}$. Но если $ab \neq 0$, т. е. $a \neq 0$ и $b \neq 0$, то $ab + 1 \neq 1$ и получаем, что в этом случае $\begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}^{-1} \notin H$. Поэтому в данном примере H – не подгруппа группы G.

Значит, H – не подгруппа группы G в общем случае.

4. Доказать, что любая бесконечная группа имеет бесконечное множество подгрупп.

1) Если $\text{ord}(a) \in \mathbf{N}$ для любого $a \in G$, то можно рассмотреть $< a >$, причем взять все различные циклические подгруппы. Таких подгрупп будет бесконечно много, иначе G была бы конечна, т. к. G представляет собой объединение всех таких подгрупп. Поэтому G содержит бесконечно много подгрупп.

2) В группе G есть элемент a бесконечного порядка. Тогда можно рассмотреть подгруппы $< a >, < a^2 >, < a^3 >, \ldots, < a^n >, \forall\, n \in \mathbf{N}$. Таких подгрупп бесконечно много, т. к. если $(m, n) = 1$, то $< a^m > \neq < a^n >$, поскольку $a^n \notin < a^m >$ и $a^m \notin < a^n >$. Поэтому G содержит бесконечно много подгрупп.

5. Найти все подгруппы циклической группы порядка $n \in \mathbf{N}$ и указать их включения. Решить задачу для заданных ниже значений порядка n.

Все подгруппы циклической группы $< a >$ являются циклическими (теорема 3.1.4) и имеют вид $H_k = < a^m >$, где $1 \leq m \leq n$, $a^n = e$. Согласно теореме 3.1.3 $|H_k| = \text{ord}(a^m) = k$. Согласно определению 3.1.10 порядка элемента группы $\text{ord}(a^m) = n/(m, n)$, откуда $(m, n) = n/k \Leftrightarrow (s_m, k) = 1$, где $s_m = m/(m, n)$, $1 \leq s_m \leq k$, по свойству 1 взаимно простых чисел. Поэтому группа $< a >$ содержит единственную подгруппу $H_k = \{a^{n/k}, \ldots, a^{k(n/k)} = e\} = < a^{n/k} >$ фиксированного порядка k, где $k \mid n$. При $k > 1$ количество образующих элементов в H_k равно $\varphi(k)$, где φ – функция Эйлера. Согласно определению 3.1.9 циклической подгруппы и теореме 3.1.3 $< a^m > \subseteq < a^l > \Leftrightarrow l \mid m$.

а) $n = 6$.

В данном случае $< a > = \{a, a^2, a^3, a^4, a^5, e\}$, k может принимать значения 1, 2, 3, 6. Тогда получаем следующие 4 подгруппы группы $< a >$:

$k = 1 = |H_1| \Rightarrow H_1 = \{e\} = < e >$;

$k = 2 = |H_2| \Rightarrow H_2 = \{a^3, e\} = < a^3 >$, т. к. $(3, 6) = 6/2 = 3$;

$k = 3 = |H_3| \Rightarrow H_3 = \{a^2, a^4, e\} = < a^2 > = < a^4 >$, т. к. $(2, 6) = (4, 6) = 6/3 = 2$;

$k = 6 = |H_6| \Rightarrow H_6 = \{a, a^2, a^3, a^4, a^5, e\} = < a > = < a^5 >$, т. к. $(1, 6) = (5, 6) = 6/6 = 1$.

Имеем следующую схему включений подгрупп:

$$\begin{array}{ccc} < e > & \subset & < a^3 > \\ \cap & & \cap \\ < a^2 > & \subset & < a > \end{array}$$

б) $n = 24$.

В данном случае $< a > = \{a, a^2, a^3, \ldots, a^{23}, e\}$, k может принимать значения 1, 2, 3, 4, 6, 8, 12, 24. Тогда получаем следующие 8 подгрупп группы $< a >$:

$k = 1 = |H_1| \Rightarrow H_1 = \{e\} = < e >$;

$k = 2 = |H_2| \Rightarrow H_2 = \{a^{12}, e\} = < a^{12} >$, т. к. (12, 24) = 24/2 = 12;

$k = 3 = |H_3| \Rightarrow H_3 = \{a^8, a^{16}, e\} = < a^8 > = < a^{16} >$, потому что (8, 24) = (16, 24) = = 24/3 = 8;

$k = 4 = |H_4| \Rightarrow H_4 = \{a^6, a^{12}, a^{18}, e\} = < a^6 > = < a^{18} >$, т. к. (6, 24) = (18, 24) = = 24/4 = 6;

$k = 6 = |H_6| \Rightarrow H_6 = \{a^4, a^8, a^{12}, a^{16}, a^{20}, e\} = < a^4 > = < a^{20} >$, т. к. (4, 24) = = (20, 24) = 24/6 = 4;

$k = 8 = |H_8| \Rightarrow H_8 = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, e\} = < a^3 > = < a^9 > = < a^{15} > = = < a^{21} >$, т. к. (3, 24) = (9, 24) = (15, 24) = (21, 24) = 24/8 = 3;

$k = 12 = |H_{12}| \Rightarrow H_{12} = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}, e\} = < a^2 > = = < a^{10} > = < a^{14} > = < a^{22} >$, потому что (2, 24) = (10, 24) = (14, 24) = (22, 24) = 24/12 = 2;

$k = 24 = |H_{24}| \Rightarrow H_{24} = \{a, a^2, a^3, \ldots, a^{23}, e\} = < a > = < a^5 > = < a^7 > = < a^{11} > = = < a^{13} > = < a^{17} > = < a^{19} > = < a^{23} >$, т. к. (1, 24) = (5, 24) = (7, 24) = (11, 24) = (13, 24) = = (17, 24) = (19, 24) = (23, 24) = 24/24 = 1.

Имеем следующую схему включений подгрупп:

$$\begin{array}{ccccccc} < e > & \subset & < a^{12} > & \subset & < a^6 > & \subset & < a^3 > \\ \cap & & \cap & & \cap & & \cap \\ < a^8 > & \subset & < a^4 > & \subset & < a^2 > & \subset & < a > \end{array}$$

Задачи

1. Какую алгебраическую систему (группоид, полугруппу, моноид, группу) образует заданное множество относительно указанной операции? Определить, является ли алгебраическая система абелевой:

а) $\mathbf{R}_{>0}$ относительно операции $*$, где $a * b = a^2 \cdot b^2$, «·» – знак умножения в **R**;

б) **Z** относительно операции $*$, где $a * b = a + b + a \cdot b$, где «+» и «·» – знаки сложения и умножения в **Z** соответственно.

2. Найти все подгруппы циклической группы $< a >$ порядка n и указать их включения:

а) $n = 7$; **б)** $n = 12$.

Ответы

1. а) абелев группоид; **б)** абелев моноид. **2. а)** $H_1 = \{e\} = < e >$, $H_7 = \{a, a^2, a^3, a^4, a^5, a^6, e\} = < a > = < a^2 > = < a^3 > = < a^4 > = < a^5 > = < a^6 >$; $< e > \subset < a >$; **б)** $H_1 = \{e\} = = < e >$, $H_2 = \{a^6, e\} = < a^6 >$, $H_3 = \{a^4, a^8, e\} = < a^4 > = < a^8 >$, $H_4 = \{a^3, a^6, a^9, e\} = = < a^3 > = < a^9 >$, $H_6 = \{a^2, a^4, a^6, a^8, a^{10}, e\} = < a^2 > = < a^{10} >$, $H_{12} = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, e\} = < a > = < a^5 > = < a^7 > = < a^{11} >$. Схема включений:

$$\begin{array}{ccccc} < e > & \subset & < a^6 > & \subset & < a^3 > \\ \cap & & \cap & & \cap \\ < a^4 > & \subset & < a^2 > & \subset & < a > \end{array}$$

§3.2. Смежные классы. Нормальные подгруппы. Факторгруппы

Определение 3.2.1. Пусть H – подгруппа группы G и $a \in G$. Множество элементов $\{a \bullet h \mid h \in H\}$ обозначим aH и назовем *левым смежным классом* группы G по подгруппе H. Элемент a называется *представителем левого смежного класса* aH. Аналогично определяется *правый смежный класс* $Ha = \{h \bullet a \mid h \in H\}$ с представителем $a \in G$.

Теорема 3.2.1. *Пусть H – подгруппа группы G. Тогда справедливы следующие утверждения*:

1) *каждый элемент $a \in G$ принадлежит какому-нибудь левому* (*правому*) *смежному классу по подгруппе H*;

2) *два элемента $a, b \in G$ принадлежат одному левому* (*правому*) *смежному классу тогда и только тогда, когда $a^{-1} \bullet b \in H$ $(b \bullet a^{-1} \in H)$*;

3) *любые два левых* (*правых*) *смежных класса либо не пересекаются, либо совпадают*;

4) *G есть объединение попарно непересекающихся левых* (*правых*) *смежных классов по подгруппе H.*

Определение 3.2.2. Мощность множества всех различных левых (правых) смежных классов группы G по подгруппе H называется *индексом* подгруппы H в группе G и обозначается $[G : H]$.

Теорема 3.2.2 (Ж. Лагранж). *Порядок конечной группы равен произведению порядка и индекса любой ее подгруппы*.

Следствие 1. *Порядок конечной группы делится на порядок любой ее подгруппы*.

Следствие 2. *Если G – конечная группа порядка n, то порядок любого элемента группы делит порядок группы и $a^n = e$ для каждого $a \in G$.*

Следствие 3. *Любая группа простого порядка является циклической и не содержит собственных подгрупп*.

Определение 3.2.3. Подгруппа H группы G называется *нормальной*, если $aH = Ha$ для всякого $a \in G$, т. е. каждый левый смежный класс по подгруппе H совпадает с правым смежным классом с тем же представителем. В этом случае используется обозначение $H \lhd G$.

Ясно, что у абелевых групп все подгруппы нормальны.

В любой группе $(G, \bullet)$ тривиальные подгруппы $\{e\}$ и G являются нормальными, т. к. для любого $a \in G$ справедливо $a\{e\} = \{a\} = \{e\}a$ и $aG = G = Ga$. Итак, $\{e\} \lhd G$ и $G \lhd G$.

Теорема 3.2.3 (критерий нормальной подгруппы). *$H \lhd G$ тогда и только тогда, когда $aHa^{-1} = H$ для каждого $a \in G$ $(a \bullet h \bullet a^{-1} \in H, \forall\, a \in G, \forall\, h \in H)$.*

Определение 3.2.4. Пусть $(G, \bullet)$ – группа и H – ее нормальная подгруппа. Множество $\{H, aH, bH, \ldots\}$ всех левых или, что то же самое, правых смежных классов (в этом случае будем говорить просто «смежных классов») называется *фактормножеством* группы G по подгруппе H и обозначается G/H.

Теорема 3.2.4. *Пусть* $(G, \bullet)$ *– группа и* $H \lhd G$. *Тогда факторможество* G/H *является группой относительно индуцированной операции, определенной формулой*

$$aH \odot bH = (a \bullet b)H$$

для любых $a, b \in G$.

Определение 3.2.5. Группа $(G/H, \odot)$ из теоремы 3.2.4 называется *факторгруппой* группы G по нормальной подгруппе H.

Свойства факторгрупп:

1. Факторгруппа абелевой группы является абелевой.

2. Факторгруппа циклической группы является циклической.

Примеры

1. Найти все левые и правые смежные классы:

а) Группы $(\mathbf{R}, +)$ по подгруппе $(\mathbf{Z}, +)$.

$(\mathbf{Z}, +) < (\mathbf{R}, +)$ согласно определению 3.1.7 подгруппы. Поскольку $(\mathbf{R}, +)$ – абелева группа, то ее левые смежные классы по подгруппе $(\mathbf{Z}, +)$ совпадают с правыми для одинаковых представителей. Пусть $\{r\}$ обозначает дробную часть $r \in \mathbf{R}$. Тогда для любого $r \in \mathbf{R}$ справедливо представление $r = [r] + \{r\}$, где $[r] \in \mathbf{Z}$, $0 \le \{r\} < 1$. Поэтому $r \in \{r\} + \mathbf{Z}$, где $\{r\} + \mathbf{Z} = \{\{r\} + z \mid z \in \mathbf{Z}\}$ – левый и одновременно правый смежный класс группы $(\mathbf{R}, +)$ по подгруппе $(\mathbf{Z}, +)$ с представителем $\{r\}$.

Пусть $\{r_1\} \ne \{r_2\}$, тогда $(\{r_1\} + \mathbf{Z}) \cap (\{r_2\} + \mathbf{Z}) = \varnothing$. Иначе бы нашлись $m_1, m_2 \in \mathbf{Z}$, такие, что $\{r_1\} + m_1 = \{r_2\} + m_2$, откуда $\{r_1\} - \{r_2\} = m_2 - m_1$, что невозможно, поскольку $\{r_1\} - \{r_2\} \notin \mathbf{Z}$, а $m_2 - m_1 \in \mathbf{Z}$.

Поэтому представителями всех различных левых (правых) смежных классов являются все значения $\{r\}$. Итак, $\mathbf{R} = \bigcup\limits_{0 \le \{r\} < 1} (\{r\} + \mathbf{Z})$.

б) Группы $(\mathbf{C}^*, \cdot)$ по подгруппе $H = \{h \in \mathbf{C}^* \mid |h| = 1\}$.

Здесь и далее A^* обозначает множество всех обратимых элементов относительно некоторой бинарной алгебраической операции, заданной на множестве A. Поэтому $\mathbf{C}^* = \mathbf{C} \backslash \{0\}$, т. е. множество всех комплексных чисел, обратимых относительно операции умножения. По критерию подгруппы (теорема 3.1.1) несложно показать, что $H < \mathbf{C}^*$. Поскольку $(\mathbf{C}^*, \cdot)$ – абелева группа, то ее левые смежные классы по подгруппе $(H, \cdot)$ совпадают с правыми для одинаковых представителей.

Для любого $u \in \mathbf{C}^*$ справедливо представление $u = |u| e^{i\phi}$, где $|u| \in \mathbf{R}_{>0}$, $|e^{i\phi}| = 1$, – показательная форма записи. Несложно видеть, что $H = \{e^{i\phi} \mid 0 \le \phi < 2\pi\}$, здесь ϕ обозначает главное значение аргумента комплексного числа. Поэтому $u \in |u|H$, где $|u|H = \{|u| e^{i\phi} \mid 0 \le \phi < 2\pi\}$ – левый и одновременно правый смежный класс группы $(\mathbf{C}^*, \cdot)$ по подгруппе $(H, \cdot)$ с представителем $|u|$.

Очевидно, что при $|u_1| \ne |u_2|$ имеем $|u_1|H \cap |u_2|H = \varnothing$. Геометрическое изображение на комплексной плоскости подгруппы H и левого (одновременно правого) смежного класса $|u|H$ при $|u| > 1$ представлено на рис. 3.2.1.

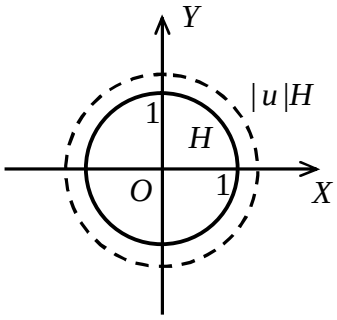

Рис. 3.2.1

Таким образом, представителями всех различных левых (правых) смежных классов являются все значения $|u|$, и $\mathbf{C}^* = \bigcup\limits_{|u|>0} |u|H$.

2. Установить, может ли H быть подгруппой группы G, если $|G| = 2000$, $|H| = 127$.

Согласно следствию 1 из теоремы 3.2.2 Лагранжа должно выполняться соотношение $|H| \,|\, |G|$. Так как $127 \nmid 2000$, то H подгруппой группы G быть не может.

3. Доказать, что $H \lhd G$:

а) H – произвольная подгруппа индекса 2 группы G.

Поскольку $H \cap gH = H \cap Hg = \varnothing$ и $G = H \cup gH = H \cup Hg$ для любого $g \in G \backslash H$ согласно утверждениям 3 и 4 теоремы 3.2.1, следовательно, $gH = Hg$ и, таким образом, $aH = Ha$ для любого $a \in G$, что означает $H \lhd G$ по определению 3.2.3.

б) $H = \{h \in G \mid a \bullet h = h \bullet a, \forall\, a \in G\}$. Множество H называется *центром группы* G.

$H \neq \varnothing$, поскольку $e \in H$. Докажем, что $H \leq G$ по критерию подгруппы (теорема 3.1.1). Возьмем произвольные $h_1, h_2 \in H$ и $a \in G$. Тогда

$$a \bullet (h_1 \bullet h_2^{-1}) = (a \bullet h_1) \bullet h_2^{-1} = (h_1 \bullet a) \bullet h_2^{-1} = h_1 \bullet (a \bullet h_2^{-1}) = h_1 \bullet (h_2 \bullet a^{-1})^{-1} =$$
$$= h_1 \bullet (a^{-1} \bullet h_2)^{-1} = h_1 \bullet (h_2^{-1} \bullet a) = (h_1 \bullet h_2^{-1}) \bullet a.$$

Значит, $h_1 \bullet h_2^{-1} \in H$.

Для любого $a \in G$ рассмотрим левый и правый смежные классы с этим представителем. Так, $aH = \{a \bullet h \mid h \in H\}$, но $a \bullet h = h \bullet a$, $\forall\, h \in H$, значит, $aH = \{h \bullet a \mid h \in H\} = Ha$. По определению 3.2.3 нормальной подгруппы $H \lhd G$.

4. $A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \in GL_2(\mathbf{Z}/3\mathbf{Z})$. Определить $\mathrm{ord}(A)$ в $GL_2(\mathbf{Z}/3\mathbf{Z})$, построить $< A >$. Является ли $< A >$ нормальной подгруппой в $GL_2(\mathbf{Z}/3\mathbf{Z})$?

Единичную квадратную матрицу порядка $n \in \mathbf{N}$ здесь и далее будем обозначать E_n. В данном случае $E_2 = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$.

$$A \neq E_2,\ A^2 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix},\ A^3 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{0} \end{pmatrix},$$

$$A^4=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar2\end{pmatrix}\begin{pmatrix}\bar2 & \bar2\\ \bar2 & \bar0\end{pmatrix}=\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar2\end{pmatrix},\ A^8=(A^4)^2=\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar2\end{pmatrix}\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar2\end{pmatrix}=\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar1\end{pmatrix}=E_2.$$

Если $\operatorname{ord}(A)<8$, например $\operatorname{ord}(A)=5, 6, 7$, то по определению 3.1.10 должно быть $8\vdots\operatorname{ord}(A)$, но $8\not\vdots 5, 6, 7$. Поэтому $\operatorname{ord}(A)=8$.

$$A^5=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar2\end{pmatrix}\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar2\end{pmatrix}=\begin{pmatrix}\bar0 & \bar2\\ \bar2 & \bar1\end{pmatrix},\ A^6=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar2\end{pmatrix}\begin{pmatrix}\bar0 & \bar2\\ \bar2 & \bar1\end{pmatrix}=\begin{pmatrix}\bar2 & \bar1\\ \bar1 & \bar1\end{pmatrix},\ A^7=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar2\end{pmatrix}\begin{pmatrix}\bar2 & \bar1\\ \bar1 & \bar1\end{pmatrix}=\begin{pmatrix}\bar1 & \bar1\\ \bar1 & \bar0\end{pmatrix}.$$

Итак, $<A>=\{A, A^2, A^3, A^4, A^5, A^6, A^7, E_2\}$.

Рассмотрим матрицу $B=\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar2\end{pmatrix}\in GL_2(\mathbf{Z}/3\mathbf{Z})$, $B\notin<A>$. Тогда

$$B^{-1}=\bar2^{-1}\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar1\end{pmatrix}=\bar2\begin{pmatrix}\bar2 & \bar0\\ \bar0 & \bar1\end{pmatrix}=\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar2\end{pmatrix}=B,$$

$$BAB^{-1}=\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar2\end{pmatrix}\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar2\end{pmatrix}\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar2\end{pmatrix}=\begin{pmatrix}\bar0 & \bar1\\ \bar2 & \bar1\end{pmatrix}\begin{pmatrix}\bar1 & \bar0\\ \bar0 & \bar2\end{pmatrix}=\begin{pmatrix}\bar0 & \bar2\\ \bar2 & \bar2\end{pmatrix}\notin<A>.$$

Значит, $<A>$ не является нормальной подгруппой $GL_2(\mathbf{Z}/3\mathbf{Z})$ согласно критерию нормальной подгруппы (теорема 3.2.3).

5. Построить факторгруппу, описать ее свойства, задать индуцированную операцию таблицей Кэли:

а) Группы $(3\mathbf{Z}, +)$ по подгруппе $(15\mathbf{Z}, +)$.

$(\mathbf{Z}, +)$ – абелева группа. Так как $3\mathbf{Z}=\{3k \mid k\in\mathbf{Z}\}$, $15\mathbf{Z}=\{15l \mid l\in\mathbf{Z}\}$, то $15\mathbf{Z}\subset 3\mathbf{Z}$. Для всех $m, n\in\mathbf{Z}$ выполняется $3m, 3n\in 3\mathbf{Z}$ и $3m-3n=3(m-n)\in$ $\in 3\mathbf{Z}$, а также $15m, 15n\in 15\mathbf{Z}$ и $15m-15n=15(m-n)\in 15\mathbf{Z}$. Таким образом, согласно критерию подгруппы (теорема 3.1.1) имеем $15\mathbf{Z}<3\mathbf{Z}<\mathbf{Z}$. Группа $(3\mathbf{Z}, +)$, как подгруппа абелевой группы $(\mathbf{Z}, +)$, является абелевой, и любая ее подгруппа, в частности $(15\mathbf{Z}, +)$, нормальна.

Найдем фактормножество $3\mathbf{Z}/15\mathbf{Z}$. Для любого $3k\in 3\mathbf{Z}$ согласно теореме 1.1.1 справедливо представление $3k=15q+3r$, где $q, r\in\mathbf{Z}$, $15q\in 15\mathbf{Z}$, $0\le 3r<15$, т. е. $3r$ может принимать значения 0, 3, 6, 9 и 12. Поэтому $3k\in 3r+15\mathbf{Z}=\overline{3r}$ – класс вычетов по модулю 15 с представителем $3r$. Поскольку классы вычетов $\bar0,\ \bar3,\ \bar6,\ \bar9,\ \overline{12}$ из $\mathbf{Z}/15\mathbf{Z}$ попарно не пересекаются и их объединение равно $3\mathbf{Z}$, то $3\mathbf{Z}/15\mathbf{Z}=\{15\mathbf{Z},$ $3+15\mathbf{Z}, 6+15\mathbf{Z}, 9+15\mathbf{Z}, 12+15\mathbf{Z}\}=\{\bar0,\ \bar3,\ \bar6,\ \bar9,\ \overline{12}\}$.

Согласно свойствам 1 и 2 факторгрупп $(3\mathbf{Z}/15\mathbf{Z}, \oplus)$ – абелева и циклическая группа, поскольку $(3\mathbf{Z}, +)$ – абелева и циклическая группа. Так как $(3\mathbf{Z}/15\mathbf{Z}, \oplus)$ – подгруппа порядка 5 циклической группы $(\mathbf{Z}/15\mathbf{Z}, \oplus)$ порядка 15, то ее образующими являются те и только те классы вычетов $\overline{3r}$, для которых $\operatorname{ord}(\overline{3r})=5$, т. е. для которых $(3r, 15)=15/5=3\Leftrightarrow(r, 5)=1$. Значит, образующими элементами являются все ненулевые классы вычетов: $\bar3,\ \bar6,\ \bar9,\ \overline{12}$. Их количество равно $\varphi(5)=4$, где φ – функция Эйлера. Индуцированную операцию сложения смежных классов в $3\mathbf{Z}/15\mathbf{Z}$ можно задать таблицей Кэли как операцию сложения соответствующих классов вычетов в $\mathbf{Z}/15\mathbf{Z}$ (рис. 3.2.2).

$\oplus$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\overline{12}$
$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\overline{12}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\overline{12}$	$\bar{0}$
$\bar{6}$	$\bar{6}$	$\bar{9}$	$\overline{12}$	$\bar{0}$	$\bar{3}$
$\bar{9}$	$\bar{9}$	$\overline{12}$	$\bar{0}$	$\bar{3}$	$\bar{6}$
$\overline{12}$	$\overline{12}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$

Рис. 3.2.2

б) Группы $(\mathbf{R}^*, \cdot)$ по подгруппе $(\mathbf{R}_{>0}, \cdot)$.

Имеем $st^{-1} \in \mathbf{R}_{>0}$ для любых $s, t \in \mathbf{R}_{>0}$, следовательно, согласно критерию подгруппы (теорема 3.1.1) $\mathbf{R}_{>0} < \mathbf{R}^*$. Так как $(\mathbf{R}^*, \cdot)$ – абелева группа, то любая ее подгруппа, в частности $(\mathbf{R}_{>0}, \cdot)$, нормальна.

Найдем фактормножество $\mathbf{R}^*/\mathbf{R}_{>0}$. Для любого $r \in \mathbf{R}^*$ справедливо представление $r = |r|\mathrm{sgn}(r)$, где $|r| \in \mathbf{R}_{>0}$, а $\mathrm{sgn}(r)$ принимает значения ± 1 в зависимости от знака r, поэтому $r \in \mathrm{sgn}(r)\mathbf{R}_{>0}$; $(-1)\mathbf{R}_{>0} = \mathbf{R}_{<0}$. Поскольку $\mathbf{R}_{>0} \cap \mathbf{R}_{<0} = \varnothing$ и $\mathbf{R}_{>0} \cup \mathbf{R}_{<0} = \mathbf{R}^*$, то $\mathbf{R}^*/\mathbf{R}_{>0} = \{\mathbf{R}_{>0}, \mathbf{R}_{<0}\}$.

Согласно свойству 1 факторгрупп $(\mathbf{R}^*/\mathbf{R}_{>0}, \otimes)$ – абелева группа, т. к. $(\mathbf{R}^*, \cdot)$ – абелева группа. Согласно следствию 3 из теоремы 3.2.2 Лагранжа $(\mathbf{R}^*/\mathbf{R}_{>0}, \otimes)$ – циклическая группа, поскольку ее порядок равен 2 – простому числу. Отметим, что сама группа $(\mathbf{R}^*, \cdot)$ не является циклической. Индуцированная операция умножения смежных классов в $\mathbf{R}^*/\mathbf{R}_{>0}$ определяется умножением их представителей, т. е. 1 и –1, и может быть задана таблицей Кэли (рис. 3.2.3). Образующим элементом факторгруппы $(\mathbf{R}^*/\mathbf{R}_{>0}, \otimes)$ является смежный класс $\mathbf{R}_{<0}$; количество образующих равно $\varphi(2) = 1$, где φ – функция Эйлера.

$\otimes$	$\mathbf{R}_{>0}$	$\mathbf{R}_{<0}$
$\mathbf{R}_{>0}$	$\mathbf{R}_{>0}$	$\mathbf{R}_{<0}$
$\mathbf{R}_{<0}$	$\mathbf{R}_{<0}$	$\mathbf{R}_{>0}$

Рис. 3.2.3

Задачи

1. $A = \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in GL_3(\mathbf{Z}/2\mathbf{Z})$. Определить $\mathrm{ord}(A)$ в $GL_3(\mathbf{Z}/2\mathbf{Z})$, построить $< A >$. Является ли $< A >$ нормальной подгруппой в $GL_3(\mathbf{Z}/2\mathbf{Z})$?

2. Построить факторгруппу группы $(4\mathbf{Z}, +)$ по подгруппе $(24\mathbf{Z}, +)$, описать ее свойства, задать индуцированную операцию таблицей Кэли.

Ответы

1. ord(A) = 4; не является. **2.** $4\mathbf{Z}/24\mathbf{Z} = \{\bar{0},\ \bar{4},\ \bar{8},\ \overline{12},\ \overline{16},\ \overline{20}\} \subset \mathbf{Z}/24\mathbf{Z}$; абелева и циклическая группа, образующие: $\bar{4},\ \overline{20}$.

§3.3. Симметрические группы

Определение 3.3.1. Пусть Ω – конечное множество из n элементов для произвольного $n \in \mathbf{N}$. Поскольку природа элементов множества Ω для нас несущественна, удобно считать, что $\Omega = \{1, 2, \ldots, n\}$. Всякая биекция, т. е. взаимно однозначное преобразование Ω, называется *подстановкой* на множестве Ω. В развернутой и наглядной форме подстановку $f\colon i \mapsto f(i)$, $i = 1, 2, \ldots, n$, удобно изображать в виде двухстрочной таблицы. В этой таблице каждый i-й столбец четко указывает, в какой элемент $f(i)$ преобразуется элемент i, $1 \le i \le n$:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Композиция подстановок, как композиция биективных преобразований, является подстановкой. Подстановки перемножаются в соответствии с общим правилом композиции функций: $gf(i) = g(f(i))$, $i = 1, 2, \ldots, n$. В общем случае $fg \ne gf$, т. е. композиция подстановок не обладает свойством коммутативности. Очевидно, что роль нейтрального элемента относительно операции композиции играет тождественная подстановка $e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$. Как известно, композиция функций – ассоциативная операция, поэтому и композиция подстановок ассоциативна. Каждая подстановка – обратимая функция. Чтобы найти для подстановки f обратную подстановку f^{-1}, достаточно в таблице $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$ переставить строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки.

Определение 3.3.2. Группу всех подстановок на n-элементном множестве относительно операции композиции называют *симметрической группой степени n* и обозначают S_n. В общем случае множество всех биективных преобразований произвольного непустого множества Ω образует группу относительно операции композиции, обозначаемую $S(\Omega)$ и называемую *симметрической группой множества* Ω.

Теорема 3.3.1. *Порядок группы S_n равен* $n!$.

Определение 3.3.3. *Циклом длины* $k \ge 2$ в группе S_n называется подстановка

$$(i_1\, i_2 \ldots i_k) = \begin{pmatrix} i_1 & \ldots & i_{k-1} & i_k \\ i_2 & \ldots & i_k & i_1 \end{pmatrix},$$

действующая тождественно на множестве $\Omega \setminus \{i_1, i_2, \ldots, i_k\}$. Цикл (i) длины 1 является тождественной подстановкой e для любого $i \in \Omega$. Циклы называются *независимыми*, или *непересекающимися*, если они действуют на непересекающихся множествах.

Пусть f – произвольная подстановка из S_n. Цикл $f_k = (i\ f(i) \dots f^{k-1}(i))$ действует как подстановка f на $\Omega_k = \{i, f(i),\dots, f^{k-1}(i)\}$ и тождественно на $\Omega\backslash\Omega_k$. Независимые циклы f_k и f_m действуют как подстановка f на непересекающихся множествах Ω_k и Ω_m и тождественно на $\Omega\backslash\Omega_k$ и $\Omega\backslash\Omega_m$ соответственно. Таким образом, разбиению $\Omega = \Omega_1 \cup\dots\cup \Omega_q$ соответствует разложение подстановки f в произведение: $f = f_1\dots f_q$, при этом циклы-сомножители независимы и перестановочны. Естественно в произведении $f_1\dots f_q$ опускать сомножители, соответствующие множествам Ω_l из одного элемента, т. к. $f_l = e$ – тождественная подстановка на Ω.

Теорема 3.3.2. *Каждая подстановка $f \in S_n\backslash\{e\}$ является произведением независимых циклов, длины которых не менее* 2. *Это разложение в произведение определено однозначно с точностью до порядка следования циклов*.

Следствие. *Порядок подстановки $f \in S_n\backslash\{e\}$ (порядок циклической группы $< f >$) равен наименьшему общему кратному длин независимых циклов, входящих в разложение f.*

Если $g_k = \begin{pmatrix} i_1 & \dots & i_{k-1} & i_k \\ i_2 & \dots & i_k & i_1 \end{pmatrix} = (i_1\, i_2 \dots i_k)$ – цикл длины $k \geq 2$, то $\mathrm{ord}(g_k) = k$ и степени g_k находятся следующим образом:

$$g_k{}^2 = \begin{pmatrix} i_1 & \dots & i_{k-1} & i_k \\ i_3 & \dots & i_1 & i_2 \end{pmatrix} = (i_1\, i_3 \dots i_{k-1}),$$

$$g_k{}^3 = \begin{pmatrix} i_1 & \dots & i_{k-1} & i_k \\ i_4 & \dots & i_2 & i_3 \end{pmatrix} = (i_1\, i_4 \dots i_{k-2}),$$

$$\dots$$

$$g_k{}^k = \begin{pmatrix} i_1 & \dots & i_{k-1} & i_k \\ i_1 & \dots & i_{k-1} & i_k \end{pmatrix} = e.$$

Определение 3.3.4. Цикл длины 2 называется *транспозицией*.

Теорема 3.3.3. *Каждая подстановка $f \in S_n\backslash\{e\}$ разлагается в произведение транспозиций*.

Непосредственным умножением транспозиций проверяется, что произвольный цикл g_k длины $k \geq 2$ можно разложить в произведение транспозиций следующим образом:

$$g_k = (i_1\, i_2 \dots i_k) = (i_1\, i_k)(i_1\, i_{k-1})\dots(i_1\, i_2). \qquad (3.3.1)$$

Но данный способ разложения цикла в произведение транспозиций не является единственным. Таким образом, разложение подстановки в произведение транспозиций неоднозначно, например:

$$g = (1\ 4\ 6\ 8\ 3)(2\ 5\ 7\ 9) = (1\ 3)(1\ 8)(1\ 6)(1\ 4)(2\ 9)(2\ 7)(2\ 5) =$$
$$= (3\ 1\ 4\ 6\ 8)(5\ 7\ 9\ 2) = (3\ 8)(3\ 6)(3\ 4)(3\ 1)(5\ 2)(4\ 6)(5\ 9)(4\ 6)(5\ 7).$$

Тем не менее важно отметить, что любые два разложения одной и той же подстановки в произведение транспозиций содержат одновременно либо четное, либо нечетное число сомножителей.

Определение 3.3.5. Подстановка называется *четной*, если она разлагается в произведение четного числа транспозиций, в противном случае она называется *нечетной*. Тождественную подстановку также относят к четным, полагая, что в ее разложении нуль транспозиций.

Таким образом, характер четности фиксированной подстановки не изменяется в зависимости от различных разложений ее в произведение транспозиций.

Теорема 3.3.4. *Все четные подстановки группы* S_n *образуют подгруппу* A_n; $A_n = S_n$ *при* $n = 1$, $|A_n| = n!/2$ *при* $n \geq 2$.

Следствие. A_n *– нормальная подгруппа группы* S_n, $[S_n : A_n] = 2$ *при* $n \geq 2$.

Определение 3.3.6. Подгруппа A_n всех четных подстановок группы S_n называется *знакопеременной группой степени* n.

Примеры

1. Найти произведения подстановок fg и gf:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix},\ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

$$\begin{array}{rccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ g\colon & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 6 & 5 & 7 & 1 & 2 & 3 & 4 \\ f\colon & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 7 & 4 & 5 & 2 & 1 & 6 & 3 \end{array} \Rightarrow fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}.$$

Аналогично получаем, что

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 3 & 7 & 1 & 4 & 2 \end{pmatrix}.$$

В данном примере $fg \neq gf$.

2. Найти f^{-1} и g^{-1} для подстановок f и g из примера 1.

Для нахождения обратной подстановки нужно поменять местами 1-ю и 2-ю строки исходной подстановки, а затем упорядочить столбцы по возрастанию элементов 1-й строки:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 6 & 3 & 4 & 7 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 7 & 3 & 6 \end{pmatrix};$$

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 1 & 2 & 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 6 & 5 & 7 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 2 & 1 & 3 \end{pmatrix}.$$

3. Разложить подстановку f в произведение независимых циклов и транспозиций. Определить характер четности подстановки f:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 4 & 7 & 5 \end{pmatrix}.$$

Подстановка f переставляет элементы множества $\Omega = \{1, 2, 3, 4, 5, 6, 7\}$ следующим образом: $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 6$, $6 \mapsto 7$, $7 \mapsto 5$, $5 \mapsto 4$, $4 \mapsto 3$. Поэтому $f = (1\ 2)(3\ 6\ 7\ 5\ 4)$ – разложение f в произведение независимых циклов.

В соответствии с (3.3.1) имеем $f = (1\ 2)(3\ 4)(3\ 5)(3\ 7)(3\ 6)$ – разложение f в произведение транспозиций. Подстановка f является нечетной, поскольку в ее разложении в произведение транспозиций количество транспозиций равно 5.

4. Для подстановки f из примера 3 определить $\mathrm{ord}(f)$ в S_7 и найти $< f >$. Является ли $< f >$ нормальной подгруппой в S_7?

Так как $f = (1\ 2)(3\ 6\ 7\ 5\ 4)$, то $\mathrm{ord}(f) = [2, 5] = 10$ согласно следствию из теоремы 3.3.2.

Пусть $(1\ 2) = t_1$, $(3\ 6\ 7\ 5\ 4) = t_2$, тогда $f = t_1 t_2$, причем $\mathrm{ord}(t_1) = 2$, $\mathrm{ord}(t_2) = 5$. Имеем $(1\ 2)^2 = e$; $(3\ 6\ 7\ 5\ 4)^2 = (3\ 7\ 4\ 6\ 5)$, $(3\ 6\ 7\ 5\ 4)^3 = (3\ 5\ 6\ 4\ 7)$, $(3\ 6\ 7\ 5\ 4)^4 = (3\ 4\ 5\ 7\ 6)$, $(3\ 6\ 7\ 5\ 4)^5 = e$. Таким образом,

$$< f > = \{e, f, f^2, f^3, f^4, f^5, f^6, f^7, f^8, f^9\} = \{e, t_1t_2, {t_2}^2, t_1{t_2}^3, {t_2}^4, t_1, t_2, t_1{t_2}^2, {t_2}^3, t_1{t_2}^4\} =$$

$$= \{e, (1\ 2)(3\ 6\ 7\ 5\ 4), (3\ 7\ 4\ 6\ 5), (1\ 2)(3\ 5\ 6\ 4\ 7), (3\ 4\ 5\ 7\ 6), (1\ 2), (3\ 6\ 7\ 5\ 4),$$

$$(1\ 2)(3\ 7\ 4\ 6\ 5), (3\ 5\ 6\ 4\ 7), (1\ 2)(3\ 4\ 5\ 7\ 6)\}.$$

Пусть $g = (3\ 5) \notin < f >$, тогда $g^{-1} = (3\ 5)$. Проверим выполнение критерия нормальной подгруппы (теорема 3.2.3) для $< f >$:

$$gf^6g^{-1} = (3\ 5)(3\ 6\ 7\ 5\ 4)(3\ 5) = (3\ 5)(3\ 4)(5\ 6\ 7) = (3\ 4\ 5)(5\ 6\ 7) = (3\ 4\ 5\ 6\ 7) \notin < f >.$$

Значит, $< f >$ не является нормальной подгруппой в S_7.

Задачи

1. Разложить подстановку f в произведение независимых циклов и транспозиций. Определить характер четности подстановки f:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 6 & 5 & 7 \end{pmatrix}.$$

2. Для подстановки f из задачи 1 определить $\mathrm{ord}(f)$ в S_7 и найти $< f >$. Является ли $< f >$ нормальной подгруппой в S_7?

Ответы

1. $(1\ 4\ 3\ 2)(5\ 6) = (1\ 2)(1\ 3)(1\ 4)(5\ 6)$, четная. **2.** $\mathrm{ord}(f) = 4$, $\{e, (1\ 4\ 3\ 2)(5\ 6), (1\ 3)(4\ 2), (1\ 2\ 3\ 4)(5\ 6)\}$; не является.

§3.4. Гомоморфизмы групп. Алгоритм *RSA*

Определение 3.4.1. Пусть $(G_1, \bullet)$ и $(G_2, *)$ – две группы. Всякая функция $f: G_1 \to G_2$, сохраняющая операцию, т. е. обладающая свойством $f(g_1 \bullet g_2) = f(g_1) * f(g_2)$ для любых $g_1, g_2 \in G_1$, называется *гомоморфизмом* из группы G_1 в группу G_2.

Определение 3.4.2. *Образом гомоморфизма* $f: G_1 \to G_2$ называется множество $\mathrm{Im}\, f = \{f(g) \in G_2 \mid g \in G_1\} = E(f)$, т. е. образ группы G_1 при гомоморфизме f (англ. *image* – образ). *Ядром гомоморфизма* $f: G_1 \to G_2$ называется множество $\mathrm{Ker}\, f = \{g \in G_1 \mid f(g) = e_2\}$, где e_2 – нейтральный элемент группы $(G_2, *)$ (англ. *kernel* – ядро).

Определение 3.4.3. Гомоморфизм $f: G_1 \to G_2$ называется *мономорфизмом* (или *вложением*), если f – инъективная функция; другими словами, если $g_1, g_2 \in G_1$ и $g_1 \neq g_2$, то $f(g_1) \neq f(g_2)$. Гомоморфизм групп $f: G_1 \to G_2$ называется *эпиморфизмом*, если f – сюръективная функция, другими словами, если $\mathrm{Im}\, f = G_2$.

Свойства гомоморфизмов групп:

1. Пусть $(G_1, \bullet)$, $(G_2, *)$, $(G_3, \times)$ – группы. Если $f: G_1 \to G_2$ и $\psi: G_2 \to G_3$ – гомоморфизмы групп, то $\psi f: G_1 \to G_3$ – гомоморфизм групп.

2. Если $f: G_1 \to G_2$ – гомоморфизм групп, то:

1) $f(e_1) = e_2$, т. е. f нейтральный элемент первой группы переводит в нейтральный элемент второй группы;

2) $f(g^{-1}) = f(g)^{-1}$ для любого $g \in G_1$ т. е. образ обратного элемента при гомоморфизме есть обратный элемент для образа;

3) $\mathrm{Im}\, f \leq G_2$, т. е. образ гомоморфизма является подгруппой группы G_2.

3. Если $f: G_1 \to G_2$ – гомоморфизм групп, то $\mathrm{Ker}\, f \lhd G_1$, т. е. ядро гомоморфизма является нормальной подгруппой группы G_1.

4. Гомоморфизм $f: G_1 \to G_2$ является мономорфизмом тогда и только тогда, когда $\mathrm{Ker}\, f = \{e_1\}$.

Теорема 3.4.1. *Пусть* $(G, \bullet)$ *– группа,* $H \lhd G$ *и* $(G/H, \odot)$ *– факторгруппа с индуцированной операцией. Тогда функция* $f: G \to G/H$, *где* $f(g) = gH$ *для всех* $g \in G$, *является эпиморфизмом и* $\mathrm{Ker}\, f = H$.

Определение 3.4.4. Гомоморфизм из теоремы 3.4.1 $f: G \to G/H$, где $H \lhd G$, называется *естественным* (или *каноническим*) *гомоморфизмом*.

Определение 3.4.5. Биективный гомоморфизм групп называется *изоморфизмом*. Изоморфные группы будем обозначать $(G_1, \bullet) \cong (G_2, *)$ или $G_1 \cong G_2$.

Отношение изоморфизма на множестве всех групп является отношением эквивалентности: оно рефлексивно, симметрично и транзитивно. Таким образом, все множество групп разбивается на непересекающиеся классы попарно изоморфных объектов. Изоморфные группы можно отождествлять.

Теорема 3.4.2 (основная теорема о гомоморфизмах групп). *Пусть* $\psi: G_1 \to G_2$ *– гомоморфизм групп. Тогда* $G_1/\mathrm{Ker}\, \psi \cong \mathrm{Im}\, \psi$.

Как доказывается в теореме 3.4.2, изоморфизмом является функция $f: G_1/\mathrm{Ker}\, \psi \to \mathrm{Im}\, \psi$, где $f(g\mathrm{Ker}\, \psi) = \psi(g)$ для любого $g\mathrm{Ker}\, \psi \in G_1/\mathrm{Ker}\, \psi$.

Теорема 3.4.3. *Все циклические группы одного и того же порядка изоморфны.*

Пусть $|G_1| = |G_2|$, где $G_1 = < a >$, $G_2 = < b >$, причем $\mathrm{ord}(a)$ и $\mathrm{ord}(b)$ могут быть одновременно конечны и равны либо одновременно бесконечны. Тогда изоморфизмом групп является функция $f: G_1 \to G_2$, где $f(a^k) = b^k$, $\forall\, k \in \mathbf{Z}$.

Замечание. Из теоремы 3.4.3 следует, что все бесконечные циклические группы изоморфны группе $(\mathbf{Z}, +)$, а все конечные циклические группы порядка $n \in \mathbf{N}$ изоморфны $(\mathbf{Z}/n\mathbf{Z}, +)$.

Теорема 3.4.4 (А. Кэли). *Всякая группа* $(G, \bullet)$ *изоморфна некоторой подгруппе симметрической группы* $S(G)$. *В частности, всякая конечная группа порядка* n *изоморфна некоторой подгруппе группы* S_n.

Здесь гомоморфизм $f: G \to S(G)$ любому элементу $a \in G$ ставит в соответствие биективное преобразование (подстановку) $\psi_a: G \to G$, т. е. $f(a) = \psi_a$, где $\psi_a(g) = a \bullet g$ для всех $g \in G$. Поскольку $\operatorname{Ker} f = \{e\}$, то согласно теореме 3.4.2 $G/\{e\} = G \cong \operatorname{Im} f$, а $\operatorname{Im} f \le S(G)$ по свойству 2 гомоморфизмов групп. Если $|G| = n$, то $S(G) \cong S_n$ и в данном случае получаем, что группа $(G, \bullet)$ изоморфна некоторой подгруппе группы S_n.

Определение 3.4.6. Если гомоморфизм $f: G \to G$ является преобразованием группы G, то его называют *эндоморфизмом*. *Автоморфизм* – это биективный эндоморфизм группы.

Теорема 3.4.5. *Пусть* G *– конечная абелева группа порядка* $n \in \mathbf{N}$. *Тогда для всякого целого* k, *такого, что* $\text{НОД}(k, n) = 1$, *функция* $f: G \to G$, *где* $f(g) = g^k$ *для всех* $g \in G$, *есть автоморфизм данной группы*.

Криптосистема *RSA* была разработана и предложена в 1977 г. исследователями Массачусетского технологического института (США) и получила название в честь ее создателей (по первым буквам их фамилий: Ривест, Шамир и Адлеман). Суть *криптоалгоритма RSA* заключается в следующем. Находятся два больших простых числа (обычно 60–70 десятичных знаков) p и q. Вычисляется $n = pq$. Тогда $\varphi(n) = (p-1)(q-1)$, где φ – функция Эйлера. Фиксируется натуральное число e с условиями $e < \varphi(n)$ и $\text{НОД}(e, \varphi(n)) = 1$. Пара (e, n) называется *открытым ключом*. Передаваемая информация шифруется в виде натурального числа c-сообщения, где $c < n$ и $\text{НОД}(c, n) = 1$. Тогда $\bar{c}$ – обратимый класс в $\mathbf{Z}/n\mathbf{Z}$, т. е. элемент абелевой мультипликативной группы $\mathbf{Z}/n\mathbf{Z}^*$ порядка $\varphi(n)$. Сообщение c шифруется и передается числом $m \equiv c^e \pmod n$, т. е. $\bar{m}$ – e-я степень $\bar{c}$ в $\mathbf{Z}/n\mathbf{Z}$. Согласно теореме 3.4.5 возведение в e-ю степень является автоморфизмом группы $(\mathbf{Z}/n\mathbf{Z}^*, \cdot)$.

Адресат получает сообщение m, знает n и e. Он должен также знать *секретный ключ* – такое натуральное число d, что $d < \varphi(n)$ и $ed \equiv 1 \pmod{\varphi(n)}$. Значит, $ed = \varphi(n)k + 1$ для некоторого натурального числа k. Тогда в $\mathbf{Z}/n\mathbf{Z}^*$, согласно следствию 2 из теоремы 3.2.2 Лагранжа, имеем следующее равенство: $\bar{m}^d = \bar{c}^{ed} = \bar{c}^{\varphi(n)k+1} = \left(\bar{c}^{\varphi(n)}\right)^k \bar{c} = \bar{1} \cdot \bar{c} = \bar{c}$. Чтобы расшифровать m, адресат должен возвести m в d-ю степень по модулю n. Для возведения в степень удобно использовать двоичное представление числа d и рекурсивный алгоритм.

Криптоаналитик для расшифровки сообщения m должен разложить n на множители p и q. Тогда вычисляется $\varphi(n)$ и d находится по значению e из открытого ключа: $\bar{d} = \bar{e}^{-1}$ в $\mathbf{Z}/\varphi(n)\mathbf{Z}$. Именно *факторизация* n (разложение на простые множители) и составляет основную сложность, на которой базируется стойкость криптосистемы *RSA*.

Примеры

1. Доказать утверждения:

а) Группа $(\mathbf{R}_{>0}, \cdot)$ изоморфна группе $(\mathbf{R}, +)$.

Рассмотрим функцию $f: \mathbf{R}_{>0} \to \mathbf{R}$, где $f(x) = \ln(x)$ для любого $x \in \mathbf{R}_{>0}$. Согласно свойству логарифмической функции $f(x_1x_2) = \ln(x_1x_2) = \ln(x_1) + \ln(x_2) = f(x_1) + f(x_2)$ для любых $x_1, x_2 \in \mathbf{R}_{>0}$, поэтому f – гомоморфизм групп.

Поскольку производная функции $f'(x) = 1/x > 0$ для всех $x \in \mathbf{R}_{>0}$, то f монотонно возрастает и является инъекцией, поэтому f – мономорфизм. Так как для любого $y \in \mathbf{R}$ существует $x = e^y \in \mathbf{R}_{>0}$, такой, что $f(x) = y$, то $\operatorname{Im} f = \mathbf{R}$ и f – эпиморфизм. Итак, функция f – изоморфизм групп, значит, $(\mathbf{R}_{>0}, \cdot) \cong (\mathbf{R}, +)$.

В качестве изоморфизма f можно было рассмотреть логарифмическую функцию с любым основанием $a \in \mathbf{R}_{>0} \setminus \{1\}$.

б) Не существует эпиморфизма группы $(\mathbf{Q}, +)$ на группу $(\mathbf{Z}, +)$.

Пусть $f: \mathbf{Q} \to \mathbf{Z}$ – гомоморфизм групп, тогда $f(a + b) = f(a) + f(b)$ для любых $a, b \in \mathbf{Q}$. Для всякого $n \in \mathbf{N}$ имеем

$$f(1) = f\left(\sum_{k=1}^{n} 1/n\right) = nf(1/n) \Rightarrow f(1/n) = f(1)/n \in \mathbf{Z} \Rightarrow n \mid f(1).$$

Отсюда $f(1) = 0$ (свойство 1 делимости целых чисел) и $f(1/n) = 0$ для всех $n \in \mathbf{N}$.

Рассмотрим любое $m/n \in \mathbf{Q}$, где $m \in \mathbf{Z}$, $n \in \mathbf{N}$. Тогда $f(m/n) = mf(1/n) = 0$, т. к. $f(1/n) = 0$ для всех $n \in \mathbf{N}$. Значит, $\operatorname{Im} f = \{0\} \neq \mathbf{Z}$. Итак, существует единственный гомоморфизм $f: \mathbf{Q} \to \mathbf{Z}$ – нулевой, не являющийся эпиморфизмом.

в) Группа $(\mathbf{Q}_{>0}, \cdot)$ не изоморфна группе $(\mathbf{Q}, +)$.

Вначале докажем, что для произвольного изоморфизма $f: G_1 \to G_2$ групп $(G_1, \bullet)$ и $(G_2, *)$ обратная функция $f^{-1}: G_2 \to G_1$ (она существует согласно теореме 2.1.1) также является изоморфизмом. По свойству 7 функций и их композиций (см. §2.1) f^{-1} – биективная функция. Для любых $a, b \in G_2$ существуют $a_1, b_1 \in G_1$, такие, что $a = f(a_1)$, $b = f(b_1)$, или $a_1 = f^{-1}(a)$, $b_1 = f^{-1}(b)$. Тогда

$$f^{-1}(a * b) = f^{-1}(f(a_1) * f(b_1)) = f^{-1}(f(a_1 \bullet b_1)) = a_1 \bullet b_1 = f^{-1}(a) \bullet f^{-1}(b).$$

Итак, f^{-1} – изоморфизм групп.

Теперь предположим, что существует $f: \mathbf{Q}_{>0} \to \mathbf{Q}$ – изоморфизм групп $(\mathbf{Q}_{>0}, \cdot)$ и $(\mathbf{Q}, +)$, тогда по доказанному выше $f^{-1}: \mathbf{Q} \to \mathbf{Q}_{>0}$ – также изоморфизм данных групп. Рассмотрим, например, число $3 \in \mathbf{Q}_{>0}$. Тогда мы имели бы

$$3 = f^{-1}(f(3)) = f^{-1}(f(3)/2 + f(3)/2) = f^{-1}(f(3)/2) \cdot f^{-1}(f(3)/2) = r^2,$$

где $r \in \mathbf{Q}_{>0}$, что невозможно, поскольку $\sqrt{3}$ – иррациональное число. Данное противоречие доказывает неверность нашего предположения и несуществование изоморфизма $f: \mathbf{Q}_{>0} \to \mathbf{Q}$. При доказательстве вместо 3 можно было рассмотреть любое $c \in \mathbf{N}_{>1}$ и подходящее $n \in \mathbf{N}_{>1}$, такое, что $\sqrt[n]{c}$ – иррациональное число.

2. Найти все гомоморфизмы из циклической группы $< a >$ порядка m в циклическую группу $< b >$ порядка n; описать образ и ядро каждого гомоморфизма,

указать все мономорфизмы, эпиморфизмы и изоморфизмы в случае их существования. Решить задачу для заданных ниже значений порядков m и n.

Если $f: < a > \to < b >$ – гомоморфизм, то $\mathrm{Im} f \le < b >$ по свойству 2 гомоморфизмов групп, $\mathrm{Ker} f \le < a >$ по свойству 3 гомоморфизмов групп и $< a > / \mathrm{Ker} f \cong \mathrm{Im} f$ согласно теореме 3.4.2 (основная теорема о гомоморфизмах групп), поэтому $[< a > : \mathrm{Ker} f] = |\mathrm{Im} f|$. Тогда $|\mathrm{Im} f \,|\, m$ согласно теореме 3.2.2 Лагранжа и $|\mathrm{Im} f \,|\, n$ согласно следствию 1 из теоремы 3.2.2. Значит, $|\mathrm{Im} f| = k$ может принимать только значения из множества ОД m и n. Рассуждение о строении подгрупп циклической группы конечного порядка было приведено в примере 5 из §3.1. Таким образом, $\mathrm{Im} f = < b^l >$, где $(l, n) = n/k$, в силу определения гомоморфизма $f(a) = b^l$, тогда $f(a^s) = b^{ls}$, $0 \le s \le m-1$. При этом $|\mathrm{Ker} f| = m/k$ и $\mathrm{Ker} f = \{a^t \mid b^{lt} = e_2\} = < a^u >$, где $(u, m) = k$. Функция f является мономорфизмом в том и только том случае, если $\mathrm{Ker} f = \{e_1\}$ (свойство 4 гомоморфизмов групп). Функция f является эпиморфизмом тогда и только тогда, когда $\mathrm{Im} f = < b >$ (определение 3.4.3). Функция f – изоморфизм тогда и только тогда, когда f является одновременно мономорфизмом и эпиморфизмом (определение 3.4.5), такое возможно только в случае $m = n$.

а) $m = 6$, $n = 18$.

$< a > = \{a, a^2, a^3, a^4, a^5, e_1\}$, $\mathrm{ord}(a) = 6$; $< b > = \{b, b^2, b^3, b^4, \ldots, b^{16}, b^{17}, e_2\}$, $\mathrm{ord}(b) = 18$. В данном случае k может принимать значения 1, 2, 3 и 6. При этом никакой гомоморфизм не может быть изоморфизмом, поскольку $|< a >| = 6 \ne \ne 18 = |< b >|$.

При $k = 1$ имеем $H_1 = \{e_2\} = < e_2 >$, значит, $\mathrm{Im} f_1 = H_1$ для гомоморфизма $f_1: < a > \to < b >$, где $f_1(a) = e_2$, тогда $f_1(a^s) = e_2{}^s = e_2$, $0 \le s \le 5$, и $\mathrm{Ker} f_1 = < a > = = < a^5 >$, т. к. $(1, 6) = (5, 6) = 1$. Так как $\mathrm{Ker} f_1 \ne \{e_1\}$, то f_1 не является мономорфизмом; $\mathrm{Im} f_1 \ne < b >$, поэтому f_1 не является эпиморфизмом.

При $k = 2$ имеем $H_2 = \{b^9, e_2\} = < b^9 >$, т. к. $(9, 18) = 18/2 = 9$, значит, $\mathrm{Im} f_2 = = H_2$ для гомоморфизма $f_2: < a > \to < b >$, где $f_2(a) = b^9$, тогда $f_2(a^s) = b^{9s}$, $0 \le s \le \le 5$, и $\mathrm{Ker} f_2 = \{a^2, a^4, e_1\} = < a^2 > = < a^4 >$, т. к. $(2, 6) = (4, 6) = 2$. Так как $\mathrm{Ker} f_2 \ne \ne \{e_1\}$, то f_2 не является мономорфизмом; $\mathrm{Im} f_2 \ne < b >$, поэтому f_2 не является эпиморфизмом.

При $k = 3$ имеем $H_3 = \{b^6, b^{12}, e_2\} = < b^6 > = < b^{12} >$, т. к. $(6, 18) = (12, 18) = = 18/3 = 6$, значит, $\mathrm{Im} f_{31} = \mathrm{Im} f_{32} = H_3$ для гомоморфизмов $f_{31}, f_{32}: < a > \to < b >$, где $f_{31}(a) = b^6$, $f_{32}(a) = b^{12}$, тогда $f_{31}(a^s) = b^{6s}$, $f_{32}(a^s) = b^{12s}$, $0 \le s \le 5$, и $\mathrm{Ker} f_{31} = = \mathrm{Ker} f_{32} = \{a^3, e_1\} = < a^3 >$, т. к. $(3, 6) = 3$. Так как $\mathrm{Ker} f_{31} = \mathrm{Ker} f_{32} \ne \{e_1\}$, то f_{31} и f_{32} не являются мономорфизмами; $\mathrm{Im} f_{31} = \mathrm{Im} f_{32} \ne < b >$, поэтому f_{31} и f_{32} не являются эпиморфизмами.

При $k = 6$ имеем $H_6 = \{b^3, b^6, b^9, b^{12}, b^{15}, e_2\} = < b^3 > = < b^{15} >$, т. к. $(3, 18) = = (15, 18) = 18/6 = 3$, значит, $\mathrm{Im} f_{41} = \mathrm{Im} f_{42} = H_6$ для гомоморфизмов $f_{41}, f_{42}: < a > \to \to < b >$, где $f_{41}(a) = b^3$, $f_{42}(a) = b^{15}$, тогда $f_{41}(a^s) = b^{3s}$, $f_{42}(a^s) = b^{15s}$, $0 \le s \le 5$, и $\mathrm{Ker} f_{41} = \mathrm{Ker} f_{42} = \{e_1\} = < e_1 >$, т. к. $(6, 6) = 6$. Так как $\mathrm{Ker} f_{41} = \mathrm{Ker} f_{42} = \{e_1\}$, то

f_{41} и f_{42} являются мономорфизмами. Поскольку $\operatorname{Im} f_{41} = \operatorname{Im} f_{42} \neq < b >$, то f_{41} и f_{42} не являются эпиморфизмами.

б) $m = 18$, $n = 6$.

$< a > = \{a, a^2, a^3, a^4, \ldots, a^{16}, a^{17}, e_1\}$, $\operatorname{ord}(a) = 18$; $< b > = \{b, b^2, b^3, b^4, b^5, e_2\}$, $\operatorname{ord}(b) = 6$. В данном случае k может принимать значения 1, 2, 3 и 6. При этом никакой гомоморфизм не может быть изоморфизмом, поскольку $|< a >| = 18 \neq$ $\neq 6 = |< b >|$.

При $k = 1$ имеем $H_1 = \{e_2\} = < e_2 >$, значит, $\operatorname{Im} f_1 = H_1$ для гомоморфизма $f_1 : < a > \to < b >$, где $f_1(a) = e_2$, тогда $f_1(a^s) = e_2^s = e_2$, $0 \le s \le 17$, и $\operatorname{Ker} f_1 = < a > =$ $= < a^5 > = < a^7 > = < a^{11} > = < a^{13} > = < a^{17} >$, т. к. $(1, 18) = (5, 18) = (7, 18) = (11, 18) =$ $= (13, 18) = (17, 18) = 1$. Так как $\operatorname{Ker} f_1 \neq \{e_1\}$, то f_1 не является мономорфизмом; $\operatorname{Im} f_1 \neq < b >$, поэтому f_1 не является эпиморфизмом.

При $k = 2$ имеем $H_2 = \{b^3, e_2\} = < b^3 >$, т. к. $(3, 6) = 6/2 = 3$, значит, $\operatorname{Im} f_2 =$ $= H_2$ для гомоморфизма $f_2 : < a > \to < b >$, где $f_2(a) = b^3$, тогда $f_2(a^s) = b^{3s}$, $0 \le s \le$ ≤ 17, и $\operatorname{Ker} f_2 = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, e_1\} = < a^2 > = < a^4 > = < a^8 > =$ $= < a^{10} > = < a^{14} > = < a^{16} >$, т. к. $(2, 18) = (4, 18) = (8, 18) = (10, 18) = (14, 18) =$ $= (16, 18) = 2$. Так как $\operatorname{Ker} f_2 \neq \{e_1\}$, то f_2 не является мономорфизмом; $\operatorname{Im} f_2 \neq$ $\neq < b >$, поэтому f_2 не является эпиморфизмом.

При $k = 3$ имеем $H_3 = \{b^2, b^4, e_2\} = < b^2 > = < b^4 >$, т. к. $(2, 6) = (4, 6) = 6/3 =$ $= 2$, значит, $\operatorname{Im} f_{31} = \operatorname{Im} f_{32} = H_3$ для гомоморфизмов f_{31}, $f_{32} : < a > \to < b >$, где $f_{31}(a) = b^2$, $f_{32}(a) = b^4$, тогда $f_{31}(a^s) = b^{2s}$, $f_{32}(a^s) = b^{4s}$, $0 \le s \le 17$, и $\operatorname{Ker} f_{31} = \operatorname{Ker} f_{32} =$ $= \{a^3, a^6, a^9, a^{12}, a^{15}, e_1\} = < a^3 > = < a^{15} >$, т. к. $(3, 18) = (15, 18) = 3$. Так как $\operatorname{Ker} f_{31} = \operatorname{Ker} f_{32} \neq \{e_1\}$, то f_{31} и f_{32} не являются мономорфизмами; $\operatorname{Im} f_{31} = \operatorname{Im} f_{32} \neq$ $\neq < b >$, поэтому f_{31} и f_{32} не являются эпиморфизмами.

При $k = 6$ имеем $H_6 = \{b, b^2, b^3, b^4, b^5, e_2\} = < b > = < b^5 >$, т. к. $(1, 6) =$ $= (5, 6) = 6/6 = 1$, значит, $\operatorname{Im} f_{41} = \operatorname{Im} f_{42} = H_6$ для гомоморфизмов f_{41}, $f_{42} : < a > \to$ $\to < b >$, где $f_{41}(a) = b$, $f_{42}(a) = b^5$, тогда $f_{41}(a^s) = b^s$, $f_{42}(a^s) = b^{5s}$, $0 \le s \le 17$, и $\operatorname{Ker} f_{41} = \operatorname{Ker} f_{42} = \{a^6, a^{12}, e_1\} = < a^6 > = < a^{12} >$, т. к. $(6, 18) = (12, 18) = 6$. Так как $\operatorname{Ker} f_{41} = \operatorname{Ker} f_{42} \neq \{e_1\}$, то f_{41} и f_{42} не являются мономорфизмами. Поскольку $\operatorname{Im} f_{41} = \operatorname{Im} f_{42} = < b >$, то f_{41} и f_{42} являются эпиморфизмами.

3. Доказать, что группы изоморфны:

а) $S_n/A_n \cong (\mathbf{Z}/2\mathbf{Z}, +)$ при всех $n \in \mathbf{N}_{>1}$.

Построим функцию $f : S_n \to \mathbf{Z}/2\mathbf{Z}$, где $f(g) = \begin{cases} \bar{0} & \text{при } g \in A_n; \\ \bar{1} & \text{при } g \in S_n \setminus A_n. \end{cases}$

Рассмотрим произвольные подстановки $g_1, g_2 \in S_n$. Согласно теореме 3.3.3 и определению 3.3.5 подстановки g_1 и g_2 разлагаются в произведение транспозиций и произведение двух подстановок одинаковой четности – четная подстановка, произведение двух подстановок различной четности – нечетная подстановка. Таким образом,

$$f(g_1g_2)=\begin{cases}\bar{0}=\bar{0}+\bar{0} \text{ при } g_1,\ g_2\in A_n;\\ \bar{1}=\bar{0}+\bar{1} \text{ при } g_1\in A_n,\ g_2\in S_n\setminus A_n;\\ \bar{1}=\bar{1}+\bar{0} \text{ при } g_1\in S_n\setminus A_n,\ g_2\in A_n;\\ \bar{0}=\bar{1}+\bar{1} \text{ при } g_1,\ g_2\in S_n\setminus A_n.\end{cases}$$

Значит, $f(g_1g_2)=f(g_1)+f(g_2)$, поэтому f – гомоморфизм групп.

Так как при $n>1$ в S_n есть как четные, так и нечетные подстановки, то $\operatorname{Im} f=\mathbf{Z}/2\mathbf{Z}$. Имеем $\operatorname{Ker} f=A_n$ по построению f. Итак, по основной теореме о гомоморфизмах групп (теорема 3.4.2) $S_n/A_n\cong(\mathbf{Z}/2\mathbf{Z},+)$.

б) $GL_n(\mathbf{R})/SL_n(\mathbf{R})\cong(\mathbf{R}^*,\cdot)$ при всех $n\in\mathbf{N}$.

Построим функцию $f\colon GL_n(\mathbf{R})\to\mathbf{R}^*$, где $f(A)=\det(A)$, $\forall A\in GL_n(\mathbf{R})$. Тогда $f(A_1A_2)=\det(A_1A_2)=\det(A_1)\det(A_2)=f(A_1)f(A_2)$ для любых $A_1, A_2\in GL_n(\mathbf{R})$ согласно свойству определителей матриц. Таким образом, f – гомоморфизм групп.

Поскольку для любого $a\in\mathbf{R}^*$ существует $A_a=\begin{pmatrix}a&0&\dots&0\\0&1&\dots&0\\\vdots&\ddots&\ddots&\vdots\\0&\dots&0&1\end{pmatrix}\in GL_n(\mathbf{R})$, где $\det(A_a)=a$ ($A_a=a$ при $n=1$), то $\operatorname{Im} f=\mathbf{R}^*$. Имеем $\operatorname{Ker} f=SL_n(\mathbf{R})$ по построению f и согласно определению $SL_n(\mathbf{R})$. Итак, по основной теореме о гомоморфизмах групп $GL_n(\mathbf{R})/SL_n(\mathbf{R})\cong(\mathbf{R}^*,\cdot)$.

в) $GL_n(\mathbf{C})/H\cong(U,\cdot)$ при всех $n\in\mathbf{N}$, где $H=\{B\in GL_n(\mathbf{C})\mid\det(B)\in\mathbf{R}_{>0}\}$, $U=\{u\in\mathbf{C}^*\mid|u|=1\}$.

Построим функцию $f\colon GL_n(\mathbf{C})\to U$, где $f(A)=\dfrac{\det(A)}{|\det(A)|}$, $\forall A\in GL_n(\mathbf{C})$. Тогда для любых $A_1, A_2\in GL_n(\mathbf{C})$ согласно свойствам определителей матриц и модулей комплексных чисел имеем

$$f(A_1A_2)=\frac{\det(A_1A_2)}{|\det(A_1A_2)|}=\frac{\det(A_1)\det(A_2)}{|\det(A_1)\det(A_2)|}=\frac{\det(A_1)}{|\det(A_1)|}\frac{\det(A_2)}{|\det(A_2)|}=f(A_1)f(A_2).$$

Таким образом, f – гомоморфизм групп.

Поскольку для любого $u\in U$ существует $A_u=\begin{pmatrix}u&0&\dots&0\\0&1&\dots&0\\\vdots&\ddots&\ddots&\vdots\\0&\dots&0&1\end{pmatrix}\in GL_n(\mathbf{C})$, где $\det(A_u)=u$, $|u|=1$ и $f(A_u)=u$ ($A_u=u$ при $n=1$), то $\operatorname{Im} f=U$.

$$\operatorname{Ker} f=\{B\in GL_n(\mathbf{C})\mid\det(B)/|\det(B)|=1\Leftrightarrow\det(B)=|\det(B)|\Leftrightarrow$$
$$\Leftrightarrow\det(B)\in\mathbf{R}_{>0}\}=H.$$

Итак, по основной теореме о гомоморфизмах групп $GL_n(\mathbf{C})/H\cong(U,\cdot)$.

4. Используя теорему Кэли (теорема 3.4.4), построить:

а) Подгруппу в $S(\mathbf{Z})$, изоморфную группе $(\mathbf{Z},+)$.

Следуя доказательству теоремы Кэли (рассуждениям, приведенным после формулировки теоремы 3.4.4), гомоморфизм $f\colon \mathbf{Z} \to S(\mathbf{Z})$ любому $a \in \mathbf{Z}$ ставит в соответствие подстановку $\psi_a\colon \mathbf{Z} \to \mathbf{Z}$, т. е. $f(a) = \psi_a$, где $\psi_a(z) = a + z$ для всех $z \in \mathbf{Z}$ – сдвиг на постоянную целочисленную величину a во множестве $\mathbf{Z}$. Действительно, $f(a + b) = \psi_{a+b} = \psi_a \circ \psi_b = f(a) \circ f(b)$ для любых $a, b \in \mathbf{Z}$. Поскольку $\operatorname{Ker} f = \{0\}$, то согласно теореме 3.4.2 $\mathbf{Z} \cong \operatorname{Im} f$, а $\operatorname{Im} f < S(\mathbf{Z})$ по свойству 2 гомоморфизмов групп. Итак, $H = \operatorname{Im} f = \{\psi_a \mid a \in \mathbf{Z}\}$ является искомой подгруппой в $S(\mathbf{Z})$. Так как $\mathbf{Z} = <1> = <-1>$ – бесконечная циклическая группа с образующими элементами 1 и -1 (по свойству 2 делимости целых чисел), то $H = <\psi_1> = <\psi_{-1}>$.

Отметим дополнительно, что для любого $a \in \mathbf{Z}\backslash\{0\}$ бесконечная циклическая подгруппа $<\psi_a> = <\psi_{-a}>$ в $S(\mathbf{Z})$ изоморфна группе $(\mathbf{Z}, +)$ согласно замечанию к теореме 3.4.3.

б) Подгруппу в S_4, изоморфную циклической группе $<a>$ порядка 4.

$<a> = \{a, a^2, a^3, e_1\}$, $\operatorname{ord}(a) = 4$. Нумерация элементов группы $\eta\colon a^k \mapsto k$, где $1 \le k \le 4$, задает взаимно однозначное соответствие между множествами $<a>$ и $\Omega = \{1, 2, 3, 4\}$. Следуя рассуждениям, приведенным после формулировки теоремы 3.4.4, гомоморфизм $f\colon <a> \to S_4$ любому a^k при $1 \le k \le 4$ ставит в соответствие подстановку $\psi_k\colon \Omega \to \Omega$, т. е. $f(a^k) = \psi_k$, где $\psi_k(\eta(a^l)) = \eta(a^{k+l})$, $1 \le l \le 4$. Таким образом,

$$\psi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\,2\,3\,4),\ \psi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\,3)(2\,4),$$

$$\psi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\,4\,3\,2),\ \psi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e.$$

Поскольку $\operatorname{Ker} f = \{e_1\}$, то согласно теореме 3.4.2 $<a> \cong \operatorname{Im} f$, а $\operatorname{Im} f < S_4$ по свойству 2 гомоморфизмов групп. Итак, $H = \operatorname{Im} f = \{(1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), e\}$ является искомой подгруппой в S_4. Так как $<a> = <a^3>$, то $H = <(1\,2\,3\,4)> = <(1\,4\,3\,2)>$.

5. Для криптоалгоритма *RSA* задан открытый ключ (n, e) и число m, которым зашифровано c-сообщение: $n = 2021$, $e = 5$, $m = 415$. Буква x зашифрована числом c по следующему правилу: $c = ASCII(x) + 1000$, где $ASCII(x)$ – *ASCII*-код буквы x. Требуется найти секретный ключ d, c-сообщение и расшифровать букву x.

Разложим число n на простые множители: $n = pq$. Для этого находим минимальное простое число p, такое, что $p \mid n$ и $p \le \lceil \sqrt{n} \rceil$. Используя «решето» Эратосфена, получаем, что $p = 43$, $q = 47$. Тогда $\varphi(n) = (p - 1)(q - 1) = 1932$.

Далее из соотношения $ed \equiv 1 \pmod{\varphi(n)}$ определяем секретный ключ d. Найдем представитель класса $\bar{d}$, обратного классу $\bar{e} = \bar{5}$ в $\mathbf{Z}/\varphi(n)\mathbf{Z}$, из соотношения Безу для чисел 1, 5 и 1932, вычислив коэффициенты по расширенному алгоритму Евклида:

$$r_{-1} = 1932,\ u_{-1} = 0,\ v_{-1} = 1;\ r_0 = 5,\ u_0 = 1,\ v_0 = 0;$$
$$q_1 = 386,\ u_1 = u_{-1} - u_0 q_1 = -386,\ v_1 = v_{-1} - v_0 q_1 = 1 \Rightarrow r_1 = 2 = 5 \cdot (-386) + 1932;$$
$$q_2 = 2,\ u_2 = u_0 - u_1 q_2 = 773,\ v_2 = v_0 - v_1 q_2 = -2 \Rightarrow r_2 = 1 = 5 \cdot 773 + 1932 \cdot (-2).$$

Тогда $5 \cdot 773 \equiv 1 \pmod{1932}$ и $d = 773$.

Для получения c возводим m в степень d по модулю n. Для этого удобно использовать двоичное представление числа d и рекурсивный алгоритм возведения в степень:

$$773 = 2^9 + 261 = 2^9 + 2^8 + 5 = 2^9 + 2^8 + 2^2 + 2^0;$$
$$c \equiv 415^{773} = 415^{2^9 + 2^8 + 2^2 + 2^0} = 415^{2^0} \cdot 415^{2^2} \cdot 415^{2^8} \cdot 415^{2^9} =$$
$$= 415 \cdot 415^{2^2} \cdot \left(415^{2^2}\right)^{2^6} \cdot \left(\left(415^{2^2}\right)^{2^6}\right)^2 \equiv ((a_0 a_1) a_3) a_5 \equiv \big((415 \cdot (-416)) a_3\big) a_5 \equiv$$
$$\equiv ((-855) \cdot (-287)) a_5 \equiv 844 \cdot (-492) \equiv 1078 \pmod{2021}.$$

Здесь $a_0 = 415$, $a_1 \equiv a_0^4$, $a_2 \equiv a_0 a_1$, $a_3 \equiv a_1^{64}$, $a_4 \equiv a_2 a_3$, $a_5 \equiv a_3^2$, $a_6 \equiv a_4 a_5$ и $c \equiv a_6 \pmod{2021}$. Для облегчения вычислений можно так же возводить в степени и перемножать множители канонического разложения числа m: $415 = 5 \cdot 83$.

Таким образом, $ASCII(x) = c - 1000 = 78$. По таблице *ASCII*-кодов находим, что x является буквой «N» с учетом регистра.

Задачи

1. Найти все гомоморфизмы из циклической группы $< a >$ порядка m в циклическую группу $< b >$ порядка n; описать образ и ядро каждого гомоморфизма, указать все мономорфизмы, эпиморфизмы и изоморфизмы в случае их существования:

а) $m = 12$, $n = 15$; **б)** $m = 6$, $n = 25$.

2. Доказать, что группы изоморфны:

а) $GL_n(\mathbf{R})/H \cong (\mathbf{R}_{>0}, \cdot)$ при всех $n \in \mathbf{N}$, где $H = \{ B \in GL_n(\mathbf{R}) \mid \det(B) = \pm 1 \}$. Указание: показать, что функция $f: GL_n(\mathbf{R}) \to \mathbf{R}_{>0}$, где $f(A) = |\det(A)|$, $\forall A \in GL_n(\mathbf{R})$, является гомоморфизмом; найти $\operatorname{Im} f$, $\operatorname{Ker} f$ и применить основную теорему о гомоморфизмах групп (теорема 3.4.2);

б) $GL_n(\mathbf{R})/H \cong (\mathbf{Z}/2\mathbf{Z}, +)$ при всех $n \in \mathbf{N}$, где $H = \{ B \in GL_n(\mathbf{R}) \mid \det(B) \in \mathbf{R}_{>0} \}$. Указание: найти $\operatorname{Im} f$, $\operatorname{Ker} f$ и применить основную теорему о гомоморфизмах групп (теорема 3.4.2), показав, что гомоморфизмом данных групп является функция $f: GL_n(\mathbf{R}) \to \mathbf{Z}/2\mathbf{Z}$, где $f(A) = \begin{cases} \bar{0} & \text{при } \det(A) > 0; \\ \bar{1} & \text{при } \det(A) < 0. \end{cases}$

3. Используя теорему Кэли (теорема 3.4.4), построить в S_6 подгруппу, изоморфную циклической группе $< a >$ порядка 6.

4. Для криптоалгоритма *RSA* задан открытый ключ (n, e) и число m, которым зашифровано c-сообщение: $n = 2491$, $e = 11$, $m = 85$. Требуется найти секретный ключ d, c-сообщение и расшифровать букву x, если $c = ASCII(x) + 1000$.

5. Выбрать открытый ключ (n, e) для криптоалгоритма *RSA* так, чтобы $n > 1300$. Вычислить секретный ключ d. Убедиться, что найден правильный ключ – зашифровать и расшифровать сообщение (число c).

Ответы

1. а) $f_1(a^s) = e_2$, $f_{21}(a^s) = b^{5s}$, $f_{22}(a^s) = b^{10s}$, $0 \le s \le 11$, $\operatorname{Im} f_1 = \{e_2\} = < e_2 >$, $\operatorname{Ker} f_1 = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, e_1\} = < a > = < a^5 > = < a^7 > = < a^{11} >$, $\operatorname{Im} f_{21} = \operatorname{Im} f_{22} = \{b^5, b^{10}, e_2\} = < b^5 > = < b^{10} >$, $\operatorname{Ker} f_{21} = \operatorname{Ker} f_{22} = \{a^3, a^6, a^9, e_1\} = < a^3 > = < a^9 >$, не существует ни мономорфизмов, ни эпиморфизмов; **б)** $f_1(a^s) = e_2$, $0 \le s \le 5$, $\operatorname{Im} f_1 = \{e_2\} = < e_2 >$, $\operatorname{Ker} f_1 = \{a, a^2, a^3, a^4, a^5, e_1\} = < a > = < a^5 >$, f_1 – ни мономорфизм, ни эпиморфизм. **3.** $H = \{(1\ 2\ 3\ 4\ 5\ 6), (1\ 3\ 5)(2\ 4\ 6), (1\ 4)(2\ 5)(3\ 6), (1\ 5\ 3)(2\ 6\ 4), (1\ 6\ 5\ 4\ 3\ 2), e\} = <(1\ 2\ 3\ 4\ 5\ 6)> = <(1\ 6\ 5\ 4\ 3\ 2)>$. **4.** $d = 435$, $c = 1110$, $x =$ «n» с учетом регистра.

Глава 4. Введение в теорию колец и полей

§4.1. Понятия кольца, поля, подкольца и идеала кольца

Определение 4.1.1. *Кольцо* $(K, +, \cdot)$ – это алгебраическая система с непустым множеством K и двумя бинарными алгебраическими операциями на нем, которые будем называть *сложением* и *умножением* (часто знак умножения «·» в записи опускается для сокращения). $(K, +)$ является абелевой группой, называемой *аддитивной группой кольца* K, а умножение и сложение связаны законами дистрибутивности: $(a + b)c = ac + bc$ и $c(a + b) = ca + cb$ для произвольных $a, b, c \in K$. Нейтральный элемент аддитивной группы кольца $(K, +)$ называют *нулем* и часто обозначают символом 0.

Определение 4.1.2. Кольцо $(K, +, \cdot)$ называется *конечным*, если K – конечное множество, в противном случае – *бесконечным*. *Порядком* конечного кольца $|K|$ называется мощность множества K. Основная классификация колец ведется по свойствам операции умножения. Различают *ассоциативные* кольца, когда операция умножения ассоциативна, и *неассоциативные* кольца соответственно. Ассоциативные кольца делятся на *кольца с единицей* (обладающие нейтральным элементом относительно умножения, который часто будем обозначать символом 1) и *без единицы*; *коммутативные* (операция умножения коммутативна) и *некоммутативные* соответственно.

Теорема 4.1.1. *Пусть* $(K, +, \cdot)$ *– ассоциативное кольцо с единицей. Тогда множество* K^* *обратимых относительно умножения элементов кольца* K *– мультипликативная группа*.

Определение 4.1.3. Группу $(K^*, \cdot)$ обратимых относительно умножения элементов ассоциативного кольца с единицей $(K, +, \cdot)$ называют *мультипликативной группой кольца*.

Определение 4.1.4. Если в ассоциативном кольце $(K, +, \cdot)$ с единицей группа K^* совпадает с $K \setminus \{0\}$, где 0 – нейтральный элемент относительно сложения, то такое кольцо называют *телом*, или *алгеброй с делением*. Коммутативное тело называется *полем*.

Из данного определения очевидно, что в теле $K^* \neq \varnothing$ и $1 \in K^*$, значит, $1 \neq 0$, поэтому минимальное тело, являющееся полем, состоит из двух элементов: 0 и 1.

Определение 4.1.5. Если в кольце найдутся ненулевые элементы a и b, такие, что $ab = 0$, то их называют *делителями нуля*, а само кольцо – *кольцом с делителями нуля*. В противном случае кольцо называется *кольцом без делителей нуля*.

Свойства колец:

1. В любом кольце $(K, +, \cdot)$ для произвольных $a, b \in K$ уравнение $a + x = b$ имеет единственное решение: $x = b + (-a)$.

Определение 4.1.6. Сумма $a+(-b)$ называется *разностью* элементов a и b и обозначается $a-b$. Разность $a-b \in K$ для произвольных $a, b \in K$. Таким образом, определена бинарная алгебраическая операция *вычитания* в любом кольце.

2. Умножение в кольце дистрибутивно относительно вычитания:

$a(b-c) = ab - ac$ и $(b-c)a = ba - ca$ для любых $a, b, c \in K$.

3. Свойство нуля: $a \cdot 0 = 0 \cdot a = 0$ для любого $a \in K$.

4. Правила знаков:

$a(-b) = (-a)b = -(ab)$, $(-a)(-b) = ab$ для любых $a, b \in K$.

5. Если $(K, +, \cdot)$ – кольцо с единицей и $|K| > 1$, то $1 \neq 0$.

6. В ассоциативном кольце с единицей делители нуля необратимы.

Свойства полей

Для полей справедливы все свойства колец. Будем обозначать в дальнейшем поле $(P, +, \cdot)$. Также отметим специфические свойства полей:

1. В поле нет делителей нуля.

2. В любом поле $(P, +, \cdot)$ для произвольных $a \in P^*$ и $b \in P$ уравнение $ax = b$ имеет единственное решение: $x = a^{-1}b$.

Определение 4.1.7. *Подкольцо* кольца $(K, +, \cdot)$ – это подгруппа L аддитивной группы $(K, +)$, в свою очередь являющаяся кольцом относительно индуцированных операций, т. е. для любых $l_1, l_2 \in L$ выполняются свойства: **1)** $l_1 - l_2 \in L$; **2)** $l_1 l_2 \in L$. Обозначения подкольца: $L \leq K$ или $L < K$, если $L \subset K$.

Очевидно, что для любого кольца $(K, +, \cdot)$ подмножества $\{0\}$ и K являются подкольцами.

Определение 4.1.8. Подкольцо L кольца K называется *собственным* (или *нетривиальным*), если $L \neq K$ и $L \neq \{0\}$.

Определение 4.1.9. Непустое подмножество Δ поля $(P, +, \cdot)$ называют *подполем* поля P, если Δ само является полем относительно индуцированных операций: **1)** Δ – подкольцо кольца P; **2)** для любого $\delta \in \Delta \backslash \{0\} \Rightarrow \delta^{-1} \in \Delta$. В этом случае поле $(P, +, \cdot)$ называется *расширением* поля $(\Delta, +, \cdot)$. Последовательность расширений полей $P_1 \leq P_2 \leq \ldots \leq P_s$, где $s \in \mathbf{N}_{\geq 3}$, называется *башней расширений* полей.

Определение 4.1.10. Подкольцо J кольца $(K, +, \cdot)$ называется *левым идеалом* кольца K, если для любых $k \in K$ и $j \in J$ выполняется условие $kj \in J$, т. е. $KJ = \{kj \mid k \in K, j \in J\} \subseteq J$. Если же $JK = \{jk \mid j \in J, k \in K\} \subseteq J$, то подкольцо J называют *правым идеалом* кольца K. *Двусторонний идеал* кольца – идеал, являющийся одновременно и левым, и правым. Для двустороннего идеала J кольца K будет использоваться обозначение $J \lhd K$.

Ясно, что в коммутативном кольце все идеалы двусторонние, в этом случае будем называть их просто *идеалами* кольца.

Легко видеть, что $\{0\}$ и K – тривиальные двусторонние идеалы любого кольца $(K, +, \cdot)$.

Целочисленное кратное элемента a кольца $(K, +, \cdot)$ для $m \in \mathbf{Z}$ обозначим ma. То есть $0a = 0 \cdot a = 0$ и $ma = \underbrace{\operatorname{sgn}(m)a + \ldots + \operatorname{sgn}(m)a}_{|m|}$ при $m \in \mathbf{Z}\backslash\{0\}$. Здесь $\operatorname{sgn}(m)a = \begin{cases} a & \text{при } m > 0; \\ -a & \text{при } m < 0. \end{cases}$ Очевидно, что $ma \in K$ для всех $a \in K$, $m \in \mathbf{Z}$.

Определение 4.1.11. Для каждого элемента a ассоциативного кольца $(K, +, \cdot)$ подмножество $Ka + \mathbf{Z}a = \{ka + ma \mid k \in K, m \in \mathbf{Z}\}$ есть левый идеал кольца K, называемый *главным левым идеалом, порожденным элементом a*. Аналогично определяется *главный правый идеал, порожденный элементом a*: $aK + \mathbf{Z}a = \{ak + ma \mid k \in K, m \in \mathbf{Z}\}$. *Двусторонний главный идеал, порожденный элементом a*, является одновременно левым и правым, т. е. имеет вид $KaK + Ka + aK + \mathbf{Z}a = \left\{k_1 a k_1' + \ldots + k_n a k_n' + k'a + ak'' + ma \mid k_i, k_i', k', k'' \in K,\ 1 \le i \le n,\ n \in \mathbf{N},\ m \in \mathbf{Z}\right\}$. Элемент a в этих случаях называется *образующим главного идеала*.

Когда $(K, +, \cdot)$ – ассоциативное кольцо с единицей, для каждого $a \in K$ главные левый, правый и двусторонний идеалы, порожденные a, выглядят соответственно следующим образом:

$$Ka + \mathbf{Z}a = Ka = \{ka \mid k \in K\},\ aK + \mathbf{Z}a = aK = \{ak \mid k \in K\},$$

$$KaK + Ka + aK + \mathbf{Z}a = KaK = \left\{k_1 a k_1' + \ldots + k_n a k_n' \mid k_i, k_i' \in K,\ 1 \le i \le n,\ n \in \mathbf{N}\right\}.$$

В коммутативном кольце понятия главных левого, правого и двустороннего идеалов с образующим элементом a эквивалентны. В таком случае для каждого фиксированного элемента a данные идеалы представляют собой одно и то же множество, которое будем называть просто *главным идеалом, порожденным элементом a*, и обозначать (a).

В собственном идеале J не может быть обратимых элементов кольца K, т. к. иначе $1 \in J$, тогда $J = K$, что приводит к противоречию. Поскольку в поле все элементы, кроме 0, обратимы, то в поле нет собственных идеалов. С другой стороны, необратимые элементы ассоциативного кольца, в том числе и делители нуля, порождают главные собственные идеалы. Отсюда, в частности, также следует, что в поле нет делителей нуля (свойство 1 полей).

Определение 4.1.12. Ассоциативное кольцо, в котором каждый идеал является главным, называется *кольцом главных идеалов*. В некоммутативном случае различают *кольцо главных левых идеалов* и *кольцо главных правых идеалов*.

Теорема 4.1.2. $(\mathbf{Z}, +, \cdot)$ – *кольцо главных идеалов*.

Замечание. Согласно теореме 4.1.2 все идеалы кольца $(\mathbf{Z}, +, \cdot)$ имеют вид (m), где $m \in \mathbf{Z}$. Поскольку $(m) = m\mathbf{Z} = -m\mathbf{Z} = (-m)$ для любого $m \in \mathbf{Z}$, то в дальнейшем для идеалов кольца $(\mathbf{Z}, +, \cdot)$ можно ограничиться обозначением вида (m), где $m \in \mathbf{Z}_{\ge 0}$.

Определение 4.1.13. Собственный идеал кольца называется *максимальным*, если он не содержится ни в каком другом собственном идеале данного кольца.

Очевидно, что идеал (m) является собственным в $(\mathbf{Z}, +, \cdot)$ тогда и только тогда, когда $m > 1$.

Теорема 4.1.3. *Идеал* (m) *максимален в* $(\mathbf{Z}, +, \cdot)$ *тогда и только тогда, когда* m *– простое число*.

Примеры

1. Выяснить, какие из следующих множеств являются кольцами, ассоциативными, коммутативными кольцами, кольцами с единицей и какие – полями относительно указанных операций (если операции не указаны, то подразумеваются обычное сложение и обычное умножение чисел):

а) $K = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$.

В данном случае $K \subset \mathbf{R}$. Как несложно проверить, $(\mathbf{R}, +, \cdot)$ – ассоциативное и коммутативное кольцо, где единицей является число 1, и поле. Проверим по определению подкольца (определение 4.1.7), будет ли $(K, +, \cdot)$ подкольцом $(\mathbf{R}, +, \cdot)$.

Рассмотрим произвольные $a_1, b_1, a_2, b_2 \in \mathbf{Z}$. Тогда:

1) $(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in K$;

2) $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \in K$.

Таким образом, $(K, +, \cdot) < (\mathbf{R}, +, \cdot)$. Значит, $(K, +, \cdot)$ – ассоциативное и коммутативное кольцо, как подкольцо кольца с такими свойствами. Так как $1 = 1 + 0\sqrt{2} \in K$, то единицей $(K, +, \cdot)$ является число 1.

Пусть $a + b\sqrt{2} \neq 0 \Leftrightarrow a \neq 0 \vee b \neq 0$, поскольку $a, b \in \mathbf{Z}$. Тогда в $(\mathbf{R}, +, \cdot)$ имеем

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

$$\left(a + b\sqrt{2}\right)^{-1} \in K \Leftrightarrow \frac{a}{a^2 - 2b^2}, \frac{b}{a^2 - 2b^2} \in \mathbf{Z},$$

что выполняется не для всех $a, b \in \mathbf{Z}$, а только если $a^2 - 2b^2$ – ОД a и b. Например, такое условие не выполняется при $a = 1$, $b = 3$, поэтому $\left(1 + 3\sqrt{2}\right)^{-1} \notin K$.

Итак, $(K, +, \cdot)$ не является полем, поскольку оно не является подполем поля $(\mathbf{R}, +, \cdot)$ согласно определению 4.1.9.

б) $K = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| \, a, b \in \mathbf{Q}\ (\mathbf{R}) \right\}$ относительно обычных операций сложения и умножения матриц.

$K \subset M_2(\mathbf{Q})$ при $a, b \in \mathbf{Q}$ и $K \subset M_2(\mathbf{R})$ при $a, b \in \mathbf{R}$. Как несложно проверить, $M_2(\mathbf{Q})$ и $M_2(\mathbf{R})$ являются ассоциативными, но некоммутативными кольцами с единицей E_2. Проверим по определению подкольца (определение 4.1.7), будет ли $(K, +, \cdot)$ подкольцом кольца $(M_2(\mathbf{Q}), +, \cdot)$ или кольца $(M_2(\mathbf{R}), +, \cdot)$ соответственно. Рассмотрим произвольные $a_1, b_1, a_2, b_2 \in \mathbf{Q}\ (\mathbf{R})$. Тогда:

1) $\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 2(b_1 - b_2) & a_1 - a_2 \end{pmatrix} \in K$;

2) $\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + b_1a_2 \\ 2(b_1a_2 + a_1b_2) & 2b_1b_2 + a_1a_2 \end{pmatrix} \in K$.

Таким образом, $(K, +, \cdot) < (M_2(\mathbf{Q}), +, \cdot)$ или $(K, +, \cdot) < (M_2(\mathbf{R}), +, \cdot)$ соответственно. $(K, +, \cdot)$ – ассоциативное кольцо, как подкольцо кольца с таким свойством. Так как матрица $E_2 \in K$, то $(K, +, \cdot)$ – кольцо с единицей E_2.

Поскольку для произвольных $a_1, b_1, a_2, b_2 \in \mathbf{Q}$ ($\mathbf{R}$) выполняется свойство

$$\begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_2a_1 + 2b_2b_1 & a_2b_1 + b_2a_1 \\ 2(b_2a_1 + a_2b_1) & 2b_2b_1 + a_2a_1 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix},$$

то $(K, +, \cdot)$ – коммутативное кольцо.

Ненулевая матрица в кольце $(M_2(\mathbf{Q}), +, \cdot)$ или $(M_2(\mathbf{R}), +, \cdot)$ обратима тогда и только тогда, когда ее определитель отличен от нуля. Пусть $a, b \in \mathbf{Q}$ ($\mathbf{R}$), причем $a \neq 0 \vee b \neq 0$. Тогда определитель матрицы из K с такими элементами равен $a^2 - 2b^2$. В $\mathbf{R}$ имеем $a^2 - 2b^2 = 0 \Leftrightarrow (a - \sqrt{2}b)(a + \sqrt{2}b) = 0 \Leftrightarrow a = \pm\sqrt{2}b$; в $\mathbf{Q}$ данное равенство возможно только при $a = b = 0$, поскольку $\sqrt{2}$ – иррациональное число. Значит, все ненулевые матрицы из K с элементами $a, b \in \mathbf{R}$ при $a = \pm\sqrt{2}b$ необратимы, откуда следует, что в случае рассмотрения матриц с вещественными элементами $(K, +, \cdot)$ не является полем. Если ограничиться рассмотрением матриц с элементами $a, b \in \mathbf{Q}$, то для произвольной ненулевой матрицы из K имеем

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}^{-1} = \frac{1}{a^2 - 2b^2}\begin{pmatrix} a & -b \\ -2b & a \end{pmatrix} \in K.$$

Значит, в случае рассмотрения матриц с рациональными элементами $(K, +, \cdot)$ является полем.

2. Доказать, что в кольце квадратных матриц порядка $n \in \mathbf{N}$ с элементами из некоторого поля P делителями нуля являются ненулевые вырожденные матрицы (т. е. матрицы с нулевым определителем), и только они.

Несложно проверить, что для любого $n \in \mathbf{N}_{>1}$ система $(M_n(P), +, \cdot)$ является ассоциативным, но некоммутативным в общем случае кольцом с единицей E_n относительно операций сложения и умножения матриц. При $n = 1$ кольцо $M_n(P)$ совпадает с полем P и не имеет делителей нуля.

Рассмотрим случай $n \in \mathbf{N}_{>1}$. Необходимость: из равенства $AB = O$ в $M_n(P)$, где O – нулевая матрица, $A \neq O$, $B \neq O$, следует, что $\det(A) = \det(B) = 0$ в силу свойства 6 колец. Значит, делителями нуля в кольце $M_n(P)$ являются ненулевые вырожденные матрицы. Достаточность: если A – ненулевая вырожденная матрица, то в качестве столбцов матрицы B можно взять ненулевые векторы-решения однородной системы линейных уравнений $A\boldsymbol{x} = \mathbf{0}$. Тогда $AB = O$, причем $B \neq O$, значит, A и B – делители нуля в кольце $M_n(P)$.

3. Установить, будут ли следующие множества подгруппами аддитивных групп, подкольцами или идеалами указанных ниже коммутативных колец:

а) $n\mathbf{Z}[x]$ – множество многочленов, коэффициенты которых кратны числу $n \in \mathbf{Z}$, в кольце $\mathbf{Z}[x]$ целочисленных многочленов с операциями почленного сложения и умножения многочленов.

Поскольку разность и произведение произвольных многочленов из $n\mathbf{Z}[x]$ являются многочленами из $n\mathbf{Z}[x]$, то $n\mathbf{Z}[x]$ является подкольцом $\mathbf{Z}[x]$ по определению 4.1.7. Так как произведение любого многочлена из $\mathbf{Z}[x]$ на произвольный многочлен из $n\mathbf{Z}[x]$ есть многочлен из $n\mathbf{Z}[x]$, то $n\mathbf{Z}[x]$ является идеалом $\mathbf{Z}[x]$ по определению 4.1.10.

б) Множество **N** в кольце $(\mathbf{Z}, +, \cdot)$.

Рассмотрим любые натуральные числа a и b с условием $a \le b$. Тогда $a - b \in \in \mathbf{Z}\backslash\mathbf{N}$. Значит, **N** не является даже подгруппой группы $(\mathbf{Z}, +)$. Следовательно, **N** – не подкольцо и не идеал кольца $(\mathbf{Z}, +, \cdot)$ согласно определениям 4.1.7 и 4.1.10.

в) Множество **Z** в кольце целых гауссовых чисел $A = \{a + bi \mid a, b \in \mathbf{Z}, i^2 = -1\}$ с обычными операциями сложения и умножения в **C**.

Так как $\mathbf{Z} \subset A$ и $(\mathbf{Z}, +, \cdot)$ является кольцом, то **Z** – подкольцо кольца $(A, +, \cdot)$. Рассмотрим любое $b \in \mathbf{Z}\backslash\{0\}$ и $i \in A$, тогда $bi \in A\backslash\mathbf{Z}$. Значит, **Z** не является идеалом кольца $(A, +, \cdot)$ согласно определению 4.1.10.

4. Установить, является ли идеалом кольца (соответственно левым, правым, двусторонним) следующее множество I:

а) $I = I_1\backslash I_2$, где I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние).

Так как $0 \in I_1$, $0 \in I_2$, то $0 \in I_1 \cap I_2$, где 0 – нуль кольца. Значит, $0 \notin I_1\backslash I_2$ для любых идеалов I_1 и I_2 произвольного кольца. Таким образом, $I = I_1\backslash I_2$ во всех случаях не является идеалом кольца и даже подгруппой его аддитивной группы, поскольку I не содержит нуля кольца.

б) $I = \{ j^2 \mid j \in J \}$, где J – идеал кольца (левый или правый, или двусторонний).

В качестве примера рассмотрим коммутативное кольцо $(\mathbf{Z}, +, \cdot)$ и его идеал $J = 2\mathbf{Z} = \{ 2z \mid z \in \mathbf{Z} \}$, являющийся одновременно левым, правым и двусторонним. Тогда $I = \{4z^2 \mid z \in \mathbf{Z} \}$. Множество I не является даже подгруппой группы $(\mathbf{Z}, +)$, поскольку для ненулевых элементов I не содержит им противоположных. Итак, в общем случае I не является идеалом кольца.

в) $I = I_1 \cup I_2$, где I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние).

В качестве примера рассмотрим коммутативное кольцо $(\mathbf{Z}, +, \cdot)$ и его идеалы $2\mathbf{Z} = \{2z \mid z \in \mathbf{Z}\}$ и $3\mathbf{Z} = \{3z \mid z \in \mathbf{Z} \}$, являющиеся одновременно левыми, правыми и двусторонними. Тогда, например, $2 \in 2\mathbf{Z}$, $3 \in 3\mathbf{Z}$, $3 - 2 = 1$; $1 \notin 2\mathbf{Z}$, $1 \notin 3\mathbf{Z} \Rightarrow 1 \notin 2\mathbf{Z} \cup 3\mathbf{Z} = I$. Значит, I не является даже подгруппой группы $(\mathbf{Z}, +)$. Итак, в общем случае I не является идеалом кольца.

Задачи

1. Выяснить, какие из следующих множеств являются кольцами, ассоциативными, коммутативными кольцами, кольцами с единицей и какие – полями относительно указанных операций (если операции не указаны, то подразумеваются обычное сложение и обычное умножение чисел):

а) $\{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\}$;

б) $\left\{\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix}\right\} \subset M_n(\mathbf{R})$, где $n \geq 2$, относительно обычных операций сложения и умножения матриц.

2. Показать, что множество $K = \{(a, b) \mid a,\ b \in \mathbf{Z}\}$ относительно операций, заданных равенствами

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 + b_2),\ (a_1, b_1) \otimes (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2),$$

где «+» и «·» – знаки обычных операций сложения и умножения в **Z**, является ассоциативным и коммутативным кольцом с единицей (1, 1). Найти множество D всех делителей нуля этого кольца.

3. Установить, будут ли следующие множества подгруппами аддитивных групп, подкольцами или идеалами указанных ниже коммутативных колец:

а) множество $B = \{b + bi \mid b \in \mathbf{Z},\ i^2 = -1\}$ в кольце целых гауссовых чисел $(A, +, \cdot)$ (см. пример 3, в);

б) множество $\mathbf{Z}[x]$ целочисленных многочленов в кольце $\mathbf{Q}[x]$ многочленов над полем рациональных чисел;

в) множество I_n многочленов, не содержащих одночленов с x^k для всех $0 \leq k < n$ при фиксированном $n \in \mathbf{N}$, в кольце $\mathbf{Z}[x]$ целочисленных многочленов.

4. Установить, является ли идеалом кольца (соответственно левым, правым, двусторонним) следующее множество I:

а) $I = I_1 \cap I_2$, где I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние);

б) $I = I_1 + I_2 = \{i_1 + i_2 \mid i_1 \in I_1,\ i_2 \in I_2\}$, где I_1, I_2 – идеалы кольца (одновременно левые или правые, или двусторонние).

5. Проверить, что матричное ассоциативное, некоммутативное кольцо $M_2(\mathbf{C})$ с единицей E_2 и делителями нуля содержит подкольцо матриц $C = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right\}$, а C, в свою очередь, содержит подкольцо скалярных матриц $S = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right\}$. Показать, что C – коммутативное кольцо с единицей и без делителей нуля, а S – поле. Проверить также, что подкольцами $M_2(\mathbf{C})$ являются следующие подмножества матриц: $J_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\right\}$, $J_2 = \left\{\begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}\right\}$, $J_3 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right\}$, $J_4 = \left\{\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}\right\}$. Доказать, что J_1–J_4 – некоммутативные кольца без единицы и с делителями нуля.

6. Проверить, что в матричном кольце $M_2(\mathbf{C})$ из задачи 5 подкольца J_1 и J_2 – левые, но не правые идеалы, а J_3 и J_4 – правые, но не левые идеалы.

Ответы

1. а) поле; **б)** ассоциативное и коммутативное кольцо с единицей E_n. **2.** $D = \{(a, 0) \mid a \in \mathbf{Z}\backslash\{0\}\} \cup \{(0, b) \mid b \in \mathbf{Z}\backslash\{0\}\}$. **3. а)** подгруппа аддитивной группы; **б)** подкольцо; **в)** идеал. **4. а)** является; **б)** является.

§4.2. Кольцо полиномов от одной переменной над полем. Неприводимость над полем и корни полиномов

Рассмотрим $P[x] = \left\{ f(x) = \sum_{i=0}^{k} a_i x^i \;\middle|\; a_i \in P,\ 0 \le i \le k,\ k \in \mathbf{Z}_{\ge 0} \right\}$ – множество полиномов (многочленов) от одной переменной x с коэффициентами из поля P. При условии $a_k \neq 0$ коэффициент a_k называется *старшим коэффициентом*, а число $k \in \mathbf{Z}_{\ge 0}$ – *степенью* многочлена $f(x)$. Условимся степень многочлена $f(x)$ обозначать $\deg f$ (англ. *degree* – степень). Тогда $\deg(fg) = \deg f + \deg g$ для всех $f(x), g(x) \in P[x]\backslash\{0\}$. Степень нулевого многочлена часто считают неопределенной либо равной $-\infty$, иногда будем отождествлять нулевой многочлен с элементом $0 \in P$. $(P[x], +, \cdot)$ является кольцом с обычными операциями почленного сложения и умножения полиномов. Это ассоциативное и коммутативное кольцо с единицей $(x^0 = 1 \in P)$ и без делителей нуля, что следует из свойств умножения, правила вычисления старшего коэффициента в $P[x]$ и свойств поля P. По своим свойствам кольцо $P[x]$ близко к кольцу целых чисел.

Теорема 4.2.1. *Обратимыми в кольце* $(P[x], +, \cdot)$ *являются многочлены нулевой степени, и только они, т. е.* $P[x]^* = P^*$.

Теорема 4.2.2 (о делении с остатком). *Для любых двух многочленов* $f(x)$ *и* $g(x) \neq 0$ *из* $P[x]$ *существуют единственные многочлены* $q(x)$ *и* $r(x)$ *из* $P[x]$, *такие, что* $r(x) = 0$ *либо* $\deg r < \deg g$, *и выполняется равенство*

$$f(x) = g(x)q(x) + r(x). \qquad (4.2.1)$$

Теорема 4.2.3. $(P[x], +, \cdot)$ – *кольцо главных идеалов*.

Определение 4.2.1. В равенстве (4.2.1) многочлен $q(x)$ называют *частным* (*неполным частным*, если $r(x) \neq 0$), а $r(x)$ – *остатком* от деления $f(x)$ на $g(x)$. Если $r(x) = 0$, то говорят, что $g(x)$, $q(x) \neq 0$ – *делители* (или *множители*) полинома $f(x)$. Также в этом случае говорят, что $g(x)$ и $q(x) \neq 0$ *делят* $f(x)$, и обозначают $g(x) \mid f(x)$, или говорят, что $f(x)$ *кратно* (*делится* на) $g(x)$ и $q(x) \neq 0$, и обозначают $f(x) \vdots g(x)$.

Если $g(x) \mid f(x)$ и $0 < \deg g < \deg f$, то многочлен $g(x)$ называют *нетривиальным делителем* многочлена $f(x)$. Очевидно, произвольный элемент $\alpha \in P^*$ является делителем любого многочлена $f(x)$ из $P[x]$. При $f(x) \neq 0$ многочлен $\alpha f(x)$ – также делитель $f(x)$. Поэтому такие делители называют *тривиальными*.

Будем обозначать $g(x) \nmid f(x)$, если $g(x) \neq 0$ не делит $f(x)$, и $f(x) \not\vdots g(x)$, если $f(x)$ не делится на $g(x) \neq 0$.

Для нахождения частного и остатка от деления многочленов в $P[x]$ можно использовать метод деления «уголком», аналогичный методу деления целых чисел.

Свойства делимости многочленов:

1. $g(x) \mid 0,\ \forall\, g(x) \neq 0$.

2. $\alpha \mid f(x),\ \forall\, \alpha \in P^*,\ \forall\, f(x) \in P[x]$.

3. $g(x) \mid f(x)\ \&\ f(x) \mid h(x) \Rightarrow g(x) \mid h(x)$ – свойство транзитивности.

4. $g(x) \mid f(x)$ & $f(x) \mid g(x) \Leftrightarrow f(x) = \alpha g(x)$ для некоторого $\alpha \in P^*$.

5. Если $g(x) \mid f_i(x)$, $i = \overline{1, s}$, то $g(x) \mid \sum_{i=1}^{s} f_i(x) w_i(x)$, где $\forall\, s \in \mathbf{N}$, $\forall\, w_i(x) \in P[x]$.

6. Если в равенстве $f_1(x) + \ldots + f_s(x) = g_1(x) + \ldots + g_t(x)$, $\forall\, s, t \in \mathbf{N}$, все многочлены, кроме, быть может, одного, делятся на $d(x)$, то и этот многочлен также делится на $d(x)$.

7. $g(x) \mid f(x) \Leftrightarrow \alpha g(x) \mid \beta f(x)$, $\forall\, \alpha, \beta \in P^*$.

Определение 4.2.2. *Общим делителем* (*ОД*) многочленов $f_1(x)$, $f_2(x)$,…, $f_s(x) \in P[x]$, где $s \in \mathbf{N}_{\geq 2}$, называется многочлен $d(x) \in P[x]$, такой, что $d(x) \mid f_i(x)$, $i = \overline{1, s}$. *Наибольшим общим делителем* (*НОД*) многочленов $f_1(x)$, $f_2(x)$,…, $f_s(x)$, хотя бы один из которых отличен от нулевого, называется такой их нормированный общий делитель (со старшим коэффициентом 1), который делится на любой другой их общий делитель. Таким образом, нормированность гарантирует однозначность НОД. Его обозначают НОД$\big(f_1(x), f_2(x),\ldots, f_s(x)\big)$ или $\big(f_1(x), f_2(x),\ldots, f_s(x)\big)$, если последнее не вызывает разночтений.

Очевидно, что если $g(x) \mid f(x)$, то $\big(f(x), g(x)\big) = b_m^{-1} g(x) = \tilde{g}(x)$ – многочлен, полученный нормированием $g(x)$, где b_m – старший коэффициент $g(x)$, $\deg g = m$.

Теорема 4.2.4. *НОД многочленов $f(x)$ и $g(x)$ из кольца $P[x]$ при условии, что* $\deg g \leq \deg f$ *и $g(x) \nmid f(x)$, совпадает с нормированным последним отличным от нуля остатком от деления $\tilde{r}_n(x)$ из следующей цепочки равенств*:

$$f(x) = g(x)q_1(x) + r_1(x),$$
$$g(x) = r_1(x)q_2(x) + r_2(x), \text{ если } r_1(x) \neq 0,$$
$$r_1(x) = r_2(x)q_3(x) + r_3(x), \text{ если } r_2(x) \neq 0,$$
$$\ldots$$
$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x), \text{ если } r_{n-1}(x) \neq 0,$$
$$r_{n-1}(x) = r_n(x)q_{n+1}(x), \text{ если } r_n(x) \neq 0.$$

Теорема 4.2.4 является аналогом для $P[x]$ алгоритма Евклида нахождения НОД целых чисел (теоремы 1.1.2). Аналог расширенного алгоритма Евклида (см. §1.1) также применим в кольце $P[x]$.

НОД многочленов вычисляется рекурсивно для любого $s \geq 3$:

$$\big(f_1(x), f_2(x),\ldots, f_s(x)\big) = \big(\big(f_1(x), f_2(x),\ldots, f_{s-1}(x)\big), f_s(x)\big).$$

Теорема 4.2.5. *Если $d(x) = \big(f_1(x), f_2(x),\ldots, f_s(x)\big)$, где $s \geq 2$, то в $P[x]$ существуют многочлены $w_1(x)$, $w_2(x)$,…, $w_s(x)$, такие, что*

$$d(x) = \sum_{i=1}^{s} f_i(x) w_i(x). \qquad (4.2.2)$$

Определение 4.2.3. Равенство (4.2.2) называют *соотношением Безу* для наибольшего общего делителя многочленов.

Замечание. Многочлены $w_1(x)$, $w_2(x)$,…, $w_s(x) \in P[x]$ в (4.2.2) не являются единственными с таким условием. Так, например, легко видеть, что при $s = 2$, если $d(x) = f_1(x)w_1(x) + f_2(x)w_2(x)$, то для любого многочлена $q(x) \in P[x]$ много-

члены $w_1(x) + q(x)f_2(x)/d(x)$ и $w_2(x) - q(x)f_1(x)/d(x)$ из $P[x]$ также являются коэффициентами данного соотношения Безу при $f_1(x)$ и $f_2(x)$ соответственно.

Определение 4.2.4. *Общим кратным* (*ОК*) ненулевых многочленов $f_1(x)$, $f_2(x),\ldots, f_s(x) \in P[x]$, где $s \in \mathbf{N}_{\geq 2}$, называется многочлен $m(x) \in P[x]$, такой, что $m(x) \vdots f_i(x), i = \overline{1, s}$. *Наименьшим общим кратным* (*НОК*) ненулевых многочленов $f_1(x), f_2(x),\ldots, f_s(x)$ называется такое их нормированное общее кратное (со старшим коэффициентом 1), на которое делится любое другое их общее кратное. Таким образом, нормированность гарантирует однозначность НОК. Его обозначают НОК$(f_1(x), f_2(x),\ldots, f_s(x))$ или $[f_1(x), f_2(x),\ldots, f_s(x)]$, если последнее не вызывает разночтений.

Очевидно, что если $g(x) \mid f(x)$, то при $f(x) \neq 0$ имеем $[f(x), g(x)] = a_k^{-1} f(x) = \tilde{f}(x)$, где a_k – старший коэффициент $f(x)$, $\deg f = k$.

НОК многочленов вычисляется рекурсивно для любого $s \geq 3$:

$$[f_1(x), f_2(x),\ldots, f_s(x)] = [[f_1(x), f_2(x),\ldots, f_{s-1}(x)], f_s(x)].$$

Определение 4.2.5. Если $(f_1(x), f_2(x),\ldots, f_s(x)) = 1$, где $s \geq 2$, то многочлены $f_1(x), f_2(x),\ldots, f_s(x)$ называются *взаимно простыми*.

Теорема 4.2.6 (критерий взаимной простоты многочленов). *Многочлены $f_1(x), f_2(x),\ldots, f_s(x) \in P[x]$, где $s \geq 2$, взаимно просты тогда и только тогда, когда найдутся такие многочлены $w_1(x), w_2(x),\ldots, w_s(x) \in P[x]$, что* $\sum_{i=1}^{s} f_i(x) w_i(x) = 1$.

Из этого критерия вытекает ряд важных следствий как свойств взаимно простых многочленов.

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

Следствие 2. *Многочлен $h(x)$ взаимно прост с каждым из многочленов $f(x)$ и $g(x)$ тогда и только тогда, когда он взаимно прост с их произведением $f(x)g(x)$.*

Определение 4.2.6. Многочлен $f(x)$ степени $n \in \mathbf{N}$ называется *неприводимым в $P[x]$* (*неприводимым над полем P*), если в любом его представлении вида $f(x) = g(x)q(x)$ его сомножители $g(x), q(x) \in P[x]$ тривиальны, т. е. один из них является элементом P^*. В противном случае многочлен $f(x)$ называется *приводимым в кольце $P[x]$* (*приводимым над полем P*).

Очевидно, что все многочлены первой степени являются неприводимыми в $P[x]$ согласно данному определению.

Теорема 4.2.7 (о разложении на множители). *Всякий многочлен $f(x) \in P[x]$ степени $n \geq 1$ представи́м в виде*

$$f(x) = a_n p_1(x) \ldots p_t(x), \qquad (4.2.3)$$

где $p_i(x)$ – нормированные неприводимые над P полиномы, $1 \leq i \leq t$;

a_n – старший коэффициент $f(x)$.

Такое представление единственно с точностью до порядка следования множителей.

Определение 4.2.7. Если в разложении (4.2.3) объединить одинаковые сомножители-многочлены в степени, то получится разложение, называемое *каноническим разложением многочлена* $f(x)$ *над полем* P:

$$f(x) = a_n p_1^{\gamma_1}(x) \dots p_s^{\gamma_s}(x),$$

где $\gamma_i \in \mathbf{N}$, $1 \le i \le s$, $p_i(x) \ne p_j(x)$ при $i \ne j$.

Теорема 4.2.8. *В* $P[x]$ *существует бесконечно много неприводимых многочленов.*

Теорема 4.2.9. *Идеал* $(f(x))$ *максимален в* $(P[x], +, \cdot)$ *тогда и только тогда, когда* $f(x)$ *неприводим над полем* P.

Определение 4.2.8. Элемент $c \in P$ или некоторого расширения поля P называется *корнем многочлена* $f(x) \in P[x]$, если $f(c) = 0$. Поле P называется *алгебраически замкнутым*, если всякий многочлен $f(x) \in P[x]$ при $\deg f \ge 1$ имеет в P корень.

Определение 4.2.9. Пусть $c \in P$ – корень полинома $f(x)$. *Кратностью корня* c называется такое число $l \in \mathbf{N}$, что $(x-c)^l \mid f(x)$, а $(x-c)^{l+1} \nmid f(x)$. При $l = 1$ корень называется *простым*, при $l > 1$ – *кратным*.

Теорема 4.2.10 (Э. Безу). *Для любого* $f(x) \in P[x]$ *и любого* $c \in P$ *значение* $f(c)$ *равно остатку от деления* $f(x)$ *на* $x - c$.

Следствие 1 (критерий корня). *Элемент* $c \in P$ *является корнем многочлена* $f(x) \in P[x]$ *тогда и только тогда, когда* $(x-c) \mid f(x)$.

Следствие 2. *Неприводимый полином кольца* $P[x]$ *степени* $n \ge 2$ *не имеет корней в поле* P.

Следствие 3. *Определение алгебраически замкнутого поля* P *эквивалентно тому, что любой многочлен* $f(x) \in P[x]$ *при* $\deg f \ge 1$ *имеет все корни в* P. *Неприводимыми над алгебраически замкнутым полем являются многочлены первой степени, и только они.*

Следствие 4. *Если* P *– алгебраически замкнутое поле, то для любого многочлена* $f(x) \in P[x]$ *при* $\deg f = n \in \mathbf{N}$ *справедливо каноническое разложение*:

$$f(x) = a_n (x - \alpha_1)^{l_1} \dots (x - \alpha_s)^{l_s}, \qquad (4.2.4)$$

где a_n *– старший коэффициент* $f(x)$;

$\alpha_1, \dots, \alpha_s$ *– все различные корни* $f(x)$ *в* P *соответственно кратностей* $l_1, \dots, l_s$.

В этом случае $l_1 + \dots + l_s = n$, *т. е. число всех корней ненулевого многочлена в алгебраически замкнутом поле* (*с учетом их кратностей*) *равно степени данного многочлена.*

Теорема 4.2.11 (о числе корней многочлена). *Пусть* $f(x) \in P[x]$ *и* $\deg f = n \in \mathbf{N}$. *Если* $\alpha_1, \dots, \alpha_s$ *– различные корни* $f(x)$ *в поле* P *соответственно кратностей* $l_1, \dots, l_s$, *где* $s \in \mathbf{N}$, *то* $f(x)$ *делится на произведение* $(x - \alpha_1)^{l_1} \dots (x - \alpha_s)^{l_s}$. *При этом справедливо неравенство* $l_1 + \dots + l_s \le n$, *которое означает, что число корней ненулевого многочлена в поле* (*с учетом их кратностей*) *не превосходит степени данного многочлена.*

Удобной для деления многочлена $f(x) \in P[x]$ при $\deg f = n \in \mathbf{N}$ на двучлен (бином) $x - c$, где $c \in P$, является *схема Горнера*. Пусть $f(x) = (x - c)g(x) + b_0$, где $f(x) = \sum_{i=0}^{n} a_i x^i,\ a_n \neq 0,\ g(x) = \sum_{i=1}^{n} b_i x^{i-1},\ b_0 = f(c)$. Вычисление коэффициентов частного от деления $g(x)$ производится рекуррентно по следующим формулам:

$$b_n = a_n,$$
$$b_{n-1} = a_{n-1} + cb_n,$$
$$\dots$$
$$b_0 = a_0 + cb_1.$$

Таким образом, $b_i = a_i + cb_{i+1},\ i = n-1, \dots, 0$. Результаты вычислений по схеме Горнера обычно представляются в виде таблицы, изображенной на рис. 4.2.1, которая имеет более компактную форму по сравнению с традиционной записью метода деления на двучлен «уголком».

	a_n	a_{n-1}	…	a_1	a_0
c	a_n	b_{n-1}	…	b_1	b_0

Рис. 4.2.1

Схема Горнера представляет собой алгоритм вычисления значения многочлена $f(x)$ при заданном значении переменной $x = c$, а также позволяет осуществить проверку, является ли c корнем $f(x)$. С помощью схемы Горнера можно определять кратность корня многочлена $f(x)$, находить коэффициенты при разложении $f(x)$ по степеням $x - c$. В этих случаях частное $g(x)$ при $\deg g \geq 1$ делится на $x - c$ и аналогично заполняется следующая строка таблицы на рис. 4.2.1 и т. д., но число столбцов каждый раз становится на один крайний правый меньше.

Важными частными случаями поля P являются числовые поля: **C**, **R** и **Q**. Отметим, что $(\mathbf{Q}[x], +, \cdot) < (\mathbf{R}[x], +, \cdot) < (\mathbf{C}[x], +, \cdot)$.

Теорема 4.2.12 (основная теорема алгебры). *Поле комплексных чисел* **C** *алгебраически замкнуто*.

Следствие 1. *Любой многочлен* $f(x) \in \mathbf{C}[x]$ *при* $\deg f \geq 1$ *имеет все корни в* **C** *и справедливо каноническое разложение* (4.2.4). *Неприводимыми над* **C** *являются многочлены первой степени, и только они*.

Следствие 2. *Любой многочлен* $f(x) \in \mathbf{R}[x]$ *при* $\deg f > 2$ *приводи́м над* **R**. *Неприводимыми над* **R** *являются многочлены первой степени и второй степени с отрицательными дискриминантами, и только они*.

Любой многочлен из $\mathbf{Q}[x]$ домножением на НОК знаменателей его коэффициентов приводится к многочлену из $\mathbf{Z}[x]$. Следовательно, вопросы о существовании корня в **Q** и неприводимости многочлена в $\mathbf{Q}[x]$ сводятся к вопросам о существовании корня в **Q** и неприводимости над **Q** полученного таким образом многочлена из $\mathbf{Z}[x]$.

Если полином имеет вид $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_l x^l$, где $\deg f = n \geq 1$, $0 < l \leq n,\ a_l \neq 0$, то, очевидно, 0 является его корнем кратности l. В таком случае

можно разделить $f(x)$ на x^l и рассматривать вопросы о корнях полученного частного и его неприводимости, если его степень ненулевая.

Теорема 4.2.13. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$, *где* $n \geq 1$, $a_n \neq 0$, $a_0 \neq 0$. *Тогда если* $\alpha/\beta \in \mathbf{Q}$, *где* $\alpha \in \mathbf{Z}$, $\beta \in \mathbf{N}$, $(\alpha, \beta) = 1$, *является корнем* $f(x)$, *то* $\alpha \mid a_0$ *и* $\beta \mid a_n$.

Следствие. *Если* $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$, *где* $n \geq 1$, $a_0 \neq 0$, *то все рациональные корни* $f(x)$ *являются целочисленными и находятся среди делителей* a_0.

Отметим следующее важное свойство, которое вытекает из свойства 7 делимости многочленов и свойств взаимно простых чисел в **Z**: если $f(x) \in \mathbf{Z}[x]$ допускает разложение на множители из $\mathbf{Q}[x]$, то $f(x)$ допускает разложение на множители из $\mathbf{Z}[x]$. Отсюда следует, что $f(x) \in \mathbf{Z}[x]$ неприводим над **Q** тогда и только тогда, когда $f(x)$ неприводим над **Z**, т. е. не допускает разложения на нетривиальные множители с коэффициентами из **Z**.

Теорема 4.2.14 (признак Эйзенштейна). *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots$ $\ldots + a_1 x + a_0 \in \mathbf{Z}[x]$, *где* $n > 1$. *Если можно подобрать простое число* p, *удовлетворяющее условиям*:

1) $p \nmid a_n$;

2) $p \mid a_i$, $0 \leq i \leq n-1$;

3) $p^2 \nmid a_0$,

то $f(x)$ *неприводим над* **Q**.

Важными частными случаями поля P являются также конечные поля, называемые еще *полями Галуа*. В дальнейшем для конечного поля, состоящего из q элементов, будет использоваться обозначение $\boldsymbol{F_q}$. Поле $\boldsymbol{F_p}$ будем отождествлять с $(\mathbf{Z}/p\mathbf{Z}, +, \cdot)$ для любого простого числа p. Отметим два следующих фундаментальных факта:

1. Поле $\boldsymbol{F_q}$ существует тогда и только тогда, когда $q = p^m$, где p – простое число, $m \in \mathbf{N}$.

2. В кольце $\boldsymbol{F_q}[x]$ существуют неприводимые многочлены любой натуральной степени n.

Согласно определению 4.2.6, теореме 4.2.7 и следствиям 1 и 2 из теоремы 4.2.10, неприводимыми в $P[x]$ являются все многочлены первой степени и все многочлены второй и третьей степеней, не имеющие корней в поле P, т. е. не имеющие делителей первой степени в $P[x]$. Неприводимыми в $P[x]$ являются все многочлены четвертой степени, не имеющие корней в P, а также не кратные нормированным неприводимым многочленам второй степени из $P[x]$. В общем случае неприводимыми над P являются все многочлены n-й степени, не имеющие в $P[x]$ нормированных неприводимых делителей степени k, где $1 \leq k \leq [n/2]$, $n \geq 2$. Данная процедура «просеивания» для определения неприводимых многочленов напоминает «решето» Эратосфена для проверки натуральных чисел на простоту. Она удобна для поиска неприводимых многочленов и разложения многочленов на неприводимые множители над конечными полями.

Примеры

1. Найти НОД полиномов $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ и $g(x) = 3x^3 + 10x^2 + 2x - 3$ с помощью алгоритма Евклида:

а) в кольце $\mathbf{Q}[x]$.

$$
\begin{array}{r|l}
x^4+3x^3-x^2-4x-3 & 3x^3+10x^2+2x-3 \\
\underline{-\,x^4+10/3x^3+2/3x^2-x} & 1/3x-1/9 \\
-1/3x^3-5/3x^2-3x-3 & \\
\underline{-\,-1/3x^3-10/9x^2-2/9x+1/3} & \\
3x^3+10x^2+2x-3 & -5/9x^2-25/9x-10/3 \quad — r_1(x) \\
\underline{-\,3x^3+15x^2+18x} & -27/5x+9 \\
-5x^2-16x-3 & \\
\underline{-\,-5x^2-25x-30} & \\
-5/9x^2-25/9x-10/3 & 9x+27 \quad — r_2(x) \\
\underline{-\,-5/9x^2-5/3x} & -5/81x-10/81 \\
-10/9x-10/3 & \\
\underline{-\,-10/9x-10/3} & \\
0 &
\end{array}
$$

$(f(x), g(x)) = \tilde{r}_2(x) = 9^{-1} r_2(x) = 1/9(9x+27) = x+3;$

б) в кольце $\boldsymbol{F_7}[x]$.

Поле $\boldsymbol{F_7}$ – это множество {0, 1, 2, 3, 4, 5, 6} с заданными на нем операциями сложения и умножения, отождествляемое с $(\mathbf{Z}/7\mathbf{Z}, +, \cdot)$ (см. §1.4, пример 1, а). Поэтому $f(x) = x^4 + 3x^3 + 6x^2 + 3x + 4$, $g(x) = 3x^3 + 3x^2 + 2x + 4$ в $\boldsymbol{F_7}[x]$.

$$
\begin{array}{r|l}
x^4+3x^3+6x^2+3x+4 & 3x^3+3x^2+2x+4 \\
\underline{-\,x^4+x^3+3x^2+6x} & 5x+3 \\
2x^3+3x^2+4x+4 & \\
\underline{-\,2x^3+2x^2+6x+5} & \\
3x^3+3x^2+2x+4 & x^2+5x+6 \quad — r_1(x) \\
\underline{-\,3x^3+x^2+4x} & 3x+2 \\
2x^2+5x+4 & \\
\underline{-\,2x^2+3x+5} & \\
x^2+5x+6 & 2x+6 \quad — r_2(x) \\
\underline{-\,x^2+3x} & 4x+1 \\
2x+6 & \\
\underline{-\,2x+6} & \\
0 &
\end{array}
$$

$(f(x), g(x)) = \tilde{r}_2(x) = 2^{-1} r_2(x) = 4(2x+6) = x+3.$

2. Найти канонические разложения полиномов над полем $\boldsymbol{F_2}$:

а) всех полиномов второй степени из $\boldsymbol{F_2}[x]$.

Применяя алгоритм «просеивания», получаем

$f_1(x) = x^2,\ f_2(x) = x^2+1 = (x+1)^2,\ f_3(x) = x^2+x = x(x+1),\ f_4(x) = x^2+x+1.$

Так как $f_4(0) = f_4(1) = 1 \neq 0$, то полином $f_4(x)$ неприводим над $\boldsymbol{F_2}$;

б) всех полиномов третьей степени из $\boldsymbol{F_2}[x]$.

Применяя алгоритм «просеивания» и схему Горнера, получаем

$$f_1(x) = x^3,\ f_2(x) = x^3+1 = (x+1)(x^2+x+1),\ f_3(x) = x^3+x = x(x+1)^2,$$
$$f_4(x) = x^3+x+1,\ f_5(x) = x^3+x^2 = x^2(x+1),\ f_6(x) = x^3+x^2+1,$$
$$f_7(x) = x^3+x^2+x = x(x^2+x+1),\ f_8(x) = x^3+x^2+x+1 = (x+1)^3.$$

Так как $f_4(0) = f_4(1) = 1 \neq 0$, $f_6(0) = f_6(1) = 1 \neq 0$, то полиномы $f_4(x)$ и $f_6(x)$ неприводимы над $\boldsymbol{F_2}$.

3. Установить, максимален ли идеал $(f(x))$ в кольце полиномов:

а) (x^4+1) в $\mathbf{C}[x]$, $\mathbf{R}[x]$, $\mathbf{Q}[x]$.

Так как $\deg f = 4$, то согласно следствиям 1 и 2 из теоремы 4.2.12 $f(x)$ приводи́м над **C** и **R**, следовательно, $(f(x))$ не является максимальным в $\mathbf{C}[x]$ и в $\mathbf{R}[x]$.

$$f(x) = x^4 + 2x^2 + 1 - 2x^2 = \left(x^2+1\right)^2 - \left(\sqrt{2}x\right)^2 = \left(x^2 - \sqrt{2}x + 1\right)\left(x^2 + \sqrt{2}x + 1\right) = p_1(x)p_2(x).$$

Многочлен $f(x)$ приводи́м над **R**, но многочлены $p_1(x)$ и $p_2(x)$ уже неприводимы над **R**, как имеющие отрицательные дискриминанты. В то же время $f(x)$ неприводим над **Q**. Если бы $f(x)$ был приводи́м над **Q**, то его разложение на неприводимые множители в $\mathbf{Q}[x]$, а значит, и в $\mathbf{R}[x]$, было бы отлично от разложения $f(x) = p_1(x)p_2(x)$, чего быть не может в силу теоремы 4.2.7.

Итак, (x^4+1) не является максимальным идеалом в $\mathbf{C}[x]$ и в $\mathbf{R}[x]$, но является максимальным идеалом в $\mathbf{Q}[x]$.

б) $(x^6 + x^5 + x^4 + x + 1)$ в $\boldsymbol{F_2}[x]$.

0 и 1 не являются корнями $f(x) = x^6 + x^5 + x^4 + x + 1$ в $\boldsymbol{F_2}$.

$x^2 + x + 1$ – единственный неприводимый многочлен второй степени над $\boldsymbol{F_2}$ (см. пример 2, а). Применяя метод деления «уголком» в $\boldsymbol{F_2}[x]$, имеем

$$f(x) = (x^2 + x + 1)x^4 + x + 1 \Rightarrow x^2 + x + 1 \nmid f(x).$$

Неприводимыми многочленами третьей степени над $\boldsymbol{F_2}$ являются $x^3 + x + 1$ и $x^3 + x^2 + 1$ (см. пример 2, б). Применяя метод деления «уголком» в $\boldsymbol{F_2}[x]$, имеем

$$f(x) = (x^3 + x + 1)(x^3 + x^2) + x^2 + x + 1 \Rightarrow x^3 + x + 1 \nmid f(x);$$

$$f(x) = (x^3 + x^2 + 1)(x^3 + x) + 1 \Rightarrow x^3 + x^2 + 1 \nmid f(x).$$

Значит, $f(x)$ неприводим над $\boldsymbol{F_2}$ и $(f(x))$ – максимальный идеал в $\boldsymbol{F_2}[x]$.

в) (x^4+1) в $\boldsymbol{F_2}[x]$.

1 является корнем $f(x) = x^4 + 1$ в $\boldsymbol{F_2}$. Имеем разложение $f(x) = (x+1)^4$ в $\boldsymbol{F_2}[x]$. Значит, многочлен $f(x)$ приводи́м над $\boldsymbol{F_2}$ и $(f(x))$ – немаксимальный идеал в $\boldsymbol{F_2}[x]$.

г) $(x^4 + 4)$ в $\mathbf{Q}[x]$.

Многочлен $f(x) = x^4 + 4$ не имеет корней в **Q** согласно следствию из теоремы 4.2.13, поскольку $f(\pm 1) = 5 \neq 0$, $f(\pm 2) = 20 \neq 0$, $f(\pm 4) = 260 \neq 0$.

$$f(x) = x^4 + 4x^2 + 4 - 4x^2 = \left(x^2+2\right)^2 - (2x)^2 = \left(x^2 - 2x + 2\right)\left(x^2 + 2x + 2\right).$$

Многочлен $x^4 + 4$ приводи́м над **Q**, следовательно, $(x^4 + 4)$ не является максимальным идеалом в $\mathbf{Q}[x]$.

д) $(x^3 + x + 1)$ в $\boldsymbol{F_2}[x]$, $\mathbf{Q}[x]$.

Так как многочлен $x^3 + x + 1$ неприводим над $\boldsymbol{F_2}$ (см. пример 2, б), то $(x^3 + x + 1)$ – максимальный идеал в $\boldsymbol{F_2}[x]$.

Многочлен $f(x) = x^3 + x + 1$ не имеет корней в **Q** согласно следствию из теоремы 4.2.13, поскольку $f(1) = 3 \neq 0$, $f(-1) = -1 \neq 0$. Значит, $f(x)$ неприводим над **Q** и $(f(x))$ – максимальный идеал в $\mathbf{Q}[x]$.

е) $(2x^5+3x^2-9x+15)$ в $\mathbf{Q}[x]$.

3 – простое число, $3 \mid 15$, $3 \mid (-9)$, $3 \mid 3$, но $3 \nmid 2$, $3^2 = 9 \nmid 15$. Значит, по признаку Эйзенштейна (теорема 4.2.14) многочлен $f(x)$ неприводим над $\mathbf{Q}$, следовательно, $(f(x))$ – максимальный идеал в $\mathbf{Q}[x]$.

Задачи

1. Найти НОД полиномов с помощью алгоритма Евклида:

а) $f(x) = x^3 + x^2 + 2x + 2$, $g(x) = x^2 + x + 1$ в $\mathbf{Q}[x]$ и в $\boldsymbol{F_3}[x]$;

б) $f(x) = 5x^3 + x^2 + 5x + 1$, $g(x) = 5x^2 + 21x + 4$ в $\mathbf{Q}[x]$ и в $\boldsymbol{F_5}[x]$.

Указание: использовать алгоритм Евклида и метод деления «уголком».

2. Найти каноническое разложение полинома над полем:

а) $x^5 + x^3 + x^2 + 1$ над $\boldsymbol{F_2}$;

б) $x^4 + x^3 + x + 2$ над $\boldsymbol{F_3}$.

Указание: использовать алгоритм «просеивания», схему Горнера и метод деления «уголком» в $\boldsymbol{F_2}[x]$ и в $\boldsymbol{F_3}[x]$ соответственно.

Ответы

1. а) 1 и $x+2$ соответственно; **б)** $x+1/5$ и 1 соответственно. **2. а)** $(x+1)^3(x^2+ + x+1)$; **б)** $(x^2+1)(x^2+x+2)$.

§4.3. Факторкольца. Гомоморфизмы колец. Характеристика

Пусть $(K, +, \cdot)$ – кольцо с двусторонним идеалом I, при этом I является нормальной подгруппой аддитивной абелевой группы $(K, +)$. На K может быть определено отношение сравнения по модулю I.

Определение 4.3.1. Элементы $a, b \in K$ называются *сравнимыми по модулю идеала I*, если $a - b \in I$, т. е. $a = b + i$ для некоторого $i \in I$.

Это отношение является отношением эквивалентности (рефлексивно, симметрично, транзитивно) и, следовательно, разбивает K на непересекающиеся классы эквивалентности сравнимых по модулю I элементов – *классы вычетов по модулю идеала I*. Для любого $a \in K$ *класс вычетов с представителем a* имеет вид $\bar{a} = a + I = \{a + i \mid i \in I\}$. Множество всех различных классов вычетов $K/I = \{\bar{0} = I, \bar{a} = a + I, \bar{b} = b + I, \ldots\}$ называется *факторможеством* кольца K по идеалу I.

Теорема 4.3.1. *Пусть* $(K, +, \cdot)$ *– кольцо и* $I \lhd K$. *Тогда факторможество* K/I *является кольцом относительно индуцированных операций сложения и умножения классов вычетов по модулю идеала I*:

$$\bar{a} \oplus \bar{b} = \overline{a + b},$$
$$\bar{a} \otimes \bar{b} = \overline{a \cdot b}$$

для любых $a, b \in K$.

Определение 4.3.2. Кольцо $(K/I, \oplus, \otimes)$ из теоремы 4.3.1 называется *факторкольцом* кольца K по двустороннему идеалу I.

Поскольку операции $\oplus$ и $\otimes$ полностью определяются сложением и умножением в кольце $(K, +, \cdot)$, то свойства этих операций переносятся на $(K/I, \oplus, \otimes)$. Если K – ассоциативное кольцо, кольцо с единицей, коммутативное кольцо, то и $(K/I, \oplus, \otimes)$ также будет соответственно ассоциативным кольцом, кольцом с единицей $\bar{1}$, коммутативным кольцом.

Рассмотрим в кольце $P[x]$ произвольный собственный идеал $I = (g(x))$, порожденный полиномом $g(x)$ степени $n \geq 1$. Согласно теореме 4.2.2 в один класс вычетов по модулю I попадают те и только те полиномы, которые имеют один и тот же остаток $r(x)$ от деления на $g(x)$. Следовательно, фактормножество $P[x]/I$ состоит из классов вычетов $\overline{r(x)} = r(x) + I = \{ r(x) + g(x)h(x) \mid h(x) \in P[x] \}$, где $r(x) = 0$ либо $\deg r < \deg g$. По теореме 4.3.1 результатом сложения или умножения таких классов вычетов является соответственно класс вычетов, представитель которого есть остаток от деления на $g(x)$ суммы или произведения представителей данных классов в $P[x]$. В частности, фактормножество $\boldsymbol{F_q}[x]/(g(x))$ конечно, поэтому сложение и умножение в факторкольце $(\boldsymbol{F_q}[x]/(g(x)), \oplus, \otimes)$ можно задать в виде таблиц Кэли.

Лемма 4.3.1. *Мощность фактормножества* $\boldsymbol{F_q}[x]/(g(x))$ *при* $\deg g = n \geq 1$ *равна* q^n.

Теорема 4.3.2. *Факторкольцо* $(K/I, \oplus, \otimes)$ *ассоциативного и коммутативного кольца с единицей* $(K, +, \cdot)$ *по собственному идеалу* I *является полем тогда и только тогда, когда* I *– максимальный идеал.*

Следствие 1. *Факторкольцо* $(\mathbf{Z}/n\mathbf{Z}, \oplus, \otimes)$ *является полем тогда и только тогда,* когда n *– простое число.*

Следствие 2. *Факторкольцо* $(P[x]/(g(x)), \oplus, \otimes)$ *является полем тогда и только тогда, когда* $g(x)$ *– неприводимый полином над полем* P.

Определение 4.3.3. Пусть $(K_1, +, \cdot)$ и $(K_2, \dot{+}, \bullet)$ – два кольца. *Гомоморфизмом колец* называется всякая функция $f: K_1 \to K_2$, обладающая следующими свойствами для любых $a, b \in K_1$:

1) $f(a + b) = f(a) \dot{+} f(b)$;

2) $f(a \cdot b) = f(a) \bullet f(b)$.

Определение 4.3.4. Инъективный гомоморфизм колец называется *мономорфизмом* (или *вложением*), сюръективный – *эпиморфизмом*, биективный – *изоморфизмом*. Всякий гомоморфизм $f: K \to K$ называют *эндоморфизмом кольца* K, а взаимно однозначный эндоморфизм – *автоморфизмом*.

Изоморфные кольца будем обозначать $(K_1, +, \cdot) \cong (K_2, \dot{+}, \bullet)$ или $K_1 \cong K_2$.

Отношение изоморфизма на множестве всех колец является отношением эквивалентности: оно рефлексивно, симметрично и транзитивно. Таким образом, все множество колец разбивается на непересекающиеся классы попарно изоморфных объектов.

Определение 4.3.5. Пусть $f: K_1 \to K_2$ – гомоморфизм колец. *Образом гомоморфизма* $f: K_1 \to K_2$ называется множество $\operatorname{Im} f = \{ f(a) \in K_2 \mid a \in K_1 \} = E(f)$.

Ядром гомоморфизма f называется множество $\operatorname{Ker} f = \{a \in K_1 \mid f(a) = 0_{K_2}\}$, где 0_{K_2} – нейтральный элемент группы $(K_2, \breve{+})$.

Очевидно, что когда $f: K_1 \to K_2$ – мономорфизм колец, $K_1 \cong \operatorname{Im} f$.

Свойства гомоморфизмов колец:

1. Композиция гомоморфизмов колец – гомоморфизм колец.

2. Если $f: K_1 \to K_2$ – гомоморфизм колец, то $\operatorname{Im} f$ – подкольцо K_2.

3. Если $f: K_1 \to K_2$ – гомоморфизм колец, то $f(0_{K_1}) = 0_{K_2}$ и $f(-a) = \breve{-} f(a)$ для любого $a \in K_1$.

4. Если $f: K_1 \to K_2$ – гомоморфизм колец, то $f(1_{K_1}) = 1_{\operatorname{Im} f}$, где 1_{K_1} – единица K_1 и $1_{\operatorname{Im} f}$ – единица $\operatorname{Im} f$, и $f(a^{-1}) = f(a)^{-1}$ в $\operatorname{Im} f$ для любого $a \in K_1^*$.

5. Если $f: K_1 \to K_2$ – гомоморфизм колец, то $\operatorname{Ker} f$ – двусторонний идеал K_1.

6. Гомоморфизм колец $f: K_1 \to K_2$ является мономорфизмом тогда и только тогда, когда $\operatorname{Ker} f = \{0_{K_1}\}$.

Из свойств 5 и 6 гомоморфизмов колец следует, что любой гомоморфизм $f: K_1 \to K_2$, где K_1 – поле, является либо нулевым, либо инъективным (т. к. поля не имеют нетривиальных идеалов).

Теорема 4.3.3. *Пусть* $(K, +, \cdot)$ *– кольцо,* $I \lhd K$ *и* $(K/I, \oplus, \otimes)$ *– факторкольцо с индуцированными операциями. Тогда функция* $f: K \to K/I$, *где* $f(a) = \overline{a}$ *для всех* $a \in K$, *является эпиморфизмом и* $\operatorname{Ker} f = I$.

Определение 4.3.6. Гомоморфизм из теоремы 4.3.3 $f: K \to K/I$, где $I \lhd K$, называется *естественным* (или *каноническим*) гомоморфизмом.

Теорема 4.3.4 (основная теорема о гомоморфизмах колец). *Пусть* $\psi: K_1 \to K_2$ *– гомоморфизм колец. Тогда* $K_1/\operatorname{Ker} \psi \cong \operatorname{Im} \psi$.

Поскольку $K/\{0\} = K$ для произвольного кольца $(K, +, \cdot)$, то из свойства 6 гомоморфизмов колец и теоремы 4.3.4 следует, что любой инъективный эндоморфизм кольца является автоморфизмом. В частности, любой ненулевой эндоморфизм поля является его автоморфизмом.

Теорема 4.3.5. *Пусть* $f: K \to K'$ *– эпиморфизм колец,* $\operatorname{Ker} f = I$. *Тогда существует взаимно однозначное и сохраняющее включения соответствие между множеством всех идеалов* U' *кольца* K' *и множеством всех идеалов* U *кольца* K, *содержащих* I, *такое, что* $f(U) = U'$ *и* $f^{-1}(U') = U$.

Пусть $(P, +, \cdot)$ – произвольное поле и $g(x)$ – неприводимый над P многочлен степени n из $P[x]$. Тогда по следствию 2 из теоремы 4.3.2 факторкольцо $(P[x]/(g(x)), \oplus, \otimes)$ является полем. Несложно проверить, что функция $f: P \to P[x]/(g(x))$, где $f(\alpha) = \overline{\alpha}$ для всех $\alpha \in P$, – мономорфизм данных полей. Получаем, что $(P, +, \cdot) \cong (\overline{P}, \oplus, \otimes)$, где $\overline{P} = \{\overline{\alpha} \mid \alpha \in P\}$, т. к. $\operatorname{Im} f = \overline{P}$. Значит, $(P, +, \cdot)$ с точностью до изоморфизма отождествляется с подполем $(\overline{P}, \oplus, \otimes)$ поля $(P[x]/(g(x)), \oplus, \otimes)$. Очевидно, что $P[x]/(g(x)) \cong P[x]/(h(x))$, если $g(x)$ и $h(x)$ – два неприводимых многочлена одной степени n.

В случае когда $P = \boldsymbol{F}_q$, поле $\big(\boldsymbol{F}_q[x]/\big(g(x)\big), \oplus, \otimes\big)$ является конечным, состоящим из q^n элементов согласно лемме 4.3.1. Так, с использованием простейших полей $\boldsymbol{F}_p$, например $(\mathbf{Z}/p\mathbf{Z}, +, \cdot)$, где p – простое число, и неприводимых над $\boldsymbol{F}_p$ многочленов можно построить конечные поля любых заданных порядков p^n, где $n \in \mathbf{N}$ (как отмечалось в §4.2).

Теорема 4.3.6 (теорема существования корня). *Для всякого неприводимого полинома $g(x) \in P[x]$ существует расширение поля $(P, +, \cdot)$, содержащее корень этого полинома и изоморфное полю* $\big(P[x]/\big(g(x)\big), \oplus, \otimes\big)$.

Определение 4.3.7. Ассоциативное и коммутативное кольцо $(K, +, \cdot)$ с единицей $e \neq 0$, без делителей нуля имеет *нулевую характеристику*, если $ne \neq 0$ для каждого $n \in \mathbf{N}$. Если для кольца $(K, +, \cdot)$ существует такое $p \in \mathbf{N}$, что $pe = 0$, причем p – наименьшее натуральное число с таким свойством, то говорят, что *характеристика кольца равна p*. Характеристику кольца K будем обозначать $\operatorname{char} K$ (англ. *characteristic* – характеристика).

Теорема 4.3.7. *Если характеристика кольца отлична от* 0, *то она является простым числом*.

Пусть p – произвольное простое число. Тогда $\boldsymbol{F}_p \cong \mathbf{Z}/p\mathbf{Z}$, и $\operatorname{char} \boldsymbol{F}_p = \operatorname{char} \mathbf{Z}/p\mathbf{Z} = p$. Любое конечное поле $\boldsymbol{F}_q$, где $q = p^m$, $m \in \mathbf{N}$, также имеет характеристику p, поскольку оно содержит $\boldsymbol{F}_p$ в качестве подполя и e – единица $\boldsymbol{F}_p$ и $\boldsymbol{F}_q$.

Кольцо $\mathbf{Z}$, а также поля $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$ имеют, очевидно, нулевую характеристику.

Для произвольного поля P кольцо полиномов $P[x]$ имеет ту же характеристику, что и P. Действительно, $P < P[x]$ и e – единица P и $P[x]$. В частности, $\operatorname{char} \boldsymbol{F}_q[x] = p$ при $q = p^m$ и любом $m \in \mathbf{N}$.

Пусть $(P, +, \cdot)$ – поле и f – вложение P в факторкольцо $\big(P[x]/\big(g(x)\big), \oplus, \otimes\big)$ для некоторого полинома $g(x) \in P[x]$ при $\deg g \geq 1$, где $f(\alpha) = \overline{\alpha}$ для любого $\alpha \in P$. Тогда $P[x]/\big(g(x)\big)$ – кольцо той же характеристики, что и P, поскольку $f(e) = \overline{e}$ и по свойству 6 гомоморфизмов колец $\overline{ne} = nf(e) = f(ne) = \overline{0} \Leftrightarrow ne = 0$ при $n \in \mathbf{N}$.

Пусть $\operatorname{char} K = p > 0$. Тогда для любого $z \in \mathbf{Z}$ согласно теореме 1.1.1 имеем $z = pu + r$, где $u, r \in \mathbf{Z}$, $0 \leq r < p$, и $za = ra$ для каждого $a \in K$, поскольку $(pu)a = p(ua) = (pe)(ua) = 0$.

Примеры

1. Построить факторкольцо $\big(P[x]/\big(g(x)\big), \oplus, \otimes\big)$, задав индуцированные операции сложения и умножения в виде таблиц Кэли. Установить, является ли данное факторкольцо полем, найти его характеристику:

а) $P = \boldsymbol{F}_2$, $g(x) = x^3 + x^2 + 1$.

Многочлен $g(x)$ неприводим над $\boldsymbol{F}_2$ (см. §4.2, пример 2, б), значит, по следствию 2 из теоремы 4.3.2 $\big(\boldsymbol{F}_2[x]/\big(g(x)\big), \oplus, \otimes\big)$ – поле. Так как $\deg g = 3$, то $\boldsymbol{F}_2[x]/\big(g(x)\big) = \big\{ \overline{r(x)} \;\big|\; r(x) \in \boldsymbol{F}_2[x], \text{ где } r(x) = 0 \vee \deg r < 3 \big\} = \boldsymbol{F}_8$ согласно лемме 4.3.1. Характеристика $\operatorname{char} \boldsymbol{F}_8 = \operatorname{char} \boldsymbol{F}_2 = 2$.

Сложение в данном поле задается таблицей Кэли, представленной на рис. 4.3.1.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

Рис. 4.3.1

Умножение в данном поле задается таблицей Кэли, представленной на рис. 4.3.2.

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\bar{1}$	$\bar{x}$	$\overline{x^2+x+1}$	$\overline{x^2}$
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+x}$
$\overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\bar{1}$
$\overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+x+1}$	$\bar{x}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+1}$
$\overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x^2+1}$	$\bar{x}$

Рис. 4.3.2

б) $P = \boldsymbol{F}_3$, $g(x) = x^2 + x + 1$.

Так как $g(1) = 0$ и $g(x) = (x+2)^2$, то многочлен $g(x)$ приводи́м над $\boldsymbol{F}_3$, значит, по следствию 2 из теоремы 4.3.2 $\left(\boldsymbol{F}_3[x]/(g(x)), \oplus, \otimes\right)$ не является полем. Поскольку $\deg g = 2$, то $\boldsymbol{F}_3[x]/(g(x)) = \left\{ \overline{r(x)} \,\middle|\, r(x) \in \boldsymbol{F}_3[x], \text{ где } r(x) = 0 \vee \deg r < 2 \right\} = R$ имеет порядок $3^2 = 9$ согласно лемме 4.3.1. Характеристика $\operatorname{char} R = \operatorname{char} \boldsymbol{F}_3 = 3$.

Сложение в данном факторкольце задается таблицей Кэли, приведенной на рис. 4.3.3. Умножение в данном факторкольце задается таблицей Кэли, представленной на рис. 4.3.4. Все ненулевые классы вычетов, кроме $\overline{x+2}$ и $\overline{2x+1}$, обратимы относительно умножения в факторкольце R. Классы вычетов $\overline{x+2}$ и $\overline{2x+1}$ – делители нуля в R.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\overline{x+2}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+2}$	$\bar{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{x+2}$	$\bar{x}$	$\overline{x+1}$

Рис. 4.3.3

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\bar{x}$	$\overline{x+2}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{2x}$	$\overline{2x+2}$	$\bar{2}$	$\overline{x+2}$	$\overline{x+1}$	$\overline{2x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{2x+2}$	$\bar{2}$	$\bar{x}$	$\overline{2x+1}$	$\bar{1}$	$\overline{x+2}$	$\overline{2x}$
$\overline{x+2}$	$\bar{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\bar{0}$	$\overline{2x+1}$	$\bar{0}$	$\overline{x+2}$
$\overline{2x}$	$\bar{0}$	$\overline{2x}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{x+2}$	$\bar{2}$
$\overline{2x+1}$	$\bar{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{x+2}$	$\bar{0}$	$\overline{x+2}$	$\bar{0}$	$\overline{2x+1}$
$\overline{2x+2}$	$\bar{0}$	$\overline{2x+2}$	$\overline{x+1}$	$\bar{1}$	$\overline{2x}$	$\overline{x+2}$	$\bar{2}$	$\overline{2x+1}$	$\bar{x}$

Рис. 4.3.4

2. Доказать, что $\mathbf{R}[x]/(x^2+1) \cong (\mathbf{C}, +, \cdot)$.

Построим функцию $f\colon \mathbf{R}[x] \to \mathbf{C}$, где $f(g(x)) = g(i)$ для всех $g(x) \in \mathbf{R}[x]$, $i^2 = -1$. Тогда для любых $g(x)$, $h(x) \in \mathbf{R}[x]$ выполняется:

1) $f(g(x) + h(x)) = f(F(x)) = F(i) = g(i) + h(i) = f(g(x)) + f(h(x))$;

2) $f(g(x)h(x)) = f(G(x)) = G(i) = g(i)h(i) = f(g(x))f(h(x))$.

Таким образом, f – гомоморфизм колец. $\operatorname{Im} f = \mathbf{C}$, т. к. для всякого $a + bi \in \mathbf{C}$ найдется многочлен $bx + a \in \mathbf{R}[x]$, такой, что $f(bx + a) = a + bi$, $\forall\, a, b \in \mathbf{R}$. Поэтому f – эпиморфизм колец.

$\operatorname{Ker} f = \{ u(x) \in \mathbf{R}[x] \mid u(i) = 0 \}$. Так как $u(x) \in \mathbf{R}[x]$, то $u(i) = 0 \Leftrightarrow \overline{u(i)} = 0 \Leftrightarrow$ $\Leftrightarrow u(\bar{i}) = u(-i) = 0$ (в данном случае черта сверху обозначает комплексное сопряжение). По следствию 1 из теоремы 4.2.10 в кольце $\mathbf{C}[x]$ имеем: $u(i) = 0 \Leftrightarrow$ $\Leftrightarrow x - i \mid u(x)$, $u(-i) = 0 \Leftrightarrow x + i \mid u(x)$. Поскольку $(x-i)(x+i) = x^2 + 1$, то $u(i) = 0 \Leftrightarrow$ $\Leftrightarrow x^2 + 1 \mid u(x)$ в кольце $\mathbf{R}[x]$. Значит, $\operatorname{Ker} f = (x^2+1)$ – идеал кольца $\mathbf{R}[x]$.

Итак, по основной теореме о гомоморфизмах колец $\mathbf{R}[x]/(x^2+1) \cong (\mathbf{C}, +, \cdot)$.

3. Найти все идеалы кольца $\mathbf{Z}/n\mathbf{Z}$, расположить их в порядке включения, указать все максимальные идеалы в случае их существования. Решить задачу для заданных ниже значений n.

Рассмотрим канонический гомоморфизм $f: \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$, где $f(z) = \bar{z}$, $\forall z \in \mathbf{Z}$, и $\operatorname{Ker} f = n\mathbf{Z} = (n)$. Так как f – эпиморфизм, то по теореме 4.3.5 существует взаимно однозначное и сохраняющее включения соответствие между множеством всех идеалов кольца $\mathbf{Z}/n\mathbf{Z}$ и множеством всех идеалов кольца $\mathbf{Z}$, содержащих (n), такое, что $f((m)) = (\overline{m})$, $f^{-1}((\overline{m})) = (m)$, где $1 \le m \le n$, $m \mid n$. Поскольку $(\mathbf{Z}, +, \cdot)$ – кольцо главных идеалов, то $(\mathbf{Z}/n\mathbf{Z}, \oplus, \otimes)$ – также кольцо главных идеалов, $(\overline{m}) \subseteq (\overline{l}) \Leftrightarrow (m) \subseteq (l) \Leftrightarrow l \mid m$. Если p – простое число, то по следствию 1 из теоремы 4.3.2 $(\mathbf{Z}/p\mathbf{Z}, \oplus, \otimes)$ – поле, не имеющее собственных, в том числе максимальных, идеалов, содержащее только тривиальные идеалы $\{\bar{0}\}$ и $\mathbf{Z}/p\mathbf{Z}$. Если n – составное число с каноническим разложением $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, то $(\overline{p_1}), \dots, (\overline{p_t})$ – все максимальные идеалы кольца $(\mathbf{Z}/n\mathbf{Z}, \oplus, \otimes)$.

Все идеалы кольца $(\mathbf{Z}/n\mathbf{Z}, \oplus, \otimes)$ являются подгруппами циклической группы $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ и имеют вид $I_k = (\overline{m}) = <\overline{m}>$, где $|I_k| = \operatorname{ord}(\overline{m}) = k$. Согласно определению 3.1.10 порядка элемента группы $\operatorname{ord}(\overline{m}) = n/(m, n)$, откуда $(m, n) = n/k$. Поэтому кольцо $\mathbf{Z}/n\mathbf{Z}$ содержит единственный идеал $I_k = \{\overline{n/k}, \dots, k\overline{n/k} = \bar{0}\} = (\overline{n/k})$ фиксированного порядка k, где $k \mid n$. При $k > 1$ количество образующих элементов в I_k равно $\varphi(k)$, где φ – функция Эйлера (см. пример 5 из §3.1).

а) $n = 29$.

В данном случае k может принимать значения 1, 29. Тогда получаем следующие 2 идеала кольца $\mathbf{Z}/29\mathbf{Z}$:

$k = 1 = |I_1| \Rightarrow I_1 = \{\bar{0}\} = (\bar{0})$;

$k = 29 = |I_{29}| \Rightarrow I_{29} = \mathbf{Z}/29\mathbf{Z} = \{\bar{1}, \bar{2}, \dots, \overline{28}, \bar{0}\} = (\bar{1}) = (\bar{2}) = \dots = (\overline{28})$, поскольку $(1, 29) = (2, 29) = \dots = (28, 29) = 29/29 = 1$.

29 – простое число, значит, $(\mathbf{Z}/29\mathbf{Z}, \oplus, \otimes)$ – поле, содержащее только тривиальные идеалы. Максимальных идеалов в $\mathbf{Z}/29\mathbf{Z}$ нет. Имеем следующее включение идеалов $\mathbf{Z}/29\mathbf{Z}$: $(\bar{0}) \subset (\bar{1})$.

б) $n = 8$.

В данном случае k может принимать значения 1, 2, 4, 8. Тогда получаем следующие 4 идеала кольца $\mathbf{Z}/8\mathbf{Z}$:

$k = 1 = |I_1| \Rightarrow I_1 = \{\bar{0}\} = (\bar{0})$;

$k = 2 = |I_2| \Rightarrow I_2 = \{\bar{4}, \bar{0}\} = (\bar{4})$, т. к. $(4, 8) = 8/2 = 4$;

$k = 4 = |I_4| \Rightarrow I_4 = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\} = (\bar{2}) = (\bar{6})$, т. к. $(2, 8) = (6, 8) = 8/4 = 2$;

$k = 8 = |I_8| \Rightarrow I_8 = \mathbf{Z}/8\mathbf{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{0}\} = (\bar{1}) = (\bar{3}) = (\bar{5}) = (\bar{7})$, поскольку (1, 8) = (3, 8) = (5, 8) = (7, 8) = 8/8 = 1.

$8 = 2^3$, значит, $(\bar{2})$ – максимальный идеал кольца ($\mathbf{Z}/8\mathbf{Z}$, $\oplus$, $\otimes$).

Имеем следующие включения идеалов $\mathbf{Z}/8\mathbf{Z}$: $(\bar{0}) \subset (\bar{4}) \subset (\bar{2}) \subset (\bar{1})$.

в) $n = 24$.

В данном случае k может принимать значения 1, 2, 3, 4, 6, 8, 12, 24. Тогда получаем следующие 8 идеалов кольца $\mathbf{Z}/24\mathbf{Z}$:

$k = 1 = |I_1| \Rightarrow I_1 = \{\bar{0}\} = (\bar{0})$;

$k = 2 = |I_2| \Rightarrow I_2 = \{\overline{12}, \bar{0}\} = (\overline{12})$, т. к. (12, 24) = 24/2 = 12;

$k = 3 = |I_3| \Rightarrow I_3 = \{\bar{8}, \overline{16}, \bar{0}\} = (\bar{8}) = (\overline{16})$, т. к. (8, 24) = (16, 24) = 24/3 = 8;

$k = 4 = |I_4| \Rightarrow I_4 = \{\bar{6}, \overline{12}, \overline{18}, \bar{0}\} = (\bar{6}) = (\overline{18})$, т. к. (6, 24) = (18, 24) = 24/4 = 6;

$k = 8 = |I_8| \Rightarrow I_8 = \{\bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \bar{0}\} = (\bar{3}) = (\bar{9}) = (\overline{15}) = (\overline{21})$, т. к. (3, 24) = = (9, 24) = (15, 24) = (21, 24) = 24/8 = 3;

$k = 12 = |I_{12}| \Rightarrow I_{12} = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \bar{0}\} = (\bar{2}) = (\overline{10}) = (\overline{14}) = (\overline{22})$, т. к. (2, 24) = (10, 24) = (14, 24) = (22, 24) = 24/12 = 2;

$k = 24 = |I_{24}| \Rightarrow I_{24} = \mathbf{Z}/24\mathbf{Z} = \{\bar{1}, \bar{2}, \ldots, \overline{23}, \bar{0}\} = (\bar{1}) = (\bar{5}) = (\bar{7}) = (\overline{11}) = (\overline{13}) = (\overline{17}) = (\overline{19}) = (\overline{23})$, т. к. (1, 24) = (5, 24) = (7, 24) = (11, 24) = (13, 24) = (17, 24) = = (19, 24) = (23, 24) = 24/24 = 1.

$24 = 2^3 \cdot 3$, значит, $(\bar{2})$ и $(\bar{3})$ – максимальные идеалы кольца ($\mathbf{Z}/24\mathbf{Z}$, $\oplus$, $\otimes$).

Имеем следующую схему включений идеалов $\mathbf{Z}/24\mathbf{Z}$:

$$\begin{array}{ccccccc} (\bar{0}) & \subset & (\overline{12}) & \subset & (\bar{6}) & \subset & (\bar{3}) \\ \cap & & \cap & & \cap & & \cap \\ (\bar{8}) & \subset & (\bar{4}) & \subset & (\bar{2}) & \subset & (\bar{1}) \end{array}$$

Задачи

1. Построить факторкольцо $(P[x]/(g(x)), \oplus, \otimes)$, задав индуцированные операции сложения и умножения в виде таблиц Кэли. Установить, является ли данное факторкольцо полем, найти его характеристику:

а) $P = \boldsymbol{F}_2$, $g(x) = x^2 + 1$; **б)** $P = \boldsymbol{F}_3$, $g(x) = x^2 + 2x + 2$.

2. Доказать, что $\mathbf{Z}[x]/(n) \cong \mathbf{Z}/n\mathbf{Z}[x]$, $\forall\, n \in \mathbf{N}$. Указание: показать, что функция $f\colon \mathbf{Z}[x] \to \mathbf{Z}/n\mathbf{Z}[x]$, где $f\left(\sum\limits_{i=0}^{k} a_i x^i\right) = \sum\limits_{i=0}^{k} \overline{a_i} x^i$, $\forall\, a_i \in \mathbf{Z}$, $0 \le i \le k$, $\forall\, k \in \mathbf{Z}_{\ge 0}$, является гомоморфизмом; найти $\operatorname{Im} f$, $\operatorname{Ker} f$ и применить основную теорему о гомоморфизмах колец (теорема 4.3.4).

Ответы

1. а) R – не поле, $|R| = 4$, $\overline{x+1}$ – делитель нуля, $\operatorname{char} R = 2$; **б)** поле $\boldsymbol{F}_9$, $\operatorname{char} \boldsymbol{F}_9 = 3$.

Перечень обозначений

N – множество натуральных чисел

Z – множество целых чисел

Q – множество рациональных чисел

R – множество вещественных чисел

C – множество комплексных чисел

$A \subset B$ – множество A является собственным подмножеством множества B

$A \subseteq B$ – множество A является подмножеством множества B

$a \in A$ – элемент a принадлежит множеству A

$A_{>a}$ – подмножество числового множества $A \subseteq \mathbf{R}$, состоящее из всех чисел, больших a

$A_{<a}$ – подмножество числового множества $A \subseteq \mathbf{R}$, состоящее из всех чисел, меньших a

$A_{\geq a}$ – подмножество числового множества $A \subseteq \mathbf{R}$, состоящее из всех чисел, больших или равных a

$A_{\leq a}$ – подмножество числового множества $A \subseteq \mathbf{R}$, состоящее из всех чисел, меньших или равных a

$a_1, a_2, \ldots, a_n \in A$ – элементы $a_1, a_2, \ldots, a_n$ принадлежат множеству A, где $n \geq 2$

$|a|$ – модуль числа a

$a \vdots b$ – целое число a делится на целое число $b \neq 0$

$b \mid a$ – целое число $b \neq 0$ делит целое число a

$a \not\vdots b$ – целое число a не делится на целое число $b \neq 0$

$b \nmid a$ – целое число $b \neq 0$ не делит целое число a

$\forall$ – квантор общности, обозначающий слова «любой», «каждый»

$\&$ – символ конъюнкции (одновременного выполнения условий), обозначающий логическое «и»

$\Rightarrow$ – символ следствия (импликации)

$\Leftrightarrow$ – символ эквивалентности (равносильности)

ОД – общий делитель

НОД – наибольший общий делитель

НОД$(a_1, a_2, \ldots, a_n)$ или $(a_1, a_2, \ldots, a_n)$ – НОД целых чисел $a_1, a_2, \ldots, a_n$, где $n \geq 2$

$i = \overline{m,n}$ – i принимает все целые значения от m до n, где $m < n$

ОК – общее кратное

НОК – наименьшее общее кратное

НОК$(a_1, a_2, \ldots, a_n)$ или $[a_1, a_2, \ldots, a_n]$ – НОК целых чисел $a_1, a_2, \ldots, a_n$, где $n \geq 2$

$\operatorname{sgn}(a)$ – сигнум вещественного числа a

$A \cup B$ – объединение множеств A и B

$[a; b]$ – отрезок (подмножество **R**, состоящее из всех чисел r, таких, что $a \leq r \leq b$)

$[a]$ – целая часть вещественного числа a

$\exists$ – квантор существования, обозначающий слова «существует», «найдется»

$n!$ – факториал целого неотрицательного числа n

$|$ – обозначение слов «такой, что», «такие, что» при описательном задании множеств

$a \equiv b \pmod{m}$ – целые числа a и b сравнимы по модулю $m \in \mathbf{N}$

$\bar{i}$ – класс вычетов по натуральному модулю с представителем $i \in \mathbf{Z}$

$A = B$ – множества A и B равны

$\mathbf{Z}/m\mathbf{Z}$ – множество классов вычетов по натуральному модулю m

$A \neq B$ – множества A и B не равны

φ – функция Эйлера (тотиент-функция)

C_n^k – число сочетаний из n элементов по k, биномиальный коэффициент

$q\colon X \to Y$ – существование соответствия q между множествами X и Y

$A \times B$ – прямое (декартово) произведение множеств A и B

$q = (X, Y, Q)$ – соответствие q с областью отправления X, областью прибытия Y и графиком Q

$D(q)$ – область определения соответствия q

$E(q)$ – область значений соответствия q

$q(x)$ – образ элемента x при соответствии q

$q^{-1}(y)$ – прообраз элемента y при соответствии q

$q(A)$ – образ множества A при соответствии q

$q^{-1}(B)$ – прообраз множества B при соответствии q

$p = q$ – отображения p и q равны

$q\colon x \mapsto y$ или $q(x) = y$ – функциональное соответствие q сопоставляет элементу x единственный элемент y

e_X – тождественная функция на множестве X

$\mathbf{R}^2$ – декартова вещественная плоскость

q^{-1} – соответствие, обратное соответствию q

$A \cap B$ – пересечение множеств A и B

$\varnothing$ – пустое множество

$g \circ f$ или gf – композиция функций f и g

f_A – сужение функции f на множество A

$A \backslash B$ – разность множеств A и B

$p \neq q$ – отображения p и q не равны

$[a; b)$ – полуинтервал (подмножество $\mathbf{R}$, состоящее из всех чисел r, таких, что $a \le r < b$)

$(a; b)$ – интервал (подмножество $\mathbf{R}$, состоящее из всех чисел r, таких, что $a < r < b$)

$(a; b]$ – полуинтервал (подмножество $\mathbf{R}$, состоящее из всех чисел r, таких, что $a < r \le b$)

$V_n(K)$ – множество n-мерных векторов с компонентами из множества K

$M_n(K)$ – множество квадратных матриц порядка n с элементами из множества K

$\boldsymbol{c}$ – обозначение вектора

A^{-1} – матрица, обратная матрице A

$\det(A)$ – определитель матрицы A

$A \leftrightarrow B$ – множества A и B равномощны

$|A|$ – мощность множества A

A^n – n-я декартова степень множества A

$P(A)$ – множество-степень (булеан) множества A

$A \triangle B$ – симметрическая разность множеств A и B

$GL_n(K)$ – полная линейная группа квадратных матриц порядка n с элементами из множества K

$H \le G$ или $H < G$ (если $H \subset G$) – H является подгруппой группы G

$SL_n(K)$ – специальная линейная группа квадратных матриц порядка n с элементами из множества K

$< a >$ – циклическая группа (подгруппа), порожденная элементом a

$\mathrm{ord}(a)$ – порядок элемента a в группе

$a \notin A$ – элемент a не принадлежит множеству A

aH – левый смежный класс с представителем a группы по подгруппе H

Ha – правый смежный класс с представителем a группы по подгруппе H

$[G : H]$ – индекс подгруппы H в группе G

$H \lhd G$ – H является нормальной подгруппой группы G

G/H – фактормножество (факторгруппа) группы G по нормальной подгруппе H

$\{a\}$ – дробная часть вещественного числа a

A^* – множество всех обратимых элементов относительно некоторой бинарной алгебраической операции, заданной на множестве A

E_n – единичная квадратная матрица порядка n

S_n – симметрическая группа степени n

$S(\Omega)$ – симметрическая группа множества Ω

$(i_1\, i_2 \ldots i_k)$ или $\left(i\ f(i) \ldots f^{k-1}(i)\right)$ – цикл длины k в группе S_n

A_n – знакопеременная группа степени n

$\mathrm{Im}\, f$ – образ группового или кольцевого гомоморфизма f

$\mathrm{Ker}\, f$ – ядро группового или кольцевого гомоморфизма f

$(G_1, \bullet) \cong (G_2, *)$ или $G_1 \cong G_2$ – группы $(G_1, \bullet)$ и $(G_2, *)$ изоморфны

K^* – мультипликативная группа ассоциативного кольца K с единицей

$L \le K$ или $L < K$ (если $L \subset K$) – L является подкольцом кольца K

$J \lhd K$ – J является двусторонним идеалом кольца K

(a) – главный идеал коммутативного кольца, порожденный элементом a

$\vee$ – символ дизъюнкции (выполнения хотя бы одного из условий), обозначающий логическое «или»

$K[x]$ – множество полиномов от одной переменной x с коэффициентами из кольца K

$\deg f$ – степень многочлена $f(x)$

$g(x) \mid f(x)$ – многочлен $g(x) \neq 0$ делит многочлен $f(x)$

$f(x) \vdots g(x)$ – многочлен $f(x)$ делится на многочлен $g(x) \neq 0$

$g(x) \nmid f(x)$ – многочлен $g(x) \neq 0$ не делит многочлен $f(x)$

$f(x) \not\vdots g(x)$ – многочлен $f(x)$ не делится на многочлен $g(x) \neq 0$

НОД$(f_1(x), f_2(x), \ldots, f_s(x))$ или $(f_1(x), f_2(x), \ldots, f_s(x))$ – НОД многочленов $f_1(x)$, $f_2(x)$,…, $f_s(x)$, где $s \ge 2$

$\tilde{f}(x)$ – многочлен, полученный нормированием многочлена $f(x)$

НОК$(f_1(x), f_2(x), \ldots, f_s(x))$ или $[f_1(x), f_2(x), \ldots, f_s(x)]$ – НОК многочленов $f_1(x)$, $f_2(x)$,…, $f_s(x)$, где $s \ge 2$

$\boldsymbol{F_q}$ – конечное поле из q элементов

$\bar{a}$ – класс вычетов с представителем a кольца по модулю двустороннего идеала

K/I – фактормножество (факторкольцо) кольца K по двустороннему идеалу I

$(K_1, +, \cdot) \cong (K_2, \dot{+}, \bullet)$ или $K_1 \cong K_2$ – кольца $(K_1, +, \cdot)$ и $(K_2, \dot{+}, \bullet)$ изоморфны

$\mathrm{char}\, K$ – характеристика кольца K

Список использованных источников

Основной

1. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. К. Барти ; пер. с англ. – 2-е изд., стер. – СПб. : Лань, 2005. – 400 с.

2. Введение в криптографию / В. В. Ященко [и др.] ; под общ. ред. В. В. Ященко. – 3-е изд., перераб. – М. : МЦНМО, 2003. – 400 с.

3. Винберг, Э. Б. Алгебра многочленов : учеб. пособие / Э. Б. Винберг. – М. : Просвещение, 1980. – 176 с.

4. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – 9-е изд., перераб. – М. : Наука, 1981. – 176 с.

5. Ерусалимский, Я. М. Дискретная математика: теория, задачи, приложения / Я. М. Ерусалимский. – М. : Вузовская книга, 2000. – 200 с.

6. Каргополов, М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – М. : Наука, 1972. – 240 с.

7. Карпов, В. Г. Математическая логика и дискретная математика : учеб. пособие / В. Г. Карпов, В. А. Мощенский. – Минск : Выш. шк., 1977. – 254 с.

8. Кострикин, А. И. Введение в алгебру. В 3 ч. Ч. 1 : Основы алгебры / А. И. Кострикин. – 3-е изд. – М. : Физматлит, 2004. – 272 с.

9. Кострикин, А. И. Сборник задач по алгебре / А. И. Кострикин. – М. : Физматлит, 2001. – 464 с.

10. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо ; пер. с англ. – М. : Постмаркет, 2001. – 328 с.

11. Кузнецов, О. П. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. – М. : Энергия, 1980. – 344 с.

12. Курош, А. Г. Курс высшей алгебры : учебник для вузов / А. Г. Курош. – 17-е изд., стер. – СПб. : Лань, 2008. – 432 с.

13. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие / В. А. Липницкий. – 2-е изд., испр. – Минск : БГУИР, 2006. – 88 с.

14. Математические и компьютерные основы криптологии : учеб. пособие / Ю. С. Харин [и др.]. – Минск : Новое знание, 2003. – 382 с.

15. Милованов, М. В. Алгебра и аналитическая геометрия : учебник для вузов. В 2 ч. Ч. 1 / М. В. Милованов, Р. И. Тышкевич, А. С. Феденко. – Минск : Амалфея, 2001. – 400 с.

16. Проскуряков, И. В. Сборник задач по линейной алгебре / И. В. Проскуряков. – 12-е изд., стер. – СПб. : Лань, 2008. – 480 с.

17. Сборник задач по алгебре и аналитической геометрии : учеб. пособие / А. А. Бурдун [и др.] ; под ред. А. С. Феденко. – 2-е изд. – Минск : Універсітэцкае, 1999. – 302 с.

18. Стройникова, Е. Д. Основы прикладной алгебры : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2010. – 120 с.

19. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел / Л. Б. Шнеперман. – 3-е изд., стер. – СПб. : Лань, 2008. – 224 с.

Дополнительный

20. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен ; пер. с англ. – М. : Мир, 1987. – 416 с.

21. Аршинов, Н. Н. Коды и математика / Н. Н. Аршинов, Л. Е. Садовский. – М. : Наука, 1983. – 124 с.

22. Баричев, С. Г. Основы современной криптографии : учеб. пособие для вузов / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – 2-е изд., испр. и доп. – М. : Горячая линия – Телеком, 2002. – 175 с.

23. Беняш-Кривец, В. В. Лекции и семинары по алгебре: группы, кольца, поля : пособие / В. В. Беняш-Кривец, Г. Е. Пунинский. – Минск : БГУ, 2015. – 152 с.

24. Беняш-Кривец, В. В. Лекции и семинары по алгебре: основные понятия алгебры и теории чисел : пособие / В. В. Беняш-Кривец, Г. Е. Пунинский. – Минск : БГУ, 2015. – 114 с.

25. Бухштаб, А. А. Теория чисел / А. А. Бухштаб. – 3-е изд., стер. – М. : URSS, 2008. – 384 с.

26. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 326 с.

27. Коршунов, Ю. М. Математические основы кибернетики : учеб. пособие для вузов / Ю. М. Коршунов. – М. : Энергоатомиздат, 1987. – 496 с.

28. Ленг, С. Алгебра / С. Ленг ; пер. с англ. – М. : Мир, 1968. – 564 с.

29. Лидл, Р. Конечные поля. В 2 т. / Р. Лидл, Г. Нидеррайтер ; пер. с англ. – М. : Мир, 1988. – 820 с.

30. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте ; пер. с англ. – М. : Мир, 1999. – 720 с.

31. Прасолов, В. В. Многочлены / В. В. Прасолов. – 3-е изд., испр. – М. : МЦНМО, 2003. – 336 с.

32. Сигорский, В. П. Математический аппарат инженера / В. П. Сигорский. – 2-е изд., стер. – Киев : Техника, 1977. – 768 с.

33. Фаддеев, Д. К. Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. – 11-е изд., перераб. и доп. – М. : Наука, 1977. – 288 с.

Св. план 2016, поз. 43

Учебное издание

Стройникова Елена Дмитриевна

АЛГЕБРА В ПРИМЕРАХ И ЗАДАЧАХ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. С. Юрец*
Корректор *Е. И. Герман*
Компьютерная правка, оригинал-макет *Е. Д. Стройникова*

Подписано в печать 22.02.2018. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,05. Уч.-изд. л. 6,2. Тираж 100 экз. Заказ 412.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6