Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина
Институт радиоэлектроники и информационных технологий

Б. М. ВЕРЕТЕННИКОВ
В. И. БЕЛОУСОВА

ДИСКРЕТНАЯ МАТЕМАТИКА
ЧАСТЬ I

Учебное пособие

Министерство образования и науки Российской Федерации
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

Б. М. Веретенников, В. И. Белоусова

ДИСКРЕТНАЯ МАТЕМАТИКА

Часть I

Рекомендовано методическим советом УрФУ
*в качестве **учебного пособия** для студентов,*
обучающихся по всем направлениям подготовки
Института радиоэлектроники и информационных технологий

Екатеринбург
Издательство Уральского университета
2014

УДК 519(075.8)
ББК 22.176А73
В31

Рецензенты:
кафедра Прикладной математики Уральского государственного экономического университета (завкафедрой, канд. физ.-мат. наук, доц. О. Б. Мельников);
канд. физ.-мат. наук, доц. И. Н. Белоусов (Институт математики и механики УрО РАН)

Научный редактор – канд. физ.-мат. наук, доц. Н. В. Чуксина

Веретенников, Б. М.
В31 Дискретная математика : учебное пособие / Б. М. Веретенников, В. И. Белоусова. – Екатеринбург : Изд-во Урал. ун-та, 2014. – Ч. I. – 132 с.

ISBN 978-5-7996-1199-6 (ч. 1)
978-5-7996-1195-8

Учебное пособие включает в себя базисные разделы дискретной математики: бинарные отношения, элементы общей алгебры и теорию чисел. В работе предлагаются упражнения для самостоятельного решения. Предназначено для студентов всех направлений подготовки Института радиоэлектроники и информационных технологий – РтФ.

Библиогр.: 10 назв. Рис. 21. Табл. 18.

УДК 519(075.8)
ББК 22.176А73

ISBN 978-5-7996-1199-6 (ч. 1)
978-5-7996-1195-8

Оглавление

Список обозначений

Множество – это совокупность, группа некоторых объектов, называемых элементами, объединенных каким-нибудь общим свойством. Множества обозначают большими латинскими буквами: $A, B, C, \dots, X, Y, \dots$.

$\emptyset$ – пустое множество, т. е. множество, не имеющее элементов;

$\mathbb{N}$ – множество всех натуральных чисел;

$\mathbb{Z}$ – множество всех целых чисел;

$\mathbb{Q}$ – множество всех рациональных чисел;

$\mathbb{R}$ – множество всех действительных чисел;

$\mathbb{C}$ – множество всех комплексных чисел;

$\forall$ – для всех, для любого;

$\exists$ – существует, найдется;

$\exists!$ – существует (найдется) единственный;

Знак $\Leftrightarrow$ заменяет выражение «если и только если»;

Знак $\Rightarrow$ заменяет выражение «влечет»;

$x \in X$ – элемент x принадлежит множеству X;

$x \notin X$ – элемент x не принадлежит множеству X;

$X \subseteq Y$ – X подмножество в Y $\{\forall x \in X: x \in Y\}$;

$X \nsubseteq Y$ – X не содержится в Y;

$X = Y$ – X равно Y, т. е. $X \subseteq Y$ и $Y \subseteq X$;

$X \subset Y$ – X строго содержится в Y, т. е. $X \subseteq Y$ и $X \neq Y$;

$X \cap Y$ – пересечение множеств X и Y, т. е. $\{x|\ x \in X$ и $x \in Y\}$;

$X \cup Y$ – объединение множеств X и Y, т. е. $\{x|\ x \in X$ или $x \in Y\}$;

$X \backslash Y$ – разность множеств X и Y, т. е. множество $\{x|\ x \in X$ и $x \notin Y\}$;

■ – конец доказательства.

Введение

Дискретная математика в наше время – это обширная наука, которая базируется на классических разделах математики – алгебре, теории чисел, математическом анализе и теории вероятностей. Особенно важны для глубокого понимания методов дискретной математики алгебра и теория чисел. Такие алгебраические структуры, как полугруппы, группы, кольца, поля, решетки, булевы алгебры используются во всех видах кодирования информации, в теории графов, теории автоматов, теории булевых функций, комбинаторике и математической логике.

Без основательного знания теории чисел также невозможно усвоить многие разделы дискретной математики и успешно применять методы дискретной математики на практике. Более того, даже весьма продвинутая и сложная наука – алгебраическая геометрия находит приложения в теории кодирования.

В данном пособии авторы излагают основные понятия и методы современной алгебры, а также классические результаты теории чисел, используемые в дискретной математике. Многие результаты даются с доказательствами, так как авторы считают, что глубокое понимание алгебры и теории чисел невозможно без умения доказывать теоремы. Кроме того, в тексте приводится достаточно много примеров вычислительного характера и задач для самостоятельного решения.

Основу данного пособия составили лекции, которые Б. М. Веретеников читал студентам разных специальностей на радиотехническом факультете в течение последних десяти лет. Лекционный материал существенно расширен за счет доказательств и большого числа дополнительных задач. Планируется продолжение, в котором будут рассмотрены конкретные области дискретной математики: теория алгебраического кодирования, алфавитное кодирование, теория автоматов, булевы функции, теория графов и комбинаторика.

Авторы надеются, что чтение пособия поможет читателю усвоить основные методы алгебры и теории чисел и использовать их в дальнейшем для изучения различных разделов дискретной математики.

Для понимания материала, изложенного в пособии, предварительной особой подготовки не требуется. Определенную математическую культуру можно развить, имея большое желание и достаточное усердие.

В заключение отметим, что авторы предполагают использование пособия студентами и преподавателями УрФУ различных факультетов и специальностей.

Глава I. Бинарные отношения

§ 1. Определение и способы задания бинарного отношения

Определение. Пусть A некоторое множество. Тогда множество упорядоченных пар (a_1, a_2), где $a_1, a_2 \in A$, называется *декартовым квадратом множества* A и обозначается $A \times A$ или A^2. Кратко $A \times A = \{(a_1, a_2) | a_1, a_2 \in A\}$.

Аналогично определяется любая натуральная степень множества.

Определение. Множество $A^k = \{(a_1, \dots, a_k) | \forall i = \overline{1,k}\ \ a_i \in A\}$ называется *k-й степенью множества* A.

Определение. Пусть A – конечное множество, состоящее из n элементов. Тогда число n называется *порядком множества* A и обозначается $|A|$.

Определение. *Бинарным отношением на множестве* A называется любое подмножество ρ декартова квадрата $A \times A$.

Отметим очевидные примеры бинарных отношений:

- $A \times A = \omega_A$ – универсальное отношение на A;
- $\emptyset$ – пустое бинарное отношение;
- $\Delta_A = \{(a, a), a \in A\}$ – диагональ $A \times A$.

Если A – конечное множество, то любое бинарное отношение на A можно задать списком упорядоченных пар, содержащихся в этом бинарном отношении. Например, на множестве

$A = \{1,\ 2,\ 3\}$ можно задать следующие бинарные отношения: $\rho_1 = \{(1,\ 2), (2,\ 2), (3,\ 1)\}$, $\rho_2 = \{(3,\ 2)\}$,…

Если ρ – бинарное отношение на A, то вместо $(a_1, a_2) \in \rho$ пишут $a_1 \rho a_2$(инфиксный способ).

Определение. Пусть $A = \{a_1, \dots, a_n\}$ и ρ – бинарное отношение на A. Тогда *матрицей отношения* ρ называется квадратная матрица размера $n \times n$, состоящая из нулей и единиц, такая, что в пересечении *i*-й строки и *j*-го столбца стоит 1 тогда и только тогда, когда $a_i \rho a_j\ \forall\ i, j = \overline{1, n}$.

Пример. На множестве $A = \{1,\ 2,\ 3,\ 4\}$ матрица отношения $\rho = \{(1,\ 4), (2,\ 4), (3,\ 2), (2,\ 2), (2,\ 3), (1,\ 1)\}$ имеет вид

$$M = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,1 \\ 0\,1\,0\,0 \\ 0\,0\,0\,0 \end{pmatrix}$$

Верно обратное – любая квадратная матрица *n*-го порядка, состоящая из 0 и 1, задает естественным образом бинарное отношение на любом множестве A порядка n.

Пример. На множестве $A = \{a_1,\ a_2,\ a_3,\ a_4\}$, матрица $M = \begin{pmatrix} 1\,1\,0\,0 \\ 0\,0\,0\,1 \\ 0\,1\,0\,0 \\ 1\,0\,1\,0 \end{pmatrix}$ задает бинарное отношение

$$\rho = \{(a_1,\ a_1), (a_1,\ a_2), (a_2,\ a_4), (a_3,\ a_2), (a_4,\ a_1), (a_4,\ a_3)\}.$$

Бинарное отношение можно задать также с помощью так называемого ориентированного графа (рис.1).

Определение. Пусть $A = \{a_1, \dots, a_n\}$ и ρ – бинарное отношение на A. Тогда *ориентированным графом* (*орграфом*) *отношения* ρ называется множество n точек на плоскости, обозначенных $a_1, \dots, a_n$, причем из a_i в a_j идет стрелка тогда и только тогда, когда $a_i \rho a_j, \forall\, i, j = \overline{1, n}$.

Пример. На множестве $A = \{1,\ 2,\ 3,\ 4,\ 5\}$ орграф отношения $\rho = \{(1,1), (1,4), (2,3), (3,3), (4,5), (5,2)\}$ представлен на рис. 1.

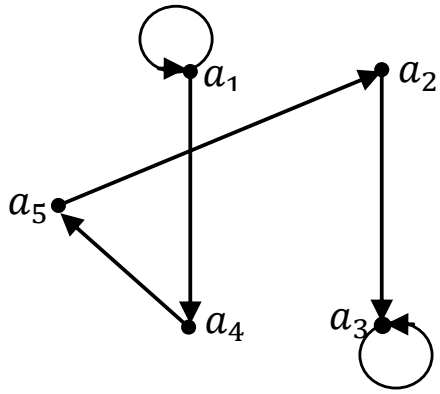

Рис.1

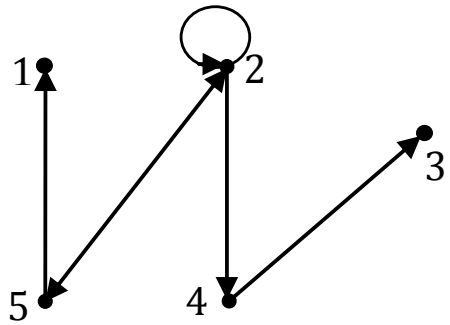

Рис.2

Верно обратное – по любому орграфу с *n* вершинами можно естественным образом составить бинарное отношение на любом множестве из n элементов.

Пример. Орграф, представленный на рис. 2, задает на множестве $A = \{1, 2, 3, 4, 5\}$ бинарное отношение $\rho = \{(2,2), (2,4), (2,5), (4,3), (5,1), (5,2)\}$.

Еще один способ задания – функциональный. Он полезен при нахождении произведений бинарных отношений, которые рассмотрим далее.

Определение. Пусть $A = \{a_1, \dots, a_n\}$ и ρ – бинарное отношение на A. Тогда *функциональной схемой отношения* ρ называется диаграмма, состоящая из двух одинаковых столбцов (рис. 3), причем стрелка из элемента a_i левого столбца идет в элемент a_jправого столбца тогда и только тогда, когда $a_i \rho a_j$.

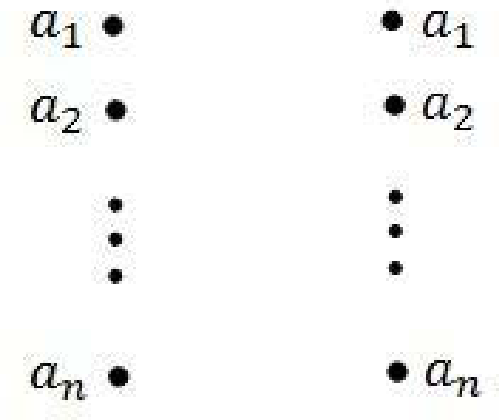

Рис. 3

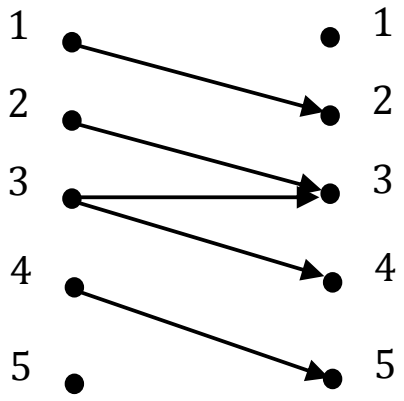

Рис.4

Пример. На множестве $A = \{1, 2, 3, 4, 5\}$ отношение $\rho = \{(1, 2), (2, 3), (3, 3), (3, 4), (4, 5)\}$ можно задать функциональной схемой, представленной на рис. 4.

Упражнения для самостоятельной подготовки

1. Постройте орграф и матрицу для каждого из приведенных ниже отношений на A.

а) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, a), (a, c), (d, e), (e, d)\}$;

б) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d),$

$(b, e), (e, b), (b, d), (d, b), (a, c), (c, a)\}$;

в) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (c, a), (a, c)\}$;

г) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d),$

$(b, e), (e, b), (b, d), (d, b)\}$.

2. Постройте функциональную схему для каждого из приведенных ниже отношений на A.

а) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, a), (a, d)\}$;

б) $A = \{a, b, c, d, e, f\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, a), (a, c), (d, e), (e, d),$

$(b, e), (e, b), (b, d), (d, b), (a, c), (c, a)\}$;

в) $A = \{a, b, c, d, e\}$,

$\rho = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e),$

$(e, d), (a, d), (d, a)\}$.

§ 2. Операции над бинарными отношениями

Определение. Пусть ρ_1, ρ_2 – бинарные отношения на A. Тогда под $\rho_1 \cup \rho_2$, $\rho_1 \cap \rho_2$, $\rho_1 \setminus \rho_2$, $\rho_1 \Delta \rho_2$ понимаются обычные теоретико-множественные операции: объединение, пересечение, разность, симметрическая разность множеств.

Определение. Пусть ρ – бинарное отношение на A. Тогда бинарное отношение $A \times A \setminus \rho = \{(a_1, a_2) | (a_1, a_2) \notin \rho\}$ называется дополнением бинарного отношения ρ и обозначается $\bar{\rho}$.

Определение. Пусть ρ – бинарное отношение на A. Тогда бинарное отношение ρ^{-1}, задаваемое условием $(a_1, a_2) \in \rho^{-1} \Leftrightarrow$ $\Leftrightarrow (a_2, a_1) \in \rho$, называется *обратным к* ρ.

Заметим, что $\bar{\rho} \neq \rho^{-1}$ в общем случае.

Чтобы получить обратное бинарное отношение ρ^{-1}, необходимо в орграфе отношения ρ сменить направления всех стрелок, не являющихся петлями, на противоположные.

Определение. Пусть ρ, σ – бинарные отношения на A. Тогда произведение отношения ρ на отношение σ (обозначается $\rho\,\sigma$ или $\rho \cdot \sigma$) равно бинарному отношению τ такому, что $(a, b) \in \tau \Leftrightarrow \exists c \in A$ и $(a, c) \in \rho, (c, b) \in \sigma$.

Эту операцию произведения для конечных множеств очень удобно производить на функциональных схемах.

Пример. На множестве $A = \{1, 2, 3, 4, 5\}$ рассмотрим отношения $\rho = \{(1, 2), (2, 2), (2, 3), (3, 5), (4, 4)\}$,
и $\sigma = \{(2, 1), (1, 3), (3, 4), (5, 1)\}$.

Тогда $\rho\sigma = \{(1,1),(2,1),(2,4),(3,1)\}$ и

$\sigma\rho = \{(1,5),(2,2),(3,4),(5,2)\}$ (рис. 5).

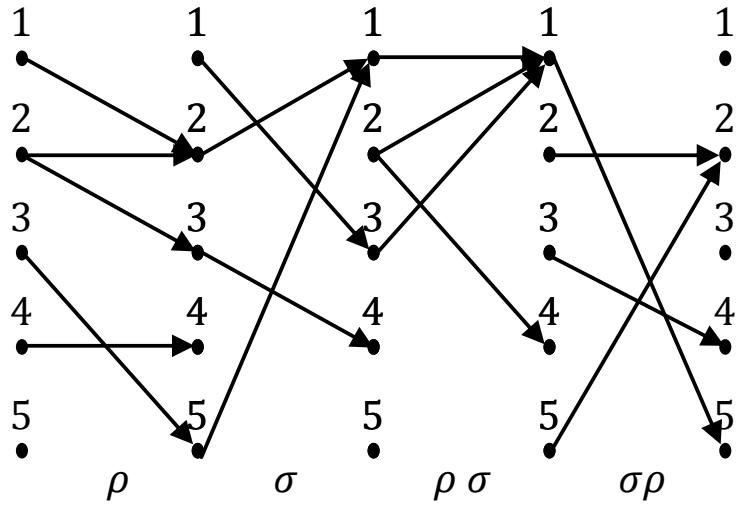

Рис. 5

Таким образом, умножение бинарных отношений не коммутативно.

Упражнения для самостоятельной подготовки

Пусть $A = \{a, b, c, d, e\}$ и $\rho, \sigma, \tau, \varphi$ – отношения на A, где

$\rho = \{(a,a),(a,b),(b,c),(b,d),(c,e),(e,d),(c,a)\}$,

$\sigma = \{(a,b),(b,a),(b,c),(b,d),(e,e),(d,e),(c,b)\}$,

$\tau = \{(a,b),(a,a),(b,c),(b,b),(e,e),(b,a),(c,b),$

$(c,c),(d,d),(a,c),(c,a)\}$,

$\varphi = \{(a,b),(b,c),(b,b),(e,e),(b,a),(c,b),(d,d),(a,c),(c,a)\}$.

Опишите отношения $\tau \cap \varphi$, $\rho \cup \sigma$, $\tau\backslash\sigma$, $\tau\Delta\rho$, τ^{-1}, $\bar{\rho}$, $\rho\varphi$.

§ 3. Основные свойства бинарных отношений

Определение. Бинарное отношение ρ на A называется *рефлексивным*, если для любого $a \in A$ выполняется $a\rho a((a,a) \in \rho)$.

Это означает, что в матрице рефлексивного бинарного отношения на главной диагонали стоят единицы, а в орграфе этого отношения у каждой вершины имеется петля.

Определение. Бинарное отношение ρ на A называется *симметричным*, если $(a_1, a_2) \in \rho \Leftrightarrow (a_2, a_1) \in \rho$.

Матрица симметричного бинарного отношения является симметричной, а в орграфе этого отношения все стрелки, не являющиеся петлями, двусторонние.

Определение. Бинарное отношение ρ на A называется *антисимметричным*, если $(a_1, a_2) \in \ , (a_2, a_1) \in \ \Longrightarrow a_1 = a_2$.

Это означает, что в орграфе этого отношения все стрелки между разными вершинами односторонние.

Определение. Бинарное отношение на A называется *транзитивным*, если из $(a, b) \in \ , (b, c) \in$ всегда следует, что $(a, c) \in$.

Транзитивность плохо распознается на матрицах, но хорошо распознается на графах: бинарное отношение транзитивно тогда и только тогда, когда любая двухзвенная направленная ломаная в соответствующем орграфе замыкается стрелкой из начала этой ломаной в ее конец (рис. 6).

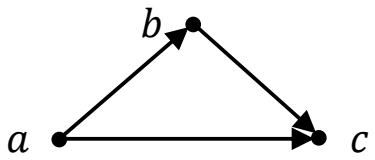

Рис. 6

Определение. Бинарное отношение на A называется *полным*, если для любых $a_1, a_2 \in A$ выполняется $(a_1, a_2) \in$ или $(a_2, a_1) \in$.

Определение. Бинарное отношение на A называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Пример. Пусть $A = \mathbb{Z}$. Зафиксируем некоторое ненулевое целое число n. Определим бинарное отношение следующим образом: $\forall a, b \in A$ $(a, b) \in$ $\Leftrightarrow a - b$ делится на n без остатка.

Докажем, что – отношение эквивалентности.

Рефлексивность: $a \in \mathbb{Z}$ $a - a = 0$ делится на n, следовательно, $\forall a \in \mathbb{Z}, (a, a) \in$.

Симметричность: $a, b \in \mathbb{Z}$ $(a, b) \in$, следовательно, $a - b$ делится на n, а значит, и $b - a$ делится на n, т. е. $(b, a) \in$.

Транзитивность: Пусть $(a, b) \in$, $(b, c) \in$. Тогда $a - b$ и $b - c$ делятся на n, откуда $a - c = (a - b) + (b - c)$ делится на n, следовательно, $(a, c) \in$.

Мы доказали, что отношение является отношением эквивалентности. Оно называется отношением сравнения по модулю n.

Упражнения для самостоятельной подготовки

1. Докажите, что пересечение рефлексивных отношений рефлексивно.

2. Докажите, что пересечение симметричных отношений симметрично.

3. Пусть $A = \{a, b, c, d, e\}$:

а) опишите отношение на A, которое рефлексивно, но не является ни симметричным, ни транзитивным;

б) опишите отношение на A, которое симметрично, но не является ни рефлексивным, ни транзитивным;

в) опишите отношение на A, которое транзитивно, но не является ни рефлексивным, ни симметричным;

4. Пусть $A = \{a, b, c, d, e\}$:

а) опишите отношение на A, которое рефлексивно и симметрично, но не является транзитивным;

б) опишите отношение на A, которое симметрично и транзитивно, но не является рефлексивным;

в) опишите отношение на A, которое рефлексивно и транзитивно, но не является симметричным;

5. $\mathbb{N} = \{1,2,3,4,5,6,7,8\}$. Проверьте для указанных ниже отношений основные свойства:

1) $x\rho_1 y \Leftrightarrow x + y$ – четно;
2) $x\rho_2 y \Leftrightarrow x + y$ – нечетно;
3) $x\rho_3 y \Leftrightarrow x + y > 0$;
4) $x\rho_4 y \Leftrightarrow x - y > 0$.

§ 4. Классы эквивалентности

Определение. Пусть $-$ отношение эквивалентности на A. Тогда *классом отношения с представителем* $a \in A$ называется множество всех $b \in A$, таких, что $(a, b) \in$. Обозначается $\overline{a}$ ($\overline{a}_{\rho}$, $[a]_{\rho}$, a^{ρ}).

Теорема. Пусть $-$ отношение эквивалентности на A. Тогда классы отношения ρ обладают следующими свойствами:

1) $\forall a \in A \;\; a \in \overline{a}$;

2) $b \in \overline{a} \;\Rightarrow \overline{b} = \overline{a}$;

3) различные классы эквивалентности пересекаются по пустому множеству;

4) $\overline{a} = \overline{b} \Leftrightarrow a \;\; b$.

Доказательство:

1) В силу рефлексивности отношения ρ имеем $a \;\; a$, а значит, $a \in \overline{a}$. Свойство 1 доказано.

2) Пусть $b \in \overline{a}$. Тогда по определению класса эквивалентности $(a, b) \in$.

Предположим $x \in \overline{b}$. Тогда $(b, x) \in$ и $(a, b) \in$. В силу транзитивности имеем $(a, x) \in$, а значит, $x \in \overline{a}$ и $\overline{b} \subseteq \overline{a}$.

Теперь пусть $x \in \overline{a}$. Тогда $(a, x) \in$ и $(b, a) \in$ (в силу симметричности). В силу транзитивности , имеем $(b, x) \in$, а значит, $x \in \overline{b}$ и $\overline{a} \subseteq \overline{b}$.

Так как $\overline{b} \subseteq \overline{a}$ и $\overline{a} \subseteq \overline{b}$, то $\overline{b} = \overline{a}$. Свойство 2 доказано.

3) Пусть $\bar{a} \cap \bar{b} \neq \emptyset$. Тогда существует элемент $x \in A$ такой, что $x \in \bar{a}$ и $x \in \bar{b}$. По пункту 2 $\bar{x} = \bar{a}$ и $\bar{x} = \bar{b}$, а значит, $\bar{a} = \bar{b}$. Свойство 3 доказано.

4) $\bar{a} = \bar{b} \Rightarrow b \in \bar{a} \Rightarrow (a, b) \in \rho$.

$a\rho b \Rightarrow b \in \bar{a} \Rightarrow \bar{b} = \bar{a}$ по свойству 2. Свойство 4, а вместе с ним и теорема, доказаны.

Определение. Разбиением множества A называется семейство его непустых подмножеств A_i, $i \in I$ таких, что

1) $A = \bigcup_{i \in I} A_i$;

2)$\forall i, j \in I\ A_i \cap A_j = \emptyset$ при $i \neq j$.

Из этого определения и предыдущей теоремы следует:

Теорема. Множество всех классов эквивалентности ρ на множестве A является разбиением этого множества A.

Определение. Множество всех классов эквивалентности ρ обозначается G/ρ и называется фактор-множеством G по отношению ρ.

Верно обратное утверждение к предыдущей теореме.

Теорема. Пусть дано разбиение $\{A_i: i \in I\}$ множества A. Определим отношение ρ на A следующим образом: $(x, y) \in \rho \Leftrightarrow$ $\Leftrightarrow \exists\, i \in I$ что $x, y \in A_i$. Тогда ρ −отношение эквивалентности на A и множества A_i − в точности классы этой эквивалентности.

Доказательство. 1) $\forall\, x \in A, (x, x) \in \rho$, так как по определению разбиения элемент x принадлежит одному из A_i. Рефлексивность ρ доказана.

2) $\forall x,\ y \in A, (x,\ y) \in \rho \Leftrightarrow\ \exists\, i \in I,$ что $x,\ y \in A\_i \Leftrightarrow \exists\, i \in I$, что $y, x \in A\_i \Leftrightarrow (y, x) \in \rho$.Симметричность ρ доказана.

3) $\forall x, y, z \in A\ (x, y) \in \rho,\ (y, z) \in \rho\ \Leftrightarrow\ x, y \in A_i,\ y, z \in A_j$ для некоторых $i, j \in I$. Поэтому $y \in A_i \cap A_j$ и в силу определения разбиения множества $A_i = A_j$, т. е. $\exists\, i \in I,$ что $x, z \in A_i$ и, значит, $(x, z) \in \rho$. Транзитивность ρ доказана.

Из 1–3-го доказательств следует, что ρ отношение эквивалентности.

Пусть $x \in A$. Тогда, в силу определения разбиения, $\exists!\, i \in I$ такое, что $x \in A_i$. Далее $\bar{x} = \{y \in A | (x, y) \in \rho\}$, т. е. $\bar{x} = \{y \in A | x, y \in A_i\} = \{y \in A | y \in A_i\} = A_i$. ■

Упражнения для самостоятельной подготовки

1. Установите, является ли каждое из перечисленных ниже отношений на A отношением эквивалентности. Для каждого отношения эквивалентности постройте классы эквивалентности.

а) A − множество целых чисел, и ρ есть отношение, заданное условием $(a, b) \in \rho$, если $a + b = 0$;

б) A − множество целых чисел, и ρ есть отношение, заданное условием $(a, b) \in \rho$, если $a + b = 5$;

в) A – множество упорядоченных пар целых чисел, и ρ есть отношение, заданное условием $(a, b)\rho(c, d)$, если $ad = bc$;

г) $A = \{-10,\ -9,\ -8, \dots, 0, 1, \dots, 9, 10\}$ и $(a, b) \in \rho$, если $a^2 = b^2$;

д) $A = \{-10,\ -9,\ -8, \dots, 0, 1, \dots, 9, 10\}$ и $(a, b) \in \rho$, если $a^3 = b^3$.

2. Установите, является ли каждое из перечисленных ниже отношений на A отношением эквивалентности. Для каждого отношения эквивалентности постройте классы эквивалентности.

а) A – множество всех подмножеств множества $\{a,\ b,\ c,\ d\}$, отношение ρ определяется следующим образом: $s\rho t$, если s и t содержит одинаковое количество элементов;

б) $A = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$, отношение ρ определяется следующим образом: $a\rho b$, если $a + b$ четное;

в) $A = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$, отношение ρ определяется следующим образом: $a\rho b$, если $a + b$ положительное.

3. Множества $A_1 = \{1,7\}, A_2 = \{2,3,8\}, A_3 = \{4,5,6\}$ образуют разбиение множества $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Соответствующую эквивалентность ρ на A задать матрицей, орграфом и функциональной схемой.

§ 5. Частичный порядок

Определение. Бинарное отношение ρ на множестве A называется *частичным порядком*, если ρ рефлексивно, антисимметрично и транзитивно. При этом A называется *частично упорядоченным множеством (ЧУМ)*.

Основные примеры.

1. Множество $\mathbb{R}$ всех действительных чисел – ЧУМ относительно обычного сравнения чисел $a\rho b \Leftrightarrow a \leq b$.

Рефлексивность, антисимметричность и транзитивность здесь очевидны.

2. Множество $\mathbb{N}$ всех натуральных чисел – ЧУМ относительно отношения делимости натуральных чисел: $a\rho b \Leftrightarrow a|b$ (a делит b).

Докажем это.

1) $\forall a \in \mathbb{N}\ \ a|a$ – очевидно.

2) $\forall a, b \in \mathbb{N}$, если $a|b$ и $b|a$, то $b = k \cdot a, a = m \times b$, откуда $b = k \cdot m \cdot b$, т. е. $k = m = 1$ и $a = b$.

3) $\forall a, b, c \in \mathbb{N}$, если $a|b$ и $b|c$, то $b = k \cdot a,\ \ c = m \times b$, откуда $c = m \cdot k \cdot a$, т. е. $a|c$.

3. Для любого множества X через $B(X)$ (или 2^X) обозначается множество всех подмножеств множества X. Множество $B(X)$ называется булеаном множества X.

На $B(X)$определим бинарное отношение ρ следующим образом:

$\forall A, B \in B(X)$ $A\rho B \Leftrightarrow A \subseteq B$. Это отношение называется отношением включения. Очевидно, что $\forall A, B, C \in B(X)$.

1) $A \subseteq A$.

2) $A \subseteq B, B \subseteq A \Rightarrow A = B$.

3) $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$.

Следовательно, отношение включения – частичный порядок на $B(X)$.

Замечание. В дальнейшем в этом параграфе частичный порядок на произвольном множестве X будем обозначать «≤», т. е. вместо $a\rho b$ будем писать $a \leq b$ для любых $a, b \in X$. Кроме того, при $a \leq b$ принято говорить, что a не превосходит b или a меньше или равно b. Далее, $a < b$ означает, что $a \leq b$ и $a \neq b$. В этом случае принято говорить, что a меньше b или b больше a.

Определение. Пусть X – ЧУМ. Элемент b из X *накрывает элемент* $a \in X$, если $a < b$ и не существует элемента c из X такого, что $a < c < b$.

Определение. Частичный порядок «≤» на X называется *линейным,* если любые два элемента из X сравнимы относительно этого порядка, т. е. для любых $a, b \in X$ $a \leq b$ или $b \leq a$. При этом X называется *линейно упорядоченным множеством*, или *цепью*.

Определение. *Диаграммой Хассе* называется множество точек на плоскости вместе с некоторыми негоризонтальными отрезками, соединяющими эти точки, без замыканий ломанных линий длины ≥ 2.

Определение. *Диаграммой Хассе частично упорядоченного множества* $X = \{x_1, \dots, x_n\}$ называется такая диаграмма Хассе, состоящая из точек, обозначенных $x_1, \dots, x_n$, что для любых i, j точка x_i соединена с точкой x_j и при этом x_i расположена ниже точки x_j тогда и только тогда, когда x_j накрывает x_i.

Пример. Пусть $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ и частичный порядок на X – отношение делимости. Тогда диаграмма Хассе (рис. 7) имеет вид

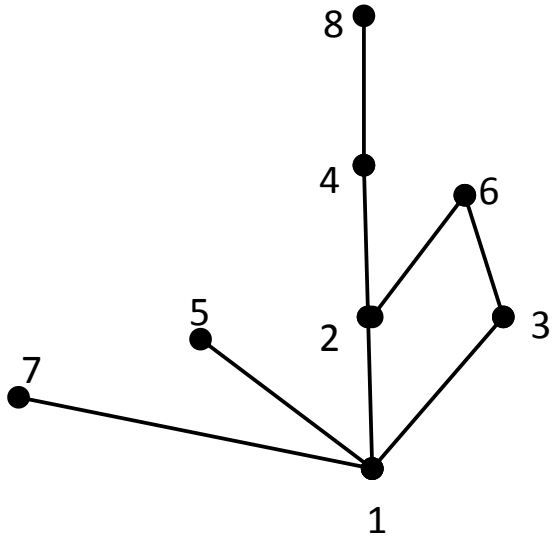

Рис.7

Ясно, что любая диаграмма Хассе с точками, обозначенными $x_1, \dots, x_n$, задает частичный порядок «≤» на множестве $X = \{x_1, \dots, x_n\}$, диаграммой Хассе которого является исходная диаграмма, а именно $x_i < x_j$, тогда и только тогда, когда от точки x_i можно добраться до точки x_j по отрезкам данной диаграммы, нигде при этом не спускаясь вниз.

Пример. Задать списком частичный порядок «≤» на множестве $X = \{1, 2, 3, 4, 5\}$, если его диаграмма Хассе (рис. 8) имеет вид

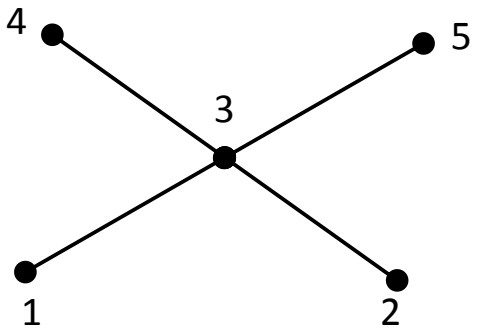

Рис.8

Ответ очевиден: $a \leq b \Leftrightarrow (a, b) \in \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5)\}$.

Отметим, что диаграммой Хассе линейно упорядоченного множества является вертикальная цепь. Например, если $|X| = 4$, то его диаграмма Хассе (рис. 9) имеет вид

Рис.9

Полурешетки и решетки

Определение. Пусть X – ЧУМ, $Y \subseteq X$. Тогда элемент $y \in Y$ называется *максимальным (минимальным)* в Y, если не существует такого элемента x в Y, для которого $y < x$ $(y > x)$.

Определение. Пусть X – ЧУМ, $Y \subseteq X$. Тогда элемент $y \in Y$ называется *наибольшим (наименьшим)* в Y, если $\forall x \in Y \ x \leq y$ $(y \leq x)$.

Ясно, что наибольший (наименьший) элемент множества Y является максимальным (минимальным). Однако то, что элемент является максимальным (минимальным), не означает, что он является наибольшим (наименьшим) в рассматриваемом множестве. Например, в последнем примере элементы 4 и 5 являются максимальными в X, но ни один из них не является наибольшим в X. Аналогично 1 и 2 – минимальные в X, но ни один из них не является наименьшим в X.

Определение. Пусть X – ЧУМ, $Y \subseteq X$. Элемент $x \in X$ называется *верхней (нижней) гранью множества* Y, если $\forall y \in Y$ $y \leq x$ $(x \leq y)$.

Определение. Пусть X – ЧУМ, $Y \subseteq X$. Наименьший элемент x в множестве всех верхних граней множества Y называется его *точной верхней гранью:* $x = \sup Y$. Аналогично наибольший элемент z в множестве всех нижних граней множества Y называется *нижней гранью*: $z = \inf Y$.

Ясно, что $\inf Y$ и $\sup Y$ не всегда существуют. Например, в последнем примере не существуют $\sup\{4,5\}$, $\inf\{1,2\}$, но существуют $\inf\{4,5\} = \sup\{1,2\} = 3$.

Определение. *Нижней (верхней) полурешеткой (или полуструктурой)* называется такой ЧУМ X, что $\forall a, b \in X$ существуют $\inf\{a, b\}(\sup\{a, b\})$.

Определение. Если ЧУМ X одновременно и нижняя, и верхняя полурешетки, то X называется *решеткой (структурой)*.

Если опять вернуться к тому же примеру, то рассматриваемый в нем ЧУМ не является ни нижней, ни верхней полурешеткой. Очевидно, что любое линейно упорядоченное множество X является решеткой:

$\forall a, b \in X$ при $a \leq b \sup\{a, b\} = b$, $\inf\{a, b\} = a$.

Кроме того, частично упорядоченные множества, рассмотренные в примерах 2 и 3 в начале параграфа, тоже являются решетками. Если $\mathbb{N}$ – ЧУМ относительно отношения делимости, то $\forall a, b \in \mathbb{N}$ $\sup\{a, b\} = \text{НОК}(a, b)$ – наименьшее общее кратное a и b, $\inf\{a, b\} = \text{НОД}(a, b)$ – наибольший общий делитель a и b. Если $B(X)$ – ЧУМ относительно включения, то $\forall A, B \in B(X)$ $\sup\{A, B\} = A \cup B$, $\inf\{A, B\} = A \cap B$.

Замечание. Обычно в нижней полуструктуре X вместо $\inf\{a, b\}$ пишут $a \wedge b$ и в верхней полуструктуре X вместо $\sup\{a, b\}$ пишут $a \vee b$ для любых $a, b \in X$.

Пример. В структуре (рис. 10)

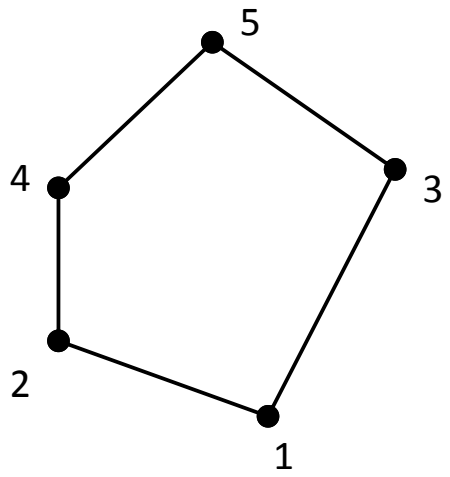

Рис. 10

$5 \wedge 2 = 2 \wedge 5 = 2, 3 \wedge 4 = 4 \wedge 3 = 1, 4 \vee 3 = 3 \vee 4 = 5.$

Определение. *Нулем* (0) упорядоченного множества X называется его наименьший элемент, *единицей* (1) X называется наибольший элемент X.

Определение. Структура X с 0 и 1 *называется структурой с дополнениями*, если $\forall a \in X\ \exists!\, b \in X$ – такой, что $a \vee b = 1, a \wedge \wedge b = 0$.

При этом b обозначается a'(или $\bar{a}$) и называется *дополнением* к a.

Определение. Структура X называется *дистрибутивной*, если $\forall a, b \in X\ \ (a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ и $(a \wedge b) \vee c = = (a \vee c) \wedge (b \vee c)$.

Определение. Дистрибутивная структура с дополнениями называется *булевой алгеброй*.

Примеры. Булевой алгеброй является, например булеан $B(X)$, где $\forall Y \in B(X),\ \bar{Y} = X \backslash Y$, и свойства дистрибутивности

легко доказываются: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

В качестве примера дистрибутивной структуры, без дополнений можно взять ЧУМ $\mathbb{R}$ относительно обычного отношения порядка.

Докажем, что$\max(\min(a, b), c) = \min(\max(a, c), \max(b, c))$.

Без ограничения общности, $a \leq b$. Рассмотрим три варианта:

1.

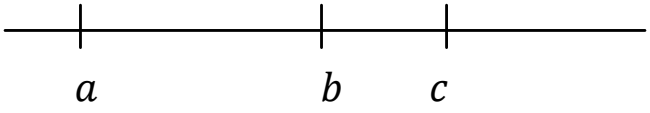

Рис.11

2.

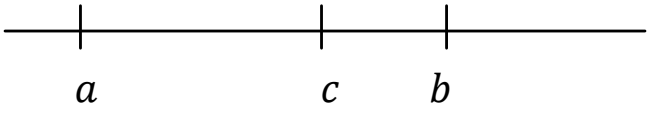

Рис.12

3.

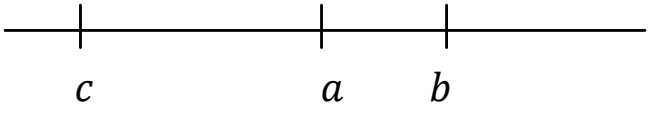

Рис.13

Легко убедиться, что в первых двух вариантах обе части доказываемого равенства равны c, а в третьем варианте обе части равны a.

Аналогично доказывается, что $\min(\max(a, b), c) =$ $= \max(\min(a, c), \min(b, c))$.

Упражнения для самостоятельной подготовки

1. Выписать все упорядоченные пары, принадлежащие соответствующему частичному порядку, (рис. 14).

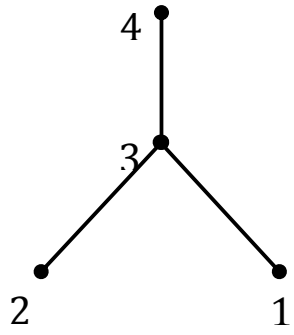

Рис. 14

2. Какое из приведенных ниже отношений ρ является отношением частичного порядка на $A = \{a, b, c, d\}$?

а) $\rho = \{(a,a),(b,b),(c,c),(d,d),(a,c),(b,c),(c,d),(a,d),(b,d)\}$;

б) $\rho = \{(a,a),(b,b),(c,c),(d,d),(a,c),(b,c),(c,d),(d,a)\}$;

в) $\rho = \{(b,b),(c,c),(d,d),(a,c),(b,c),(c,d),(a,d),(b,d)\}$;

г) $\rho = \{(a,a),(b,b),(c,c),(d,d),(a,b),(a,c),(b,c)(c,d),(a,d),$
$(b,d),(c,d)\}$.

§ 6. Рефлексивное, симметричное и транзитивное замыкание бинарного отношения

Определение. Пусть $\rho -$ бинарное отношение на M. Тогда его *рефлексивным замыканием* называется наименьшее рефлексивное бинарное отношение на M, содержащее ρ.

Определение. Пусть ρ – бинарное отношение на M. Тогда его *симметричным замыканием* называется наименьшее симметричное бинарное отношение на M, содержащее ρ.

Определение. Пусть ρ – бинарное отношение на M. Тогда его *транзитивным замыканием* называется наименьшее транзитивное бинарное отношение на M, содержащее ρ.

Теорема 1. Чтобы получить транзитивное замыкание ρ на множестве M, надо в орграфе ρ замкнуть все направленные ломаные линии этого орграфа.

Доказательство:

Докажем, что после этой операции (замыкания всех ломаных) получится действительно транзитивное замыкание.

Пусть ρ – исходное бинарное отношение,

ρ^* – бинарное отношение, полученное из ρ путем замыкания всех ломаных.

$(a, b) \in \rho^*$, $(b, c) \in \rho^*$. Требуется доказать, что $(a, c) \in \rho^*$.

По условию в орграфе ρ существуют направленные ломаные L_1 от a до b и L_2 от b до c. Объединение L_1 и L_2 – это ломаная L, соединяющая a и c. Следовательно, $(a, c) \in \rho^*$.

Далее, $\rho \subseteq \rho^*$, так как любая стрелка является замыканием самой себя.

Осталось доказать, что ρ^* – наименьшее бинарное отношение, содержащее ρ.

Пусть $\rho \subseteq \sigma$, σ транзитивно.

Требуется доказать, что $\rho^* \subseteq \sigma$.

Пусть $(a, b) \in \rho^*$.

Тогда $(a, a_1) \in \rho$, $(a_1, a_2) \in \rho$, $\cdots, (a_m, b) \in \rho$ для некоторых $a_1, \ldots, a_m \in M$ или $(a, b) \in \rho$.

Следовательно, $(a, a_1) \in \sigma, (a_1, a_2) \in \sigma, \cdots, (a_m, b) \in \sigma$ или $(a, b) \in \sigma$. Так как σ транзитивно, то $(a, b) \in \sigma$. Теорема доказана полностью.

Следствие. Если ρ – бинарное отношение на множестве A и $|A| = n$, то транзитивное замыкание отношения ρ равно $\rho \cup \rho^2 \cup \ldots \cup \rho^n$.

Алгоритм Уоршалла для нахождения транзитивного замыкания

Все элементы данного множества M, для которого рассматривается отношение ρ, получают свой номер: $1, 2, 3, 4, \ldots, n$. Замыкаются все ломаные в орграфе ρ, где 1 является посредником, потом замыкаются все ломаные в новом орграфе, где 2 является посредником, и так далее до n.

Упражнения для самостоятельной подготовки

1. Обосновать алгоритм Уоршалла.
2. Найти транзитивное замыкание бинарного отношения $\rho = \{(12), (23), (24), (31), (43), (51), (53)\}$ на множестве $M = \{1,2,3,4,5\}$ с использованием следствия к теореме 1 и с помощью алгоритма Уоршалла.

§ 7. Бинарные отношения из множества в множество

Определение. *Бинарным отношением* из A в B называется подмножество в $A \times B$.

Рассмотренные ранее бинарные отношения на множестве M – бинарные отношения из Mв M.

Определение. Если ρ – бинарное отношение из A в B, то *образом* $x \in A$ называется $\{y \in B | (x, y) \in \rho\}$, *прообразом* $y \in B$ называется $\{x \in A | (x, y) \in \rho\}$. Образ x обозначается $(x)\rho$, или просто $x\rho$, а прообраз y – $(y)\ \rho^{-1}$, или просто $y\ \rho^{-1}$. Часто вместо $(x)\rho$ пишут $\rho(x)$, вместо $(y)\ \rho^{-1}$ – $\rho(y)$.

Определение. *Областью определения* бинарного отношения ρ из A в B называется множество всех элементов из A, имеющих непустой образ, а *областью значений* отношения ρ называется множество элементов из B, для которых прообраз непустой.

Бинарное отношение из A в B удобно рассмотреть на схемах.

Пример.

$A = \{1, 2, 3, 4\}, B = \{\alpha, \beta, \gamma\}, \rho = \{(1, \gamma), (2, \alpha), (2, \beta), (4, \alpha), (4, \beta)\}$.

Область определения – $\{1, 2, 4\}$.

Область значений– $\{\alpha, \beta, \gamma\}$.

$\rho(2) = \{\alpha, \beta\}, \rho(4) = \{\alpha, \beta\}, \rho^{-1}(\alpha) = \{2,4\}, \rho^{-1}(\beta) = \{2,4\}, \rho^{-1}(\gamma) = \{1\}$.

Определение. Пусть ρ – бинарное отношение из A в B. Тогда *обратным бинарным отношением* к ρ называется отношение ρ^{-1} из B в A: $(b, a) \in \rho^{-1} \Leftrightarrow (a, b) \in \rho$.

Чтобы получить ρ^{-1}, надо в схеме обратить все стрелки.

Определение. Пусть ρ – бинарное отношение из A в B, σ – бинарное отношение из B в C. Тогда ρσ – бинарное отношение из A в C такое, что $(a,c) \in \rho\sigma \Leftrightarrow \exists b \in B, (a,b) \in \rho, (b,c) \in \sigma$.

Определение. Бинарное отношение ρ из A в B называется отображением A в B, если $\forall a \in A \ |\rho(a)| = 1$, то есть $\forall a \in A, \exists! b \in B$, что $a\rho b$; $b = \rho(a) -$ образ a.

$\rho^{-1}(b) = \{a \in A | \rho(a) = b\}$.

Полезны отображения специального вида, которые будут рассмотрены далее.

Определение. Отображение f из A в B называется *инъективным (инъекцией)*, если $\forall a_1, a_2 \in A \ a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.

Определение. Отображение f из A в B называется *сюръективным (сюръекцией)*, если каждый элемент из B имеет хотя бы один прообраз. $\forall b \in B \ \exists a \in A$ – такой, что $f(a) = b$.

Определение. Отображение f из A в B называется биективным (биекция), если оно инъективно и сюръективно.

Теорема. Пусть $|A| = |B| < +\infty$,

$f -$ отображение из A в B. Тогда $f -$инъекция $\Leftrightarrow$ $f -$сюръекция. Доказательство предоставляем читателю.

Замечание. То, что f – отображение множества A в множество B, записывается следующим образом: $f: A \to B$.

Упражнения для самостоятельной подготовки

1. Выясните, какие из приведенных ниже функций из $\mathbb{R}$ в $\mathbb{R}$ являются инъективными, сюръективными, имеют обратную функцию:

   а) $f(x) = |x|$;

   б) $f(x) = x^2 + 4$;

   в) $f(x) = x^3 + 6$;

   г) $f(x) = |x| + x$;

   д) $f(x) = x(x-2)(x+2)$.

2. Пусть $f: A \longrightarrow B,\ g: B \longrightarrow C,\ h: C \longrightarrow D$,

   $A = \{1,2,3,4,5\}, B = \{a,b,c,d\}, C = \{x,y,z,v\}, D =$
   $= \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ и f, g, h заданы схемами (рис. 15):

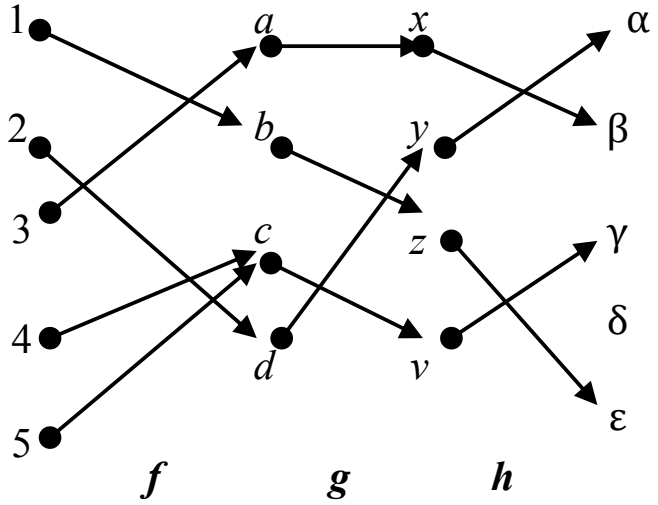

Рис. 15

Составить схемы для $fg, gh, (fg)h$. Проверить для отображений $f, g, h, fg, gh, (fg)h$ инъективность и сюръективность.

Глава II. Элементы общей алгебры

§ 1. Группоиды и полугруппы

Определение. На множестве G задана (определена) бинарная операция, обозначаемая «·», если каждой упорядоченной паре элементов $a, b \in G$ поставлен в соответствие элемент снова из G, обозначаемый $a \cdot b$ и называемый произведением a и b. Само множество G при этом называется *группоидом.*

Если $G -$ конечное множество, то бинарную операцию можно задавать с помощью таблицы Кэли (табл. 1).

Таблица 1

$G = \{g_1, \dots, g_n\}$

	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1	g_1g_1	$\cdots$	g_1g_j	$\cdots$	g_1g_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_i	g_ig_1	$\cdots$	g_ig_j	$\cdots$	g_ig_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_n	g_ng_1	$\cdots$	g_ng_j	$\cdots$	g_ng_n

Верно и обратное утверждение: любая таблица Кэли, т. е. таблица указанного вида, заполненная элементами из $G = \{g_1, \dots, g_n\}$, определяет группоид.

Если для обозначения операции используется «·», то операция группоида записывается мультипликативно.

Определение. Пусть G – группоид с мультипликативной записью бинарной операции. Тогда G называется полугруппой,

если в G выполняется ассоциативный закон: $\forall a, b, c \in G\ (ab)c = a(bc)$.

Определение. Пусть G – группоид с мультипликативной операцией. Элемент $e \in G$. Тогда e называется *правой единицей* G, если $\forall a \in G\ ae = a$ и e называется *левой единицей*, если $\forall a \in G\ ea = a$. Если e одновременно и правая, и левая единица, то e называется просто *единицей* (либо двусторонней единицей).

Лемма. Если в группоиде G имеются правая единица e_1 и левая единица e_2, то они совпадают.

Доказательство. $e_1 = e_1 e_2 = e_2 \Rightarrow e_1 = e_2$.

Следствие. Если в группоиде G имеется единица, то она определяется однозначно. В то же время отдельно левых и отдельно правых единиц может быть бесконечно много.

Определение. Пусть $G -$ группоид, $0 \in G$. 0 – называется *правым нулем* G, если $\forall a \in G\ a0 = 0$ и 0 называется *левым нулем*, если $\forall a \in G\ 0a = 0$. Если 0 одновременно и правый, и левый ноль, то 0 называется двусторонним нулем.

Для нулей имеют место предыдущие лемма и следствие.

Определение. Группоид G называется *полугруппой*, если для любых $a, b, c \in G\ (ab)c = a(bc)$, т. е. операция в G ассоциативна.

Определение. Полугруппа с единицей называется *моноидом.*

Примеры полугрупп.

1) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – полугруппы относительно обычного сложения чисел и относительно обычного умножения чисел.
2) $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ – полугруппы относительно обычного умножения чисел.
3) Обозначим T_X – множество всех так называемых преобразований множества X, т. е. отображений X в себя.

   T_X – полугруппа относительно следующего произведения преобразований: если $\varphi, \psi \in T_X$, то $\forall x \in X \ \ x(\varphi\psi) = (x\varphi)\psi$. Если $X = \{1, \dots, n\}$, то T_X обозначается T_n.

   Элементы из T_n записывают в виде:

   $$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ 1\varphi & 2\varphi & \dots & n\varphi \end{pmatrix}$$
4) Пусть X – любое множество. Определим умножение в X по формуле: $\forall x, y \in X \ xy = y$. Ассоциативность этой операции очевидна. X называется полугруппой правых нулей.

Определение. Группоид G называется *конечным*, если в нем конечное число элементов, называемое *порядком* G и обозначаемое $|G|$.

Определение. Подмножество H в группоиде G называется *подгруппоидом*, если для любых $x, y \in H \ xy \in H$, т. е. H замкнуто относительно операции в G.

Ясно, что любой подгруппоид сам является группоидом и подгруппоид полугруппы является полугруппой.

Определение. Отображение f группоида G в группоид G' называется *гомоморфизмом*, если для любых $x, y \in G$ $f(xy) = = f(x)f(y)$.

Определение. Гомоморфизм f группоида G в группоид G' называется *изоморфизмом*, если f – биекция G на G'; G' при этом называется группоидом, изоморфным G (обозначение: $G \backsimeq G'$).

С точки зрения общей алгебры изоморфные группоиды одинаковы.

§ 2. Алгоритм Лайта

Определение. Группоид S порождается элементами $a_1, \dots, a_n$, если любой элемент из S, отличный от $a_1, \dots, a_n$, представлен в виде произведения $a_{i_1} \dots a_{i_k}$ с некоторой правильной расстановкой скобок $(k \geq 2)$. В этом случае пишут, что $S = =< a_1, \dots, a_n >$.

Определение. *Операцией* $(*)$ для элемента a из группоида S называется бинарная операция на S, определяемая формулой $x * y = x(ay)$.

Определение. *Операцией* $(\circ)$ для элемента a из группоида S называется бинарная операция на S, определенная формулой $x \circ y = (xa)y$.

Пусть $S = \{s_1, \dots, s_n\}$. Ясно, что S – полугруппа $\Leftrightarrow$ для любого элемента a из S таблицы Кэли для операций $(*)$ и $(\circ)$ совпадают.

Лемма. Если для любых x, y из группоида S и некоторых a, b из S $x(ay) = (xa)y$ и $x(by) = (xb)y$, то $\forall x, y \in S$ $x\big((ab)y\big) = \big(x(ab)\big)y$.

Доказательство.

$x\big((ab)y\big) = x(a(by)) = (xa)(by) = \big((xa)b\big)y = \big(x(ab)\big)y.$

Из леммы вытекает, что для доказательства ассоциативности операции в группоиде S достаточно проверить совпадение

$(*)$-таблицы Кэли и $(\circ)$-таблицы Кэли для каждого элемента a из некоторого множества порождающих элементов группоида S.

Проверку такого совпадения можно организовать следующим образом.

Чтобы нарисовать таблицу Кэли для $(*)$-операции, соответствующей элементу a, надо любой y-столбец в исходной таблице Кэли заменить на (ay)-столбец, а чтобы получить таблицу Кэли для $(\circ)$-операции, соответствующей a, надо каждую -строку в исходной таблице Кэли заменить на (xa)-строку.

Однако обе таблицы для $(*)$ операции и $(\circ)$-операции рисовать не надо. Рисуем $(*)$ таблицу Кэли и помечаем каждую -строку этой таблицы элементом xa слева. Этот элемент xa указывает, с какой строкой исходной таблицы надо сравнивать помеченную этим элементом строку рассматриваемой $(*)$-таблицы.

Пример. Пусть группоид S задан таблицей Кэли (табл. 2):

Таблица 2

	a	*b*	*c*	*d*
a	*b*	*a*	*d*	*c*
b	*a*	*b*	*c*	*d*
c	*d*	*c*	*b*	*a*
d	*c*	*d*	*a*	*b*

Ясно, что $S = < a, d >$. Проверим совпадение $(*)$-операции и $(\circ)$-операции для элемента a. Таблица Кэли для $(*)$-операции с помеченными, как указано выше, строками, имеет вид (табл. 3):

Таблица 3

	b	a	d	c
b	a	b	c	d
a	b	a	d	c
d	c	d	a	b
c	d	c	b	a

Первую строку этой таблицы в соответствии с меткой слева сравниваем с b-строкой исходной таблицы Кэли. Получим совпадение строк. Вторую строку данной $(*)$-таблицы сравниваем с a-строкой исходной таблицы. Получим опять совпадение. И, наконец, сравнивая третью строку данной таблицы с d-строкой исходной таблицы, а четвертую строку данной таблицы с c-строкой исходной таблицы, снова получим совпадение строк. Значит, $(*)$-операция и $(\circ)$-операция для элемента a совпадают.

Аналогично строим $(*)$-таблицу для элемента d (табл. 4).

Таблица 4

	c	d	a	b
c	d	c	b	a
d	c	d	a	b
a	b	a	d	c
b	a	b	c	d

Повторяя процесс сравнения строк этой таблицы с соответствующими строками исходной таблицы Кэли, рассмотренной выше, получим снова требуемые совпадения (читатель непременно должен в этом убедиться). Значит, $(*)$-операция и $(\circ)$-операция совпадают и для элемента d.

Следовательно, с учетом леммы S – полугруппа.

Упражнения для самостоятельной подготовки

1. Доказать ассоциативность операции, заданной таблицей Кэли (табл. 5).

Таблица 5

	a	b	c	d	e	f
a	c	e	f	b	d	a
b	d	f	e	a	c	b
c	f	d	a	e	b	c
d	b	a	d	c	f	e
e	b	a	d	c	f	e
f	a	b	c	d	e	f

2. Выписать все таблицы Кэли на множестве $\{a, b\}$ с ассоциативной операцией.

§ 3. Конгруэнции и гомоморфизмы группоидов

Определение. Эквивалентность ρ на группоиде G называется конгруэнцией, если из того, что $a_1 \rho a_2$ и $b_1 \rho b_2$, всегда следует, что $(a_1 b_1)\rho(a_2 b_2)$.

Если ρ – конгруэнция на G, то на фактор-множестве можно определить бинарную операцию следующим образом: $\forall \bar{a}, \bar{b} \in G/\rho \ \bar{a}\bar{b} = \overline{ab}$. Проверим корректность этого определения. Пусть $\bar{c} = \bar{a}$, $\bar{d} = \bar{b}$. Тогда $c \rho a$ и $d \rho b$. Из определения выше следует, что $(cd)\rho(ab)$, а значит, $\overline{cd} = \overline{ab}$, и корректность доказана. Фактор-множество G/ρ с данной бинарной операцией называется фактор-группоидом. Очевидно, что если G – полугруппа, то и G/ρ тоже полугруппа.

Определение. Эквивалентность ρ на группоиде G называется стабильной справа (слева), если из $a \rho b$ и $c \in G$ всегда следует $(ac)\rho(bc)$ $((ca)\rho(cb))$.

Лемма 1. Эквивалентность ρ на группоиде G – *конгруэнция* $\Leftrightarrow \rho$ стабильна и слева, и справа.

Доказательство. Необходимость очевидна. Докажем достаточность. Пусть $a_1 \rho a_2$ и $b_1 \rho b_2$.Тогда $a_1 \rho a_2 \Rightarrow (a_1 b_1)\rho(a_2 b_1)$ и $b_1 \rho b_2 \Rightarrow (a_2 b_1)\rho(a_2 b_2)$, откуда в силу транзитивности ρ имеем $(a_1 b_1)\rho(a_2 b_2)$, что и требовалось доказать.

Пример 1. Построить группоид из 6 элементов с конгруэнцией ρ с тремя классами по 2 элемента и записать таблицу Кэли для G/ρ.

Решение. Удобнее сначала составить таблицу Кэли для классов X_1, X_2, X_3 конгруэнции ρ. Составляем ее произвольным образом (табл. 6):

Таблица 6

	X_1	X_2	X_3
X_1	X_3	X_2	X_1
X_2	X_1	X_1	X_2
X_3	X_2	X_2	X_3

Затем положим $X_1 = \{a, b\}, X_2 = \{c, d\}, X_3 = \{e, f\}$ и построим таблицу Кэли на множестве $\{a, b, c, d, e, f\} = G$ таким образом, чтобы произведение любых элементов $x_i \in X_i$ и $x_j \in X_j$ лежало в классе $X_i X_j$ в соответствии с таблицей выше. Здесь тоже большой элемент произвола. Например, таблица Кэли для G может быть такой (табл. 7):

Таблица 7

	a	b	c	d	e	f
a	f	f	d	c	a	a
b	e	f	c	d	a	a
c	a	b	b	b	c	d
d	b	b	a	a	d	c
e	c	c	d	c	e	f
f	d	d	c	c	e	f

Задача решена.

Более трудными являются задачи обратного типа.

Пример 2. Найти нетривиальную конгруэнцию ρ для группоида $G = \{a, b, c, d, \}$ с таблицей Кэли (табл. 8):

Таблица 8

	a	*b*	*c*	*d*
a	*b*	*c*	*d*	*c*
b	*a*	*b*	*a*	*d*
c	*d*	*a*	*b*	*a*
d	*a*	*d*	*c*	*b*

Решение. Предположим, что $a\rho b$. Тогда в силу правой стабильности ρ имеем $b\rho a$, $c\rho b$, $d\rho a$, $c\rho d$ (из первых строк таблицы), откуда $\bar{a} = G$ и ρ тривиальна.

Предположим теперь, что $a\rho c$. Тогда из первой и третьей строки таблицы Кэли имеем $b\rho d, c\rho a$, $d\rho b$, $c\rho a$ в силу правой стабильности ρ и из первого столбца и третьего столбца имеем $b\rho d, a\rho a$, $d\rho b$, $a\rho c$. Поэтому есть надежда, что эквивалентность ρ с классами $\{a, c\}$ и $\{b, d\}$ является конгруэнцией. Проверяем эту гипотезу на исходной таблице Кэли. Она оказывается верной, и если $X = \{a, c\}$, $Y = \{b, d\}$, то G/ρ имеет таблицу Кэли (табл. 9):

Таблица 9

	X	Y
X	Y	X
Y	X	Y

Задача решена.

Определение. Пусть S – полугруппа. Тогда непустое подмножество L в S называется *левым идеалом* S, если $SL \subseteq L$, т. е. $\forall s \in S, \forall x \in L, sx \in L$. Аналогично определяется *правый идеал*.

Определение. *Двусторонним идеалом (или просто «идеалом»)* полугруппы S называется подмножество I в S, являющееся одновременно и левым, и правым идеалом, т. е. $SI \subseteq S$ и $IS \subseteq I$.

Очевидно, что идеал в S любого вида является подполугруппой в S.

Пусть I – произвольный идеал в полугруппе S. Определим эквивалентность ρ на S следующим образом: $\forall a \in S$ при $a \notin I$, $\bar{a} = \{a\}$ и при $a \in I$ $\bar{a} = I$.

Лемма 2. Определенная выше эквивалентность ρ – конгруэнция.

Доказательство. Пусть $a\rho b$, $c \in S$. Если $a \notin I$, то $b = a$ и то, что $(ac)\rho(bc)$ и $(ca)\rho(cb)$, является очевидным.

Если $a \in I$, то $b \in I$, и т. к. I – идеал, то $ac\rho bc$ и ρ стабильно и справа, и слева. Значит, по лемме 1 ρ – конгруэнция.

Определение. Фактор-полугруппа S/ρ по конгруэнции, описанной выше, называется *фактор-полугруппой Риса по идеалу I (или по модулю I)* и обозначается S/I.

Лемма 3. Пусть $f: S \to S'$ – гомоморфизм группоидов. Тогда отношение ρ на S такое, что $a\rho b \Leftrightarrow f(a) = f(b)$ является конгруэнцией.

Доказательство. Пусть $a\rho b$ и $c \in S$. Тогда $f(a) = f(b)$, откуда $f(ac) = f(a)f(c) = f(b)f(c) = f(bc)$, т. е. $ac\rho bc$ и, значит, ρ стабильно слева. Аналогично, ρ стабильно справа и, следовательно, ρ – конгруэнция. ■

Рассмотренное выше отношение ρ, называется *ядром гомоморфизма* f.

Лемма 4. Если ρ – произвольная конгруэнция на группоиде S, то отображение $\rho: S \to \frac{S}{\rho}$, определенное формулой $f(s) = \bar{s}\ \forall s \in S$, является гомоморфизмом S на S/ρ.

Отображение f из леммы 4 называется *каноническим* и обозначается как ε_ρ.

Теорема. Пусть f – гомоморфизм группоида S на группоид S', а ρ – его ядро. Тогда существует однозначно определенный изоморфизм $S/\rho \to S'$ такой, что $\forall s \in S\ f(s) = \varphi(\varepsilon_\rho(s))$.

Доказательство. Гомоморфизм φ удовлетворяет равенству выше $\Leftrightarrow \forall s \in S\ f(s) = \varphi(\bar{s})$, т. е. φ определяется однозначно. Докажем корректность последней формулы. Если $\bar{s}=\bar{t}$, то $s\rho t$, откуда $f(s) = f(t)$, т. е. $\varphi(\bar{s}) = \varphi(\bar{t})$, и корректность доказана. Гомоморфность φ очевидна. Докажем инъективность.

Пусть $\varphi(\bar{s}) = \varphi(\bar{t})$. Тогда $f(s) = f(t)$, т. е. $s\rho t$ и, значит, $\bar{s} = \bar{t}$, откуда следует инъективность. И, наконец, $\forall s' \in S'\ \exists s \in S$ такой, что $f(s) = s'$ в силу сюръективности f, а значит, $s' = \varphi(\bar{s})$, и сюръективность φ доказана. ■

Содержание теоремы иллюстрируется диаграммой (рис. 16).

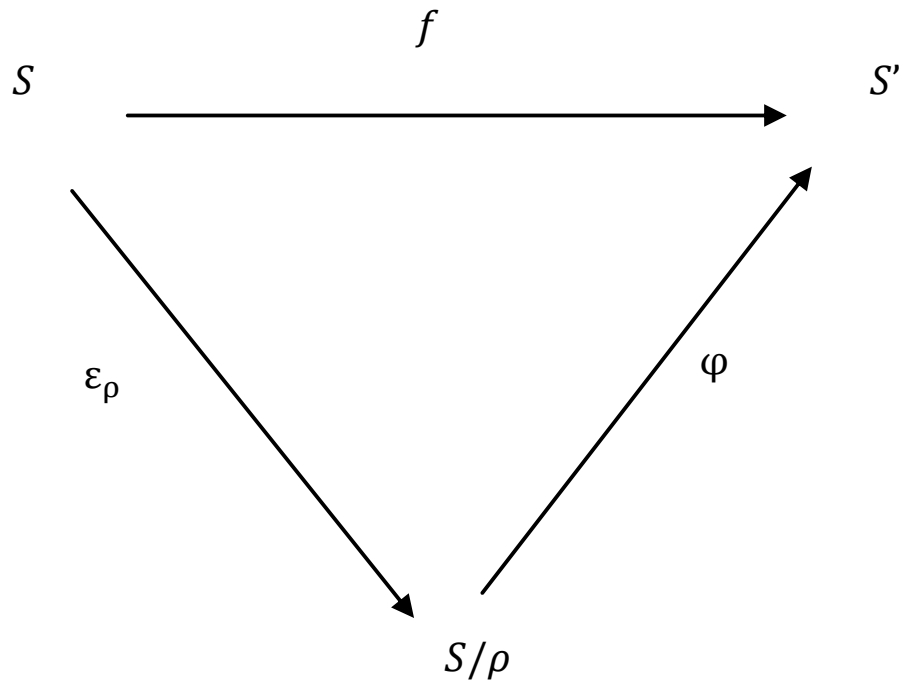

Рис.16

§ 4. Группы

Определение. Группоид G (полугруппа) называется *коммутативным*, если выполняется закон коммутативности, то есть $ab = ba$ для всех $a, b \in G$.

Если для записи операции в группоиде используется знак , то говорят об аддитивной записи. Коммутативный закон имеет вид $a + b = b + a$.

Ассоциативный закон:$(a + b) + c = a + (b + c)$.

Единичный элемент в группоиде G в случае аддитивной записи обозначается нулем:$a = a + 0 = 0 + a \ \ \forall a \in G$.

Кроме того, при необходимости для записи бинарных отношений используются и другие обозначения: $a * b$ или $a \circ b, a \oplus b$.

Определение. Пусть G – множество с бинарной операцией, записываемой мультипликативно. Тогда G называется группой, если:

1) $(ab)c = a(bc) \ \ \forall a, b, c \in G$;

2) Существует элемент 1 *в* G такой, что $\forall a \in G \ \ a1 = 1a = a$ (1 – единица группы);

3) $\forall a \in G \ \ \exists b \in G$ такой, что $ab = ba = 1$($b = a^{-1}$ – обратны к a)

Следствие 1. В группе G выполняются законы сокращения: $ab = ac \Leftrightarrow b = c, ba = ca \Leftrightarrow b = c, \forall a, b, c \in G$.

Доказательство.

$ab = ac \Leftrightarrow a^{-1}(ab) = a^{-1}(ac) \Leftrightarrow (a^{-1}a)b = (a^{-1}a)c \Leftrightarrow 1b = 1c \Leftrightarrow b = c.$

Следствие 2. a^{-1} определяется однозначно для любого $a \in G$.

Доказательство. Пусть b и c – обратные к a. Тогда $ab = 1$, $ca = 1$, откуда $c = c1 = c(ab) = (ca)b = 1b = b$.

Следствие 3. Если $ab = 1$, то $b = a^{-1}$.

Доказательство.

Пусть $ab = 1$. Тогда $a^{-1}(ab) = a^{-1}1 = a^{-1}$, т. е. $(a^{-1}a)b = = 1b = a^{-1}$.

Определение. Если в группе G выполняется закон коммутативности, т. е. $\forall a, b \in G \ \ ab = ba$, то G называется коммутативной, но чаще абелевой группой.

Операцию в абелевой группе обычно записывают аддитивно. Для аддитивной записи аксиомы группы будут выглядеть следующим образом:

1)$(a + b) + c = a + (b + c) \ \ \forall a, b, c \in G$;

2) $a + 0 = 0 + a = a \ \forall a \in G$;

3)$\forall a \in G \ \exists \ b \in G$ такой, что $a + b = b + a = 0$ ($b = -a$ – противоположный элемент к a);

Для абелевой группы – аксиома коммутативности:

4) $a + b = b + a$.

Пример.

1. $\mathbb{N} = \{1,2, \dots\}$, операция – обычное сложение чисел;

1) замкнутость, $\forall a, b \in \mathbb{N}, a + b \in \mathbb{N}$ −верно;

2) $(a + b) + c = a + (b + c)$;

3) $a + 0 = a \ \forall a$, но $0 \notin \mathbb{N}$;

4) $a + b = b + a$.

Таким образом, $\mathbb{N}$ – коммутативная полугруппа без единицы, относительно обычного сложения.

2. $\mathbb{N} = \{1,2, \dots\}$, операция – обычное умножение чисел:

1) $\forall a, b \in \mathbb{N}, ab \in \mathbb{N}$ −верно;

2) $(ab)c = a(bc)$;

3) $1a = a1 \ \forall a \Rightarrow 1 -$ единичный элемент;

4) $2 \cdot \frac{1}{2} = 1$, но $\frac{1}{2} \notin \mathbb{N}$.

Таким образом, $\mathbb{N}$ – коммутативный моноид относительно обычного умножения.

3. $\mathbb{Z}$, операция – обычное сложение чисел:

1) $(a + b) + c = a + (b + c)$

2) $a + 0 = 0 + a = a \ \forall a \in \mathbb{Z}$.

3) $\exists b \in \mathbb{Z}$ такой, что $a + b = b + a = 0 \ (b = -a)$.

$\mathbb{Z}$ −абелева группа относительно обычного сложения.

4. $\mathbb{Q} -$ абелева группа относительно обычного сложения

5. $\mathbb{R} -$ абелева группа относительно обычного сложения

6. $\mathbb{C} -$ абелева группа относительно обычного сложения.

7. $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ – коммутативный моноид относительно умножения чисел, но не группа:

1) $ab \in \mathbb{Z}\backslash\{0\}$ при $a, b \in \mathbb{Z}\backslash\{0\}$;

2) ассоциативность есть;

3) коммутативность есть;

4) $1a = a1 = a \ \ \forall a \in \mathbb{Z}^*$;

5) $2^{-1} = \frac{1}{2} \notin \mathbb{Z}^*$.

8. $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ относительно умножения – абелева группа:

1) $ab \in \ \mathbb{Q}\backslash\{0\}$, при $a, b \in \ \mathbb{Q}\backslash\{0\}$;

2) ассоциативность есть;

3) коммутативность есть;

4) $1a = a1 = a \ \ \forall a \in \mathbb{Z}^*$;

5) $\left(\frac{p}{q}\right)^{-1} = \frac{q}{p} \in \mathbb{Q}^*$, при $\frac{p}{q} \in \mathbb{Q}^*$.

9. $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ – абелева группа относительно умножения.

10. $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ – абелева группа относительно умножения.

Рассмотренные выше примеры – числовые группы и полугруппы.

11. $G = GL(n, \mathbb{R})$ –множество всех невырожденных квадратных вещественных матриц -го порядка.

1)$A, B \in G \Rightarrow AB \in G$ ($|A| \neq 0, |B| \neq 0 \Rightarrow |AB| = |A||B| \neq 0 \ \Rightarrow AB \in G$), т. е. G замкнуто относительно умножения матриц;

2) $(AB)C = A(BC) \ \forall A, B, C \in G$;

3)$EA = AE = A$, где $E = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$

4) Если $A \in G$, то $\exists \ A^{-1}: AA^{-1} = A^{-1}A = E$.

Заметим, что свойства 2–4 известны из линейной алгебры.

G называется общей линейной группой над $\mathbb{R}$.

$AB \neq BA$ в общем случае при $n \geq 2$, т. е. $GL(n, \mathbb{R})$. Группа не является абелевой.

12. $G = GL(n, \mathbb{Q})$ – общая линейная группа над $\mathbb{Q}$.

13. $G = GL(n, \mathbb{C})$ – общая линейная группа над $\mathbb{C}$.

Определение. Пусть G – группа. Тогда ее подмножество $H \neq \emptyset$ называется *подгруппой*, если:

1. H замкнуто относительно операции произведения: $\forall x, y \in H \; xy \in H$;
2. H замкнуто относительно операции взятия обратного элемента: $\forall x \in H, x^{-1} \in H$.

То, что H – подгруппа, обозначается как $H \leq G$.

Следствие 1. Единица группы всегда лежит в любой ее подгруппе.

Доказательство. Пусть $H \leq G$. Тогда $x \in H \Rightarrow x^{-1} \in H$, $xx^{-1} \in H \Rightarrow 1 \in H$,

Что и требовалось доказать.

Следствие 2.

Если G – конечная группа, то второе условие в определении подгруппы можно опустить.

Доказательство. Пусть $|G| < \infty$, H замкнуто относительно умножения в группе G, $|H| = s$, $x \in H$.

Так как $|H| < \infty$, то существуют натуральные числа s, t, где $t > s$ такие, что $x^t = x^s$. Тогда $x^{t-s} = 1$ и $x^{-1} = x^{t-s-1} \in H$, т. к. $t - s - 1 \geq 0$.

Следствие 3. Из определения подгруппы следует, что любая подгруппа является группой относительно операции в исходной группе.

Тривиальные примеры подгрупп группы G:

1) $\{1\}$ – единичная подгруппа;

2) сама группа G является собственной подгруппой.

Если H – подгруппа в группе G, то пишут $H \leq G$.

Определение. Подгруппа H группы G называется *собственной подгруппой* группы G, если H не совпадает с группой G.

Определение. Пусть G – группа, X – непустое подмножество в G. Тогда говорят, что группа G *порождается множеством* X, если любой элемент $g \in G, g \neq 1$ можно представить в виде произведения элементов из X с показателями ± 1:

$g = x_1^{\delta_1} \cdot \ldots \cdot x_k^{\delta_k}$, где $\forall i \ x_i \in X, \varepsilon_i = \pm 1$.

X называется *системой образующих (порождающих)* группы G. Если X конечно, то группу G называют *конечнопорожденной* независимо от конечности X и пишут $G =< X >$.

Определение. Пусть G – группа, $X \subseteq G, X \neq \emptyset$. *Подгруппой группы G, порожденной множеством X,* называется наименьшая подгруппа в G, содержащая X.

Утверждение. Подгруппа группы G, порожденная множеством X, состоит из всевозможных произведений вида $x_1^{\delta_1} \cdot \ldots \cdot x_k^{\delta_k}$, где $\forall i\ x_i \in X, \varepsilon_i = \pm 1$.

Доказательство очевидно.

Упражнения для самостоятельной подготовки

1. Какие из указанных числовых множеств с операциями являются группами:

   а) A – относительно обычной операции сложения, где $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$.

   б) A – относительно обычной операции умножения, где $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$.

   в) $A^* = A\{0\}$ – относительно обычного умножения чисел, где $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$.

   г) $n\mathbb{Z} = \{n\mathbb{Z} | z \in \mathbb{Z}\}$ – относительно обычного сложения чисел.

   д) множество всех комплексных корней фиксированной степени n из 1 – относительно умножения.

   е) множество комплексных корней всех степеней из 1 относительно умножения.

   2. Доказать, что если группа имеет конечную систему порождающих, то из любой системы порождаю-

щих можно выбрать конечную подсистему, порождающую всю группу.

§ 5. Циклические группы

Определение. *Порядок* $|a|$ элемента a в группе G – это наименьшее натуральное число n со свойством $a^n = 1$. Если $a^n \neq 1 \; \forall \, n \in \mathbb{N}$, то a называется элементом бесконечного порядка.

Теорема 1. Пусть $|a| = n$. Тогда

1) $a^m = 1 \Leftrightarrow n|m$;

2) $\forall \, m \in \mathbb{Z} \;\; a^m = a^r$, где r – остаток от деления m на n.

Доказательство. Докажем достаточность первого утверждения 1. $n|m \Rightarrow m = nk$ для некоторого целого k. Тогда $a^m = (\, a^m)^k = 1^k = 1$.

Докажем теперь вторую часть теоремы

Пусть $m = nq + r$, где r– остаток от деления m на n. Тогда $a^m = a^{nq} \cdot a^r = 1 \cdot a^r = a^r$, и теорема доказана.

Докажем, наконец, необходимость утверждения 1.

Пусть $a^m = 1$. По пункту 2: $a^m = a^r$, где $0 \leq r \leq n - 1$. Имеем $a^r = 1$, Отсюда в силу минимальности n имеем $r = 0$. Теорема доказана.

Определение. Группа G называется *циклической*, если в G найдется элемент a такой, что любой элемент из G является целой

степенью элемента a. G обозначается в этом случае как $< a >$, элемент a называется порождающим элементом группы G.

Теорема 2. Пусть $G =< a >$ и G конечная группа порядка n. Тогда

1) $G = \{1, a, \dots, a^{n-1}\}$ и $|a| = n$;
2) $G =< a^k > \Leftrightarrow$ k взаимно просто с n;
3) любая подгруппа группы G циклична, причем для любого делителя m числа n существует ровно одна подгруппа G порядка m.

Доказательство. Заметим прежде всего, что утверждение 1-е следует из 2-го теоремы 1.

Докажем пункт 2 теоремы 2. Пусть k и n взаимно просты.

Тогда по известной теореме теории чисел существуют целые x, y такие, что $kx + ny = 1$. Тогда $a = a^{kx} \cdot a^{ny} = (a^k)^x$, т. е. a является целой степенью элемента a^k. Тогда $G =< a^k >$.

Предположим теперь, что k не взаимно просто с n, т. е. существует натуральное $d \geq 2$, делящее k и n. Предположим, что $a = (a^k)^x$ для некоторого целого x. Тогда $a = a^{kx}$ и $a^{kx-1} = 1$. Отсюда $kx - 1$ делится на n по теореме 1, т. е. $kx - 1 = nq$ для некоторого целого q и $1 = kx - nq$. Отсюда $d|1$. Противоречие, которое доказывает утверждение 2.

Докажем пункт 3. Пусть $H < G$, $|H| = m$. Тогда по теореме Лагранжа $m|n$. Очевидно, что $\left|a^{\frac{n}{m}}\right| = m$. Следовательно, $< a^{\frac{n}{m}} >$ – циклическая группа порядка m. Пусть $x \in G$, $|x| = k|m$, $x = a^l$.

Имеем $a^{lm} = 1$, откуда lm делится на n, т. е. l делится на $\frac{n}{m}$, $x \in < a^{\frac{n}{m}} >$, что доказывает единственность подгруппы порядка m в G. Теорема доказана.

Теорема 3. Все циклические подгруппы одного конечного порядка изоморфны. Бесконечная циклическая подгруппа изоморфна группе $\mathbb{Z}$ относительно обычного сложения.

Доказательство. Пусть $< a >$ и $< b >$ – две циклические подгруппы порядка n. Определим отображение $\varphi: < a > \to < b >$ следующим образом:

$\varphi(a^k) = b^k \; \forall k \in \mathbb{Z}$.

Это определение корректно, т.к. если $a^k = a^m$, то $a^{k-m} = 1$, отсюда $k - m$ делится на n, и тогда $b^{k-m} = 1$ и $b^k = b^m$, т. е. $\varphi(a^k) = \varphi(a^m)$.

φ гомоморфно, т. к. $\varphi(a^k \cdot a^m) = \varphi(a^{k+m}) = b^{k+m} =$

$= \varphi(a^k)\varphi(a^m)$.

Инъективность φ также очевидна: $\varphi(a^k) = \varphi(a^m) \Rightarrow b^k =$ $= b^m \Rightarrow k - m$ делится на $n \Rightarrow a^{k-m} = 1 \Rightarrow a^k = a^m$.

Сюръективность φ очевидна. Следовательно, φ – изоморфизм $< a >$ на $< b >$. Теорема доказана для конечного случая. Вторая часть теоремы доказывается аналогично.

Пример. Пусть $G =< a >, |G| = 20$. Изобразим схематично все подгруппы группы G. Сначала составим диаграмму Хассе

множества $X = \{1, 2, 3, 5, 10, 20\}$ всех делителей 20 относительно отношения делимости (рис. 17):

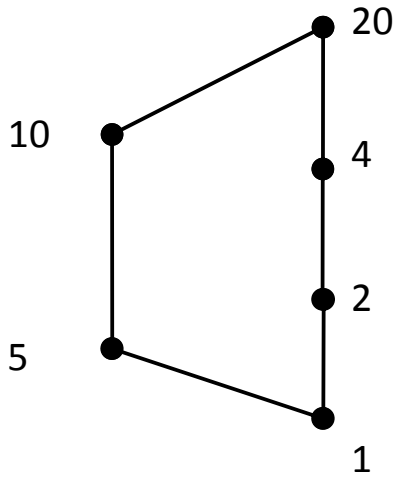

Рис. 17

Затем в соответствии с пунктом 3 теоремы 2 строим схему подгруппы G (рис. 18):

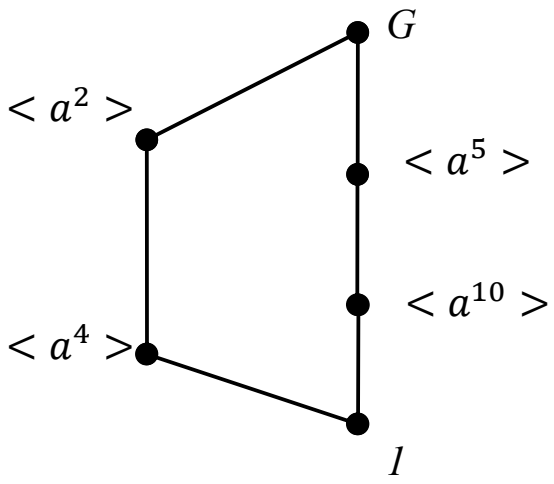

Рис. 16

Упражнения для самостоятельной подготовки

Составить схему подгруппы в циклической группе $< a >$ порядка 36.

§ 6. Группы подстановок

Определение. *Подстановкой* на конечном множестве X называется любое биективное преобразование этого множества, то есть взаимно однозначное отображение X на себя.

Множество всех подстановок на X обозначим S_X.

В теории групп подстановок есть два способа записи действия подстановки π на элемент $x \in X$: $\pi(x)$ или $(x)\pi$. В данной главе используем второй способ. Вместо $(x)\pi$ иногда пишем $x(\pi)$ или $x\pi$.

Определение. Произведение $\alpha\beta$ подстановок α и β из S_X определяется формулой: $\forall x \in X \ x(\alpha\beta) = (x\alpha)\beta$, то есть на x сначала действует α, а потом на то, что получилось, действует β.

Определение. *Единичной (или тождественной) подстановкой* на X называется такая подстановка ε_X, которая любой элемент x из X оставляет на месте, то есть $\forall x \in X \ x(\varepsilon_X) = x$.

Теорема. S_X с бинарной операцией умножения подстановок, определенной выше, является группой.

Доказательство. Сначала проверим замкнутость S_X относительно рассматриваемого умножения подстановок. Достаточно доказать в силу конечности X, что если $\alpha, \beta \in S_X$, то $\alpha\beta$ – инъективно.

В самом деле, пусть $x(\alpha\beta) = y(\alpha\beta)$. Тогда $(x\alpha)\beta = (y\alpha)\beta$, Отсюда $x\alpha = y\alpha$ в силу инъективности β и, наконец, $x = y$, так как $\alpha -$ инъективно.

Докажем ассоциативность умножения подстановок. Пусть $\alpha, \beta, \gamma \in S_X$, $x \in X$.

Тогда $x((\alpha\beta)\gamma) = \big(x(\alpha\beta)\big)\gamma = \big((x\alpha)\beta\big)\gamma = (x\alpha)(\beta\gamma) =$

$= x(\alpha(\beta\gamma))$. Отсюда в силу произвольности x $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Далее, $\forall x \in X$ $x(\alpha\varepsilon_X) = (x\alpha)\varepsilon_X = (x)\alpha$ и $x(\varepsilon_X\alpha) =$

$\big(x(\varepsilon_X)\big)(\alpha) = (x)\alpha$. Отсюда $\alpha\varepsilon_X = \varepsilon_X\alpha = \alpha$.

И, наконец, если $\alpha \in S_X$, то определено преобразование β множества X следующим образом:

$$x\beta = y \Leftrightarrow y\alpha = x.$$

Так как $y_1\alpha = y_2\alpha$ влечет $y_1 = y_2$ в силу инъективности α, то данное определение β корректно. Далее, $x_1\beta = x_2\beta = z$ влечет $(z)\alpha = x_1$, $(z)\alpha = x_2$, Отсюда в силу однозначности α $x_1 = x_2$. Значит $\beta \in S_X$. Очевидно, что $\forall x \in X$ $x(\alpha\beta) = x$ и $x(\beta\alpha) = x$. Стало быть, $\alpha\beta = \beta\alpha = \varepsilon_X$.

Итак, мы проверили все три групповые аксиомы для произведения подстановок.

Теорема доказана.

Если $X = \{1,2, \dots, n\}$, то S_X обозначается как S_n и называется *симметрической группой* степени n.

Далее, если $\pi \in S_n$, то удобно π записывать в следующем виде: $\begin{pmatrix} 1 & 2 & \dots & n \\ (1)\pi & (2)\pi & \dots & (n)\pi \end{pmatrix}$. Подстановки в таком виде удобно перемножать.

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} =$$

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

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

При записи подстановки π из S_n необязательно числа в верхней строке записывать в порядке возрастания: главное, чтобы под каждым элементом верхней строки внизу стоял его образ под действием π. И еще: столбцы в данной подстановке π с одинаковыми элементами вверху и внизу можно опускать.

Например, если $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 5 & 4 \end{pmatrix} \in S_6$,

то $\pi = \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 1 & 6 & 4 \end{pmatrix}$, так как $3\pi = 3$ и $5\pi = 5$.

Разложение подстановки в произведение независимых циклов

Определение. *Циклом длины* k, где $k \geq 2$, называется подстановка вида $\begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}$, которая обозначается $(i_1, \dots i_k)$.

Определение. Цикл (ij) длины 2 называется *транспозицией,* а цикл (ijk) длины 3 называется *тройным циклом*.

Определение. Два цикла называются *независимыми*, если множества элементов, передвигаемых этими циклами, не пересекаются.

Теорема 1. Любая подстановка π из S_n, отличная от ε_X, представима в виде произведения попарно независимых циклов, причем это представление однозначно с точностью до перестановки этих циклов.

Доказательство. Доказательство существования такого разложения для π проведем индукцией по n. Так как $\pi \neq \varepsilon_X$, то существует число $m \leq n$ такое, что $m\pi \neq m$.

Ввиду конечности множества, на котором действует π, существует такое наименьшее $l \geq 2$, что $m\pi^l = m\pi^k$ для некоторого целого неотрицательного $k < l$.

Если $k \geq 1$, то $m\pi^{l-k} = m = m\pi^0$, что противоречит минимальности l. Стало быть, элементы $m, m\pi, \dots, m\pi^{l-1}$ попарно различны, а $m\pi^l = m$, то есть $\alpha = \begin{pmatrix} m & m\pi & \dots & m\pi^{l-1} \\ m\pi & m\pi^2 & \dots & m \end{pmatrix}$ –

цикл $(m, m\pi, \dots, m\pi^{l-1})$ длины l. По предположению индукции π как подстановка на множестве $\{1, \dots, n\} \backslash \{m, m\pi, m\pi^{l-1}\}$ представима в виде произведения попарно независимых циклов $\alpha_1, \alpha_2 \dots, \alpha_s$. Тогда $\pi = \alpha\alpha_1\alpha_2 \dots \alpha_s$ – требуемое представление для π как подстановки из S_n. Теорема доказана.

Следствие. Любая подстановка из S_n представляется в виде произведения транспозиций.

Доказательство. Заметим, что цикл $\tau = (\alpha_1, \alpha_2 \dots, \alpha_k) = = (\alpha_1\alpha_2)(\alpha_1\alpha_3) \dots (\alpha_1\alpha_k)$, так как под действием правой части $\alpha_1 \to \alpha_2, \alpha_2 \to \alpha_1 \to \alpha_3$, $\alpha_3 \to \alpha_1 \to \alpha_4, \dots, \alpha_k \to \alpha_1$. Теперь из теоремы 1 следует требуемое.

Пример. Разложить в произведение независимых циклов подстановку

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 7 & 2 & 5 \end{pmatrix} \in S_8.$$

Считаем: $1\pi = 3, 3\pi = 4, 4\pi = 1$. Получили цикл (134) длины 3.

Далее берем любой элемент, отличный от $1, 3, 4$, например 2.

Считаем аналогично: $2\pi = 6, 6\pi = 7, 7\pi = 2$. Получили еще один цикл (267).

Теперь берем любой элемент, не содержащийся в построенных иклах, например 5. Имеем: $5\pi = 8, 8\pi = 5$, то есть получили цикл длины 2.

Ответ: $\pi = (134)(267)(58)$.

Четные и нечетные подстановки

Лемма 1. Если транспозицию (ij) умножить слева на подстановку $\pi = \begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & \alpha_i & \dots & \alpha_j & \dots \end{pmatrix}$, то α_i и α_j поменяются местами, в остальном π не изменится.

Доказательство. При умножении $\tau = (ij)$ на π произойдет следующее: $i \xrightarrow{\tau} j \xrightarrow{\pi} \alpha_j$, $j \xrightarrow{\tau} i \xrightarrow{\pi} \alpha_i$, а если s не принадлежит $\{i, j\}$, то $s \xrightarrow{\tau} s \xrightarrow{\pi} \alpha_s$, то есть образ s под действием $\tau\pi$ равен образу s под действием π. Лемма доказана.

Определение. *Перестановкой n-го порядка* называется любая последовательность без повторений натуральных чисел от 1 до n.

Определение. Два числа α и β в перестановке образуют *инверсию,* если $\alpha > \beta$ и α стоит в данной перестановке раньше β.

Определение. Перестановка называется *четной*, если в ней четное число инверсий, в противном случае – *нечетной*.

Лемма 2. При перестановке двух чисел в перестановке ее четность меняется на противоположную.

Доказательство. Пусть сначала меняются местами рядом стоящие α и β. Тогда число инверсий либо уменьшается на 1 (при $\alpha > \beta$), либо увеличивается на 1 (при $\alpha < \beta$), то есть в любом случае четность перестановки меняется.

Пусть теперь между α и β находятся k чисел $\alpha_1, \alpha_2 \dots, \alpha_k$. Поменять местами α *и* β можно следующим образом: β менять

местами с числами, стоящими слева, до того момента, когда он не встанет на место α, причем α будет находиться справа от него. Затем α меняем с $\alpha_1, \alpha_2 \dots, \alpha_k$, пока α не встанет на старое место β. В результате получим подстановку, в которой лишь α и β поменялись местами по сравнению с исходной подстановкой. Однако результирующая подстановка получилась в результате $k + 1 + k = 2k + 1$ перемен местами соседних чисел, т. е. $2k + 1$ раз менялась четность подстановки. Следовательно, четность результирующей подстановки отличается от четности исходной. Лемма доказана.

Определение. Подстановка $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$ называется *четной*, если перестановка $\alpha_1, \alpha_2 \dots, \alpha_n$ четная, в противном случае π – *нечетная*.

Теорема 2. $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$ четная ⇔ π можно представить в виде произведения четного числа транспозиций.

Доказательство. Заметим прежде всего то, что любая транспозиция – нечетная подстановка, и по леммам 1, 2 при умножении подстановки на транспозицию слева ее четность меняется. Следовательно, четные подстановки – это те подстановки, которые могут быть представлены в виде произведения четного числа транспозиций. Теорема доказана.

Теорема 3. Число нечетных подстановок в S_n равно $\frac{1}{2}n!$ и все четные подстановки образуют подгруппу в S_n.

Доказательство. Пусть M и N – множество всех четных и нечетных подстановок в S_n соответственно. Определим отображение $\varphi: M \to N$: $\forall \pi \in M\ \varphi(\pi) = (12)\pi$.

Ясно, что φ – инъекция M в N. Пусть π'– любая нечетная подстановка. Тогда $(12)\pi'$ – четная подстановка и $\pi' = = \varphi((12)\pi')$, Отсюда φ – сюръекция M на N, а значит, и биекция M и N (инъективность была отмечена выше). Следовательно, $|M| = |N|$.

То, что M – подгруппа в S_n, следует из того, что единичная подстановка четна, и из теоремы 2.

Подгруппа всех четных подстановок в S_n обозначается A_n и называется *знакопеременной группой n-й степени*.

В виду теоремы 3 $|A_n| = \frac{1}{2}n!$

Теорема 4. Любая неединичная подстановка из A_n представима в виде произведения тройных циклов.

Доказательство. Заметим, что $(ij)(ik) = ijk$ и $(ij)(kl) = = (ilj)(jkl)$ (это легко проверить в качестве упражнения). Теперь справедливость теоремы 4 следует из теоремы 2.

Пример. Представить четную подстановку

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 5 & 6 & 8 & 1 & 7 \end{pmatrix}$ в виде произведения транспозиций и в виде произведения тройных циклов.

Сначала представим π в виде произведения попарно независимых циклов: $\pi = (145687)(23)$, затем, используя формулу в доказательстве следствия к теореме 1, получим $(145687) = (14)(15)(16)(18)(17)$ и $\pi = (14)(15)(16)(18)(17)(23)$. Далее, используя формулы в доказательстве теоремы 4, получим $(14)(15) = (145)$, $(16)(18) = (168)$, $(17)(23) = (137)(723)$ и в результате имеем $\pi = (145)(168)(137)(237)$.

Упражнения для самостоятельной подготовки

1. Перемножить подстановки в указанном и обратном порядках:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix}$

2. Записать в виде произведения независимых циклов подстановки:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 7 & 3 & 6 & 2 \end{pmatrix}$

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ 2 & 1 & 4 & 3 & \dots & 2n & 2n-1 \end{pmatrix}$

в) $\begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \cdots & 2n \\ n+1 & n+2 & 4 & \dots & 2n & 1 & 2 & \cdots & n \end{pmatrix}$

3. Записать в виде таблицы подстановки:

а) $(1\ 3\ 6)(2\ 4\ 7)(5)$

б) $(1\ 6\ 5\ 4\ 2\ 3\ 7)$

в) $(1\ 3\ 5\ \ldots 2n-1)(2\ 4\ 6\ \ldots 2n)$

4. Перемножить подстановки:

а) $((1\ 3\ 5\ )(2\ 4\ 6\ 7)) \times ((1\ 4\ 7)(2\ 3\ 5\ 6))$

б) $((1\ 3)(5\ 7)(2\ 4\ 6)) \times ((1\ 3\ 5)(2\ 4)\ (6\ 7))$

5. Определить четность подстановок:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 4 & 7 & 2 & 1 & 3 \end{pmatrix}$

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 1 & 6 & 4 & 8 & 7 \end{pmatrix}$

в) $\begin{pmatrix} 3 & 5 & 6 & 4 & 2 & 1 & 7 \\ 2 & 4 & 1 & 7 & 6 & 5 & 3 \end{pmatrix}$

6. Определить четность подстановок:

а) $(1\ 2\ 3\ \ldots k)$

б) $(i_1\ i_2\ i_3\ i_4\ \ldots\ i_k)$

в) $(1\ 4\ 7\ 3)(6\ 7\ 2\ 4\ 8)(3\ 2)$

7. Доказать, что всякая перестановка $\sigma \in S_n$ может быть представлена как произведение транспозиций вида

а) $(12), (13), \ldots, (1, n)$

б) $(12), (23), \ldots, (n-1, n)$

8. Доказать, что всякая перестановка $\sigma \in S_n$ может быть представлена как произведение нескольких сомножителей, равных циклам (12) и $(1\ 2\ 3\ \ldots n)$.

9. Доказать, что всякая четная подстановка может быть представлена как произведение циклов вида $(123), (124), \dots, (12n)$.

§ 7. Матричные группы

Определение. Пусть F – $\mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$. Тогда *полной линейной группой* $GL(n, F)$ степени n над F называется множество всевозможных невырожденных матриц порядка n с элементами из F, с бинарной операцией умножения матриц.

То, что $GL(n, F)$ – группа, доказано в § 4.

Определение. *Специальная линейная группа* $SL(n, F)$ степени n над F – множество всех матриц порядка n с элементами из F, определитель которых равен 1.

Определение. *Треугольная группа*

$$T(n, F) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix} \mid \forall\, i \in \{1, \dots, n\}\ a_{ii} \neq 0 \right\}$$

степени n над F состоит из всевозможных невырожденных верхнетреугольных матриц.

Определение. *Унитриугольная группа* $UT(n,F) = \left\{ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & 1 & & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \mid \forall\, i,j \in \{1,\dots,n\}\, a_{ij} \in F \right\}$ степени n над F состоит из всевозможных верхнетреугольных матриц, все диагональные элементы которых равны 1.

Определение. Ортогональная группа – множество всех матриц A из $GL(n,F)$ с условием $A^tA = E$.

Доказательство того, что все указанные выше множества матриц являются группами, предоставляются читателям.

Упражнения для самостоятельной подготовки

1. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

а) множество симметрических (кососимметрических) матриц относительно сложения;

б) множество симметрических (кососимметрических) матриц относительно умножения;

в) множество невырожденных матриц относительно сложения;

г) множество невырожденных матриц относительно умножения;

д) множество матриц с фиксированным определителем d относительно умножения;

е) множество диагональных матриц относительно сложения;

ж) множество диагональных матриц относительно умножения;

з) множество диагональных матриц, все элементы диагоналей которых отличны от 0, относительно умножения;

и) множество верхних треугольных матриц относительно умножения;

к) множество всех ортогональных матриц относительно умножения;

л) множество верхних нильтреугольных матриц, т. е. матриц вида $\begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & a_{n-1,n} \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ относительно умножения;

м) множество верхних нильтреугольных матриц относительно сложения;

н) множество верхних унитреугольных матриц относительно умножения.

2. Показать, что множество $O_n(\mathbb{Z})$ всех целочисленных ортогональных матриц порядка n образует группу относительно умножения. Найти порядок этой группы.

§ 8. Смежные классы

Определение. Пусть $H \leq G, x \in G$. Левым (правым) смежным классом группы G по H с представителем x называется множество $Hx = \{hx | h \in H\}$ ($xH = \{xh | h \in H\}$).

Свойства левых и правых смежных классов.

Теорема 1. Пусть $H \leq G$. Тогда верны следующие утверждения:

1. $\forall x \ \ x \in Hx$.

2. y$\in Hx \Rightarrow Hy = Hx$.

3. Разные левые смежные классы не пересекаются: $Hx \cap Hy = \emptyset$ при $Hx \neq Hy$.

Доказательство. Утверждение 1 следует из того, что $1 \in H$.

Докажем утверждение 2: $y \in Hx \Rightarrow \exists h \in H: y = hx,$

$g \in Hy \Rightarrow \exists h' \in H: g = h'y = h'(hx) = (h'h)x \in Hx \Rightarrow$ $Hy \subseteq Hx$.

$y = hx \Rightarrow h^{-1}y = h^{-1}hx \Rightarrow h^{-1}y = x \Rightarrow x \in Hy$ и по доказанному выше $Hx \subseteq Hy$.

Значит, $Hx = Hy$. Утверждение 2 доказано. ■

Пусть $s \in Hx \cap Hy$. Тогда $s \in Hx$ и $s \in Hy$, и по утверждению 2 $Hs = Hx$ и $Hs = Hy$. Поэтому $Hx = Hy$. Итак, если два левых смежных класса пересекаются, то они совпадают, что эквивалентно утверждению 3.

Из теоремы следует, что различные левые смежные классы G по H образуют разбиение группы G. Аналогично для правых смежных классов. ■

Теорема 2. Если $H \leq G$ и $|H| < \infty$, то любые ее левые смежные классы имеют одинаковый порядок, равный порядку H: $|Hx| = |H|$.

Доказательство. Рассмотрим отображение $\varphi: Hx \to H$ такое, что $\varphi(hx) = h$. Очевидно, что φ – биекция. Поэтому $|Hx| = |H|$. Утверждение доказано. ■

Теорема 3. Если $H \leq G$ и $|H| < \infty$, то$\forall x, y \in G\ Hx = yH$.

Доказательство легко понять: отображение $\varphi: Hx \to yH$, такое, что $\varphi(Hx) = yH$ – биекция. Поэтому $|Hx| = |yH|$.

Определение. Пусть $H \leq G, |G| < \infty$. Тогда её индексом $|G: H|$ (индексом группы H в G) называется число левых смежных классов.

Теорема (Лагранжа).

Если $|G| < \infty$ и $H \leq G$, то $|G| = |H| \cdot |G: H|$.

Доказательство. Из предыдущей теоремы следует, что $G = Hx_1 \cup Hx_2 \cup \ldots \cup Hx_s$. А из предыдущего утверждения – $|H| = |Hx_2| = \cdots = |Hx_s|$. Поэтому $|G| = |H|s$, т. е. $|G| = |H| \times$ $\times |G: H|$.■

Замечание. Ввиду теоремы 3 при $|H| < \infty, H \leq G$ $|G: H|$ – это также число и правых смежных классов G по H.

Примеры разложения группы на смежные классы.

Пример 1. Пусть $G = S_4$, $H = <(132)>$. Найти $|H|$, $|G:H|$ и разложить G в виде объединения попарно непересекающихся левых смежных классов по H.

Решение. $(132)^2 = (123)$, $(132)^3 = (132)(123) = \varepsilon$ – тождественная подстановка. Следовательно, $|H| = |132| = 3$, а $|G:H| = \frac{|S_4|}{3} = \frac{24}{3} = 8$, т. е. имеется 8 различных левых смежных классов G по H. Сначала в строку выписываем элементы H: $\varepsilon\ (132)\ (123)$.

Затем берем любую подстановку π_2 из S_4, не принадлежащую H, и элементы класса $H\pi_2$ вписываем под элементами из H. Получаем вторую строку:

$$\varepsilon\pi_2\ (132)\pi_2\ (123)\pi_2.$$

Затем берем любую подстановку π_3, не лежащую в двух уже написанных строках, и элементы класса $H\pi_3$ вписываем под второй строкой. Продолжая процесс, мы выпишем все 8 левых классов G по H (табл. 10).

Таблица 10

$\pi_1 = \varepsilon$	(132)	(123)
$\pi_2 = (12)$	(13)	(23)
$\pi_3 = (14)$	(1324)	(1234)
$\pi_4 = (24)$	(1342)	(1423)

Окончание табл. 10

$\pi_5 = (34)$	(1423)	(1243)
$\pi_6 = (124)$	(134)	$(14)(23)$
$\pi_7 = (234)$	(142)	$(13)(24)$
$\pi_8 = (243)$	$(12)(34)$	(143)

Следующий пример относится к так называемым бинарным группам.

Определение. *Бинарной группой* E_{2^n} называется множество всех n-ок $\bar{a} = (\alpha_1, \dots, \alpha_n)$, где все $\alpha_i \in \{0,1\}$, причем $(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$ и сложение в $\{0,1\}$ определяются таблицей Кэли (табл. 11):

Таблица 11

+	0	1
0	0	1
1	1	0

(такое сложение называется сложением по модулю 2).

Нетрудно проверить, что относительно данного сложения n-ок E_{2^n} является абелевой группой порядка 2^n.

Пример 2. Найти разложение E_{2^5} по подгруппе $H = <\bar{a} = (1,0,0,0,1),\ \bar{b} = (0,1,1,0,1)>$. Поскольку $\bar{a} + \bar{a} = \bar{0}$, $\bar{b} + \bar{b} = \bar{0}$, то $H = <\bar{0}, \bar{a}, \bar{b}, \bar{a} + \bar{b}>$. В частности, $|H| = 4$, $|G:H| = 8$.

Выпишем элементы H в строку (запятые между нулями и единицами в n-ке будем опускать) и далее будем поступать, как в примере 1.

(0 0 0 0 0) (1 0 0 0 1) (0 1 1 0 1) (1 1 1 0 0)

(0 0 0 0 1) (1 0 0 0 0) (0 1 1 0 0) (1 1 1 0 1)

(0 0 0 1 0) (1 0 0 1 1) (0 1 1 1 1) (1 1 1 1 0)

(0 0 1 0 0) (1 0 1 0 1) (0 1 0 0 1) (1 1 0 0 0)

(0 1 0 0 0) (1 1 0 0 1) (0 0 1 0 1) (1 0 1 0 0)

(0 0 0 1 1) (1 0 0 1 0) (0 1 1 1 0) (1 1 1 1 1)

(0 1 0 1 0) (1 1 0 1 1) (0 0 1 1 1) (1 0 1 1 0)

(0 0 1 1 0) (1 0 1 1 1) (0 1 0 1 1) (1 1 0 1 0)

Заметим, что в роли представителей смежных классов мы старались брать n-ки с наименьшим числом единиц, не выписанных в ранее построенных строках.

Упражнения для самостоятельной подготовки

1. Доказать, что во всякой группе:

   а) пересечение любого набора подгрупп является подгруппой;

   б) объединение двух подгрупп является подгруппой тогда и только тогда, когда одна из этих подгрупп содержится в другой;

   в) если подгруппа C содержится в объединении подгрупп A и B, то либо $C \subseteq A$, либо $C \subseteq B$.

2. Доказать, что в группе S_n:

   а) порядок нечетной подстановки является четным числом;

   б) порядок любой подстановки является наименьшим общим кратным длин независимых циклов, входящих в ее разложения.

3. Существует ли бесконечная группа, все элементы которой имеют конечный порядок?

4. Найти все подгруппы в группах:

   а) S_3; б) A_4; в) S_4.

5. Пусть $H \leq K \leq G$, $|G| < \infty$, тогда $|G:H| = |G:K||K:H|$.

   Доказать, что если подгруппа H группы S_n содержит одно из множеств

   $\{(1,2),(1,3),\dots,(1,n)\}\{(1,2),(1,2,3\dots n)\}$, то $H = S_n$.

6. Пусть K – правый смежный класс группы G по подгруппе H. Доказать, что если $x, y, z \in K$, то $xy^{-1}z \in K$.

7. Пусть K – непустое подмножество в группе G, причем если $x, y, z \in K$, то $xy^{-1}z \in K$. Доказать, что K является правым смежным классом группы G по некоторой подгруппе H.

8. Разложить $G = S_4$ на правые смежные классы по $H =< (1324) >$;

9. Разложить E_{64} по подгруппе

   $H =< (100100), (111001), (001001) >$.

§ 9. Нормальные подгруппы. Фактор-группы

Определение. Подгруппа $H \leq G$ называется *нормальной (инвариантной)*, если $\forall x \in H, Hx = xH$. Обозначается подгруппа как $H \trianglelefteq G$. Если H – собственная нормальная подгруппа, то обозначение выглядит так: $H \triangleleft G$.

Утверждение. $H \trianglelefteq G \Leftrightarrow \forall x \in G, x^{-1}Hx = H$.

Доказательство.

$H \trianglelefteq G \Leftrightarrow \forall x \ \ Hx = xH \Leftrightarrow \forall x \in G$

Имеем $x^{-1}Hx = (x^{-1}x)H = 1 \cdot H = H$.

Для любой нормальной подгруппы группы G можно построить фактор-группу G/H – множество всех левых смежных классов $\{Hx\} = G/H$ с операцией $Hx \cdot Hy = H(xy)$. Докажем корректность этого определения.

Пусть $x_1 \in Hx$, $y_1 \in Hy$. Докажем, что $Hxy = Hx_1y_1$.

$x_1 = hx$, $y_1 = h'y$ для некоторых $h, h' \in H$.

Так как $H \trianglelefteq G$, то $xh' = h''x$ для некоторого $h'' \in H$.

Тогда $x_1y_1 = hxh'y = hh''xy \in Hxy$, откуда по теореме 1 (см. § 8) $Hx_1y_1 = Hxy$.

Корректность доказана.

Замкнутость данной операции очевидна: $HxHy = H(xy) \in G/H$.

Далее, $(HxHy)Hz = H(xy)Hz = H\big((xy)z\big) = H\big(x(yz)\big) =$ $= HxH(yz) = HxH(yz) = Hx(HyHz)$, т. е. данная операция ассоциативна.

Ясно, что $H \cdot 1$ – единица для данной операции. Действительно, $HxH1 = Hx1 = Hx$.

И, наконец, Hx^{-1}– обратный элемент. Действительно, $Hx \cdot Hx^{-1} = H = Hx^{-1}Hx$.

Часть информации о самой группе несет в себе G/H, то есть, зная H и G/H, можно получить информацию и о самой группе G.

Утверждение. Подгруппа индекса 2 произвольной группы G всегда нормальна в этой группе.

Доказательство. Пусть $x \in H$. Тогда ясно, что $xH = H = Hx$.

Пусть $x \notin H$. Тогда $xH = G\backslash H$ и $Hx = G\backslash H$, т. е. снова $Hx = xH$.

Примечание. Если брать подгруппу индекса не 2, а больше, то утверждение неверно в общем случае.

Упражнения для самостоятельной подготовки

1. Доказать, что подгруппа H группы G нормальна:

а) G – абелева группа, H – любая ее подгруппа;

б) $G = GL_n(n, \mathbb{R})$, H – подгруппа матриц с определителем, равным 1;

в) $G = S_n$, $H = A_n$;

г) $G = S_4$, $H = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$.

2. Найти все нормальные подгруппы, отличные от единичной и от всей группы в группах:

   а) S_3; а) A_4; в) S_4.

3. Доказать, что фактор-группа группы S_4 по нормальной подгруппе $\{\varepsilon, (12)(34), (13)(24), (14)(23)\}$ изоморфна группе S_3.

§ 10. Изоморфизмы и гомоморфизмы

Определение. Биекция f группы G на группу G' называется *изоморфизмом*, если $\forall x, y \in G\ f(xy) = f(x)f(y)$.

Следствие. Пусть $f: G \to G'$ – изоморфизм. Тогда

1) $f(1_G) = 1_{G'}$;

2) $\forall a \in G\ f(a^{-1}) = (f(a))^{-1}$.

Доказательство.

1) $f(a) = f(1_G \cdot a) = f(1_G) \cdot f(a) \Longrightarrow f(1_G) = 1_{G'}$. Первый пункт доказан.

2) $f(aa^{-1}) = f(1_G) = 1_{G'}$,

$f(aa^{-1}) = f(a^{-1}) \cdot f(a)^{-1}$.

Значит, $f(a^{-1})f(a)^{-1} = 1_{G'}$, откуда $f(a^{-1}) = (f(a))^{-1}$, и второй пункт следствия доказан.

Пример.

Рассмотрим биекцию f группы $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ на группу $G' = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\backslash\{0\}\right\}$, определенную формулой $f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Проверим, что f является изоморфизмом указанных групп.

$$f\big((a + bi)(c + di)\big) = f\big(\big(ac - bd + i(bc + ad)\big) =$$

$$= \begin{pmatrix} ac - bd & -bc - ad \\ bc + ad & ac - bd \end{pmatrix};$$

$$f(a+bi)f(c+di) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} =$$

$$= \begin{pmatrix} ac-bd & -bc-ad \\ bc+ad & ac-bd \end{pmatrix} = f\big((a+bi)(c+di)\big).$$

Итак, группа $\mathbb{C}^*$ изоморфна группе $G' = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2+b^2 > 0\right\}$.

Если в определении изоморфизма отказаться от биективности, то получим понятие гомоморфизма.

Определение. Отображение f группы G в G' называется *гомоморфизмом,* если $\forall x, y \in G\ f(xy) = f(x)f(y)$.

Следствие, рассмотренное выше, справедливо и для гомоморфизма.

Определение. *Ядро гомоморфизма* $f: G \to G'$ – это $\{x \in G \mid f(x) = 1\}$. Ядро гомоморфизма обозначается $\mathrm{Ker}\, f$.

Лемма. $\mathrm{Ker}\, f$ – нормальная подгруппа в G.

Доказательство. Пусть $f(g) = 1$. Тогда $\forall x \in G$ имеем

$f(x^{-1}gx) = f(x^{-1})f(g)f(x) = f(x^{-1})f(x) = 1,$ т. е. $\forall x \in G\ \ \forall g \in \mathrm{Ker}\, f\ \ x^{-1}gx \in \mathrm{Ker}\, \varphi$.

Отсюда следует, что $\mathrm{Ker}\, \varphi \trianglelefteq G$.

Основная теорема о гомоморфизмах групп. Пусть f – гомоморфизм G на группу G'. Тогда существует однозначно определенный гомоморфизм $\varphi: G/\mathrm{Ker}\, \varphi \to G'$ такой, что $\forall x \in G\ f(x) = \varphi(\varepsilon(x))$, где ε – канонический гомоморфизм G на $G/\mathrm{Ker}\, \varphi$: $\forall x \in G\ \varepsilon(x) = x\mathrm{Ker}\, \varphi$.

Следующая схема иллюстрирует эту теорему (рис. 19):

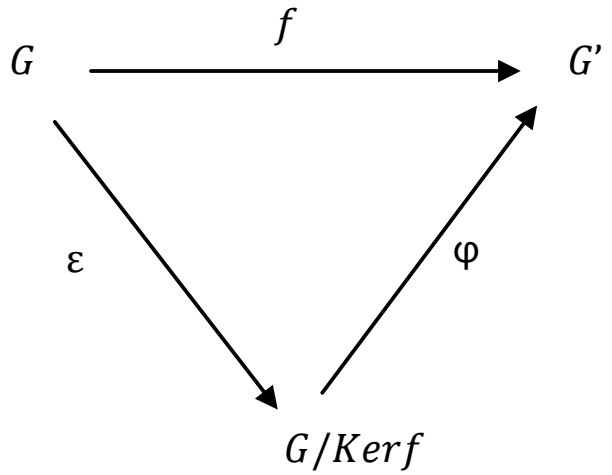

Рис. 19

Определение. Гомоморфизм G в себя называется *эндоморфизмом.*

Определение. Изоморфизм G в себя называется *автоморфизмом.*

Упражнения для самостоятельной подготовки

1. Найти все гомоморфизмы циклической группы $< a >$ порядка 20 в циклическую группу $< b >$ порядка 4.
2. Найти все эндоморфизмы группы $\mathbb{Q}$ относительно сложения.
3. Найти все автоморфизмы циклической группы порядка n.
4. Найти все автоморфизмы группы S_3.
5. Доказать, что группа порядка 6 либо коммутативна, либо изоморфна группе S_3.

§ 11. Кольца и поля

Определение. *Кольцо* R – множество с двумя замкнутыми бинарными операциями на нем – сложением и умножением, т. е. $\forall\, a, b \in R \;\; a + b \in R$, $ab \in R$, причем выполняются свойства:

1) $(a + b) + c = a(b + c)$;
2) $\exists 0 \in R\colon \forall a \in R \; a + 0 = a$ (нуль кольца);
3) $a + b = b + a$;
4) $\forall a \in R \; \exists b \in R\colon a + b = 0$ (b обозначается $-a$);
5) $(a + b)c = ac + bc$;
6) $a(b + c) = ab + ac$.

В кольце могут быть потребованы дополнительные аксиомы:

7) $(ab)c = a(bc)$ (кольцо ассоциативно);
8) $ab = ba$ (кольцо коммутативно);
9) $\exists 1 \in R\colon \forall a \in R \; a1 = 1a = a$ (существование единицы);
10) $\forall x \in R\backslash\{0\} \; \exists y \in R\colon xy = yx = 1$ ($y = x^{-1}$) (существование обратного).

Если кольцо удовлетворяет всем десяти свойствам, оно называется *полем*.

Если кольцо удовлетворяет всем свойствам, кроме коммутативности умножения, оно называется *телом.*

Замечание. Кольцо R, рассматриваемое только относительно операции сложения, называется аддитивной группой R.

Определение. Подмножество M кольца R называется *подкольцом*, если

1) $\forall x, y \in M\ x + y \in M$;

2) $\forall x, y \in M\ xy \in M$;

3) $\forall x \in M\ (-x) \in M$.

Следствия из аксиом поля:

1) $xy = xz \Rightarrow y = z$,

$yx = zx \Rightarrow y = z$, при $x \neq 0$;

2) $\exists!\, x^{-1}\ \forall x \neq 0$;

3) $\forall\ a, b \in R$ при $a \neq 0\ \ \exists!\, x\ \in R$, такой, что $ax = b$;

4) $a, b \neq 0 \Rightarrow ab \neq 0$.

Доказательство этих свойств предоставим читателю.

Определение. Пусть a, b в кольце R – делители нуля, если $a, b \neq 0$, но $ab = 0$.

Так что следствие четвертое говорит о том, что в поле нет делителей нуля.

Определение. Мультипликативная группа F^* поля F – это группа $F\backslash\{0\}$ относительно левого умножения.

Примеры.

1. $\mathbb{Z}$ – кольцо относительно обычных сложения и умножения (ассоциативно, коммутативно, с единицей, не является полем).
2. $\mathbb{Q} = \{\frac{p}{q}\}$ – поле ($(\frac{p}{q})^{-1} = \frac{q}{p},\ \frac{p}{q} \neq 0$).
3. $\mathbb{R}, \mathbb{C}$ – поля.

4. $F[x]$ – множество всех многочленов с коэффициентами из F – ассоциативное, коммутативное кольцо с единицей (F – произвольное поле).
5. $\mathbb{H}$ – тело кватернионов $\{a + bi + cj + dk | \, a, b, c, d \in \mathbb{R}\}$, i, j, k – мнимые единицы (табл. 12, рис. 20):

Таблица 12

	i	*j*	*k*
i	*-1*	*k*	*-j*
j	*-k*	*-1*	*i*
k	*j*	*-i*	*-1*

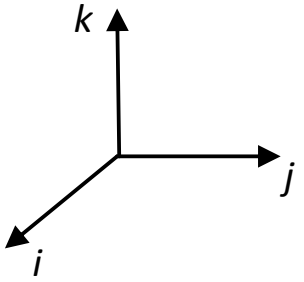

Рис. 20

$\mathbb{H}$ – тело относительно покомпонентной операции сложения кватернионов и относительно умножения кватернионов, индуцированного таблицей выше.

Пример.

$(3 + 2i + k)(j - 2k) = 3j - 6k + 2(ij) \; - 4(ik) + (kj) - 2(kk) =$

$= 3j - 6k + 2k + 4j - i + 2 = 2 - i + 7j - 4k.$

Можно доказать, что $(a + bi + cj + dk)^{-1} =$

$= \frac{1}{\sqrt{a^2+b^2+c^2+d^2}}(a - bi - cj - dk)$ при $a^2 + b^2 + c^2 + d^2 > 0$.

§ 12. Линейное пространство над произвольным полем F

Определение. Линейное пространство над полем F – это множество L с замкнутой бинарной операцией $a + b \in L\ \forall a, b$ и операцией умножения λa любого элемента $\lambda \in F$ на любой элемент a из L, причем для этих операций выполняются те же 8 аксиом, которые были для линейного пространства над $\mathbb{R}$ или $\mathbb{C}$ в курсе линейной алгебры. Элементы из F называются скалярами, элементы из L – векторами. Справедливы и следствия из аксиом:

1) $a + x = b + x \Rightarrow a = b$;
2) $0a = \bar{0}\ \forall a \in L$;
3) $\lambda\bar{0} = \bar{0}\ \forall \lambda \in L$;
4) $\lambda x = \bar{0} \Rightarrow \lambda = 0$ или $x = \bar{0}$.

Пример. $F^n = \{\bar{x} = (x_1, \dots, x_n) | \forall i\ x_i \in F\}$ – арифметическое линейное пространство над F.

Теория линейной зависимости вместе со всеми теоремами для $\mathbb{R}$ и $\mathbb{C}$ полностью переносится на случай произвольного поля.

Определение. Система $(a_1, \dots, a_n)$ в L над F линейно независима, если $\lambda_1 a_1 + \dots + \lambda_n a_n = \bar{0} \Leftrightarrow \lambda_i = 0\ \forall i$.

Определение. Система $(a_1, \dots, a_n) = A$ – базис в L над F, если:

1) A – линейно независима;
2) $\forall b \in L\ \exists \lambda_1, \dots, \lambda_n \in F: b = \lambda_1 a_1 + \dots + \lambda_n a_n$.

Определение. Если A – базис в L и $|A| = n$, то размерность $L(\dim L)$ равна n.

§13. Идеалы и гомоморфизмы ассоциативных колец

Ниже все кольца предполагаются ассоциативными, т. е. такими, в которых умножение элементов является ассоциативной операцией: $(xy)z = (x)yz$. В частности, при рассмотрении произведений $x_1, \dots, x_n$ любого числа сомножителей мы можем не заботиться о расстановке скобок.

Определение. *Левым (правым) идеалом кольца* R называется его любое непустое подмножество L, удовлетворяющее двум условиям:

а) L – подгруппа в аддитивной группе R;

б) $RL \subseteq L$ $(LR \subseteq L)$, т. е. $\forall x \in R$, $\forall a \in L$ $xa \in L$ $(ax \in L)$.

Определение. Подмножество в кольце R, являющееся одновременно левым и правым идеалом, называется *идеалом в* R *(или двусторонним идеалом).*

Предложение. Имеют место следующие утверждения:

1) Идеал любого вида в кольце R содержит ноль этого кольца;
2) идеал любого вида в кольце R является подкольцом в R.
3) если R коммутативно, то любой его левый и правый идеал является двусторонним.

Доказательство очевидно.

Определение. Коммутативное кольцо без делителей нуля называют *целостным*.

Лемма. Если R – кольцо, то для любого его элемента a подмножество Ra является его левым идеалом, а подмножество aR – правым идеалом.

Доказательство. Докажем, что Ra – левый идеал. Пусть $x, y \in Ra$. Тогда $x = ua$, $y = va$ для некоторых элементов $u, v \in R$, откуда $x + y = ua + va = (u + v)a \in Ra$ и $(-x) = = (-ua) = (-u)a \in Ra$, т.е. Ra – подгруппа в аддитивной группе R. Далее, если z – любой элемент из R, то $zx = z(ua) = = (zu)a \in Ra$ и, значит, Ra – левый идеал. Доказательство для aR аналогичное.

Идеал Ra из предыдущий леммы называется главным левым идеалом, а идеал aR – главным правым идеалом, причем в обоих случаях a называется порождающим элементом соответствующего идеала.

Определение. Коммутативное кольцо называется кольцом главных идеалов, если в нем любой идеал является главным.

Теорема 1. Кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов $F[x]$ над полем F являются целостными кольцами главных идеалов.

Доказательство. Целостность обоих колец очевидна. Докажем, что $\mathbb{Z}$ – кольцо главных идеалов (для $F[x]$ доказательство аналогичное). Пусть L – идеал в $\mathbb{Z}$ и пусть m – наименьшее натуральное число, содержащееся в L. Предположим, что a – любой элемент из L. Поделим a на m с остатком, т.е. представим

a в виде $a = qm + r$, где $0 \leq r < m$. Так как $qm \in L$, то и $r \in L$, откуда в силу минимальности m число r должно равняться 0. Тогда $a = qm \in Rm$, т.е. $L = Rm$.

Определение. Отображение f кольца R в кольцо R' называется гомоморфизмом, если $\forall\, x, y \in R$ 1) $f(x+y) = f(x) + f(y)$, 2) $f(xy) = f(x)f(y)$.

Лемма. Если $f\colon R \to R'$– гомоморфизм колец, то

1) $f(0) = 0$;

2) $f(-x) = -f(x)\ \forall x \in R$.

Доказательство. Так как $f(0) = f(0+0) = f(0) + f(0)$, то $f(0)$ является нулем кольца R'. Далее, $\forall x \in R \quad f(0) = f\big(x + (-x)\big) = f(x) + f(-x)$, откуда ввиду доказанного пункта первого $f(-x) = -f(x)$. Лемма доказана.

Замечание. Если кольца R и R' – кольца с единицами, то для гомоморфизма $f\colon R \to R'$ обычно предполагается выполнение условия $f(1) = 1$, где справа стоит единица кольца R'.

Определение. Ядром кольцевого гомоморфизма $f\colon R \to R'$ называется $\{x \in L \mid f(x) = 0\}$ и обозначается ядро $\mathrm{Ker} f$.

Теорема 2. $\mathrm{Ker} f$ – идеал в R.

Доказательство. Поскольку f – групповой гомоморфизм аддитивной группы R в аддитивную группу R', то $\mathrm{Ker} f$ – подгруппа в R. Пусть теперь $a \in \mathrm{Ker} f$ и $x \in R$. Тогда $f(xa) = f(x)f(a) = f(x)\,0 = 0$ и $f(ax) = f(a)f(x) = 0 \cdot f(x) = 0$, откуда xa и ax лежат в $\mathrm{Ker} f$. Теорема доказана.

Пусть теперь R – произвольное кольцо, L – подгруппа в аддитивной группе кольца R. Обозначим множество всех смежных классов $x + L$ аддитивной группы R по ее подгруппе L, как и в теории групп, R/L. Определим операции на R/L следующим образом: $\forall x, y \in L$.

$(x + L) + (y + L) = (x + y) + L$ и $(x + L)(y + L) = (xy) + L$.

Теорема 3. Множество R/L является кольцом относительно вышеопределенных операций.

Доказательство. Корректность определения первой операции была уже доказана в теории групп. Докажем корректность операции умножения. Пусть $x' \in x + L$, $y' \in y + L$. Тогда $x' = x + a$, $y' = y + b$, где $a, b \in L$, откуда $x'y' = (x + a)(y + b) = xy + + xb + ay + ab \in xy + L$, так как L – двусторонний идеал. Тогда $x'y' + L = xy + L$, что и требовалось доказать.

Проверка всех кольцевых аксиом для $\frac{R}{L}$ очевидна. Проверим, например, дистрибутивность. $\big((x + L) + (y + L)\big)(z + L) = = \big((x + y) + L\big)(z + L) = (x + y)z + L = (xz + yz) + L = = (xz + L) + (yz + L) = (x + L)(z + L) + (y + L)(z + L)$.

Замечание. Если R – кольцо с единицей 1, то R/L также кольцо с единицей, где роль единицы выполняет смежный класс $1 + L$.

Определение. Кольцо R/L называется фактор-кольцом R по идеалу L.

Лемма. Определим отображение $\varepsilon: R \to R/L$ следующим образом: $\forall x \in R\ \varepsilon(x) = x + L$. Тогда ε – гомоморфизм. Доказательство очевидно.

Определение. Гомоморфизм ε называется каноническим гомоморфизмом R на его фактор-кольцо R/L.

Также как и в теории групп, имеет место основная теорема о гомоморфизмах.

Теорема 4. Пусть f – гомоморфизмом кольца R на кольцо R'(т.е. сюръективный гомоморфизм). Тогда существует единственный изоморфизм φ кольца $R/\mathrm{Ker}f$ на R такой, что $\forall x \in R\ f(x) = \varphi(\varepsilon(x))$, т.е. следующая диаграмма (рис. 21) коммутативна:

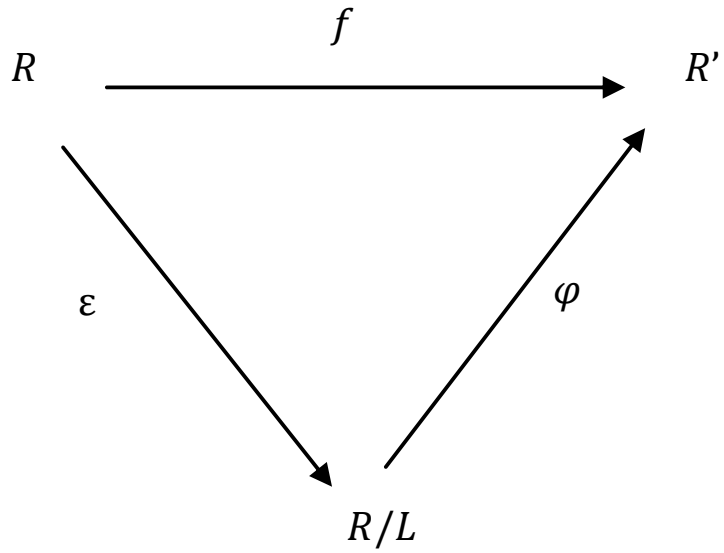

Рис.21

Доказательство этой теоремы такое же, как доказательства аналогичных теорем в теориях полугрупп и групп, и также имеем следующий результат.

Следствие. Любой гомоморфный образ кольца R изоморфен фактор-кольцу R по некоторому двустороннему идеалу R.

В заключение заметим, что элементы фактор-кольца R/L называют *классами вычетов кольца R по модулю L*, и элементы a и b кольца R называются сравнимыми по модулю L, если $a + L = b + L$, т.е. $a - b \in L$. Так как смежные классы группы по подгруппе образуют разбиение этой группы, то *отношение сравнения по модулю L является эквивалентностью на* R, классами которой являются классы вычетов по модулю L. Если a и b сравнимы по модулю L, то пишут $a \equiv b \bmod L$. Особенно важными для приложений являются кольца классов вычетов кольца $\mathbb{Z}$ по модулю идеала $n\mathbb{Z}$ и кольца $F[x]$ по модулю главного идеала $f(x)F[x]$. Эти кольца и связанные с ними результаты мы рассмотрим в следующей главе.

Глава III. Теория чисел и теория многочленов

§ 1. Элементарная теория чисел

Определение. Натуральное число p называется *простым,* если $p > 1$ и его натуральными делителями являются лишь 1 и само p. Непростое натуральное число, отличное от единицы, называется составным.

Теорема 1. Множество простых чисел бесконечно.

Доказательство. Предположим, что $p_1, \dots, p_k$ – все простые числа. Рассмотрим число $n = p_1 \dots p_k + 1$. По предположению n составное. Тогда оно должно делиться на p_i при некотором $i \leq k$. Но $n - p_1 \dots p_k = 1$, откуда p_i делит 1. Получили противоречие, которое доказывает теорему.

Следующие две теоремы входят в школьную программу, и мы их приводим без доказательства.

Теорема 2 (о делении с остатком). Для любых целых чисел a и b, где $b \neq 0$, существуют однозначно определенные целые числа q и r такие, что $a = bq + r$, где $0 \leq r \leq |b| - 1$.

Заметим, что при этом q называется частным, а r – остатком при делении a на b.

Теорема 3 (о разложении натурального числа в произведение простых сомножителей). Любое натуральное число n, большее единицы, представляется в виде $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, где $k \geq 1$, все $\alpha_i \in \mathbb{N}$, и представление n в таком виде однозначно с точностью до перестановки сомножителей.

Очевидно, что для любых целых чисел a и b при условии, что хотя бы одно из них не равно нулю, существует наибольший натуральный общий делитель этих чисел. Он обозначается (a, b) или НОД(a, b).

Лемма. Если d' – общий делитель a и b и $d = \text{НОД}(a, b)$, то d' делит d.

Доказательство легко следует из теоремы 3.

Наибольший общий делитель натуральных чисел a и b при $b \neq 0$ находится с помощью так называемого *алгоритма Евклида.*

Поделим a на b с остатком r_1, затем b поделим на r_1 с остатком r_2 и т.д. Так как $r_1 > r_2 > \cdots$ – строго убывающая последовательность натуральных чисел, то на каком-то шаге r_s поделится на r_{s+1} без остатка. Итак, получим систему равенств:

$a = bq_1 + r_1$

$b = r_1q_2 + r_2$

$r_1 = r_2q_3 + r_3$

……

$r_{s-1} = r_sq_{s+1} + r_{s+1}$

$r_s = r_{s+1}q_{s+2}$

Теорема 4. $r_{s+1} = \text{НОД}(a, b)$.

Доказательство. Докажем, что r_{s+1} – общий делитель a и b. Двигаясь по данной системе равенств снизу вверх, имеем $r_{s+1}|r_s$. Переходя ко второму неравенству снизу, получим $r_{s+1}|r_{s-1}$, из третьего равенства снизу получим $r_{s+1}|r_{s-2}$ и т. д. Дойдя до вто-

рого равенства сверху, получим $r_{s+1}|b$ и, перейдя к верхнему равенству, получим $r_{s+1}|a$.

Пусть теперь d' – общий делитель a и b. Рассматривая ту же цепочку равенств, но уже сверху вниз, получим

$d'|r_1,\ d'|r_2, \ldots, d'|r_s$ и из предпоследнего равенства – $d'|r_{s+1}$. Таким образом, $r_{s+1} = \text{НОД}(a, b)$.

Теорема 5. Для любых целых a и b, одновременно не обращающихся в ноль, существуют целые числа u и v так, что $au + bv = d$, где $d = \text{НОД}(a, b)$.

Доказательство. Можно считать, что $a, b \neq 0$. Снова используем систему равенств перед теоремой 4. Из первого равенства получим $r_1 = a - bq_1$. Из второго равенства получим $r_2 = b - r_1 q_2 = b - (a - bq_1)q_2 = -aq_2 + b(1 + q_1 q_2)$. Обозначив $(-q_2) = u_2$, $1 + q_1 q_2 = v_2$, имеем $r_2 = au_2 + bv_2$. Далее поступаем аналогично. Пусть $r_{n-2} = au_{n-2} + bv_{n-2}$, $r_{n-1} = au_{n-1} + bv_{n-1}$, при $n \geq 3$. Тогда $r_n = r_{n-2} - r_{n-1}q_n = (au_{n-2} + bv_{n-2}) - (au_{n-1} + bv_{n-1})q_n = a(u_{n-2} - u_{n-1}q_n) + b(v_{n-2} - v_{n-1}q_n)$.

Продолжая счет таким образом, в итоге получим $r_{s+1} = au_{s+1} + bv_{s+1}$.

Вычисление членов последовательностей u_n, v_n удобно организовать с помощью таблицы с применением начальных условий $u_1 = 1$, $v_1 = -q_1$, $u_2 = -q_2$, $v_2 = 1 + q_1 q_2$ и рекуррентных соотношений:

$u_n = u_{n-2} - u_{(n-1)}q_n$, $v_n = v_{n-2} - v_{(n-1)}q_n$.

Пример 1. Найти НОД $(1729, 1547)$ и такие целые числа u, v, что $1729u + 1547v = d$.

Решение. $1729 = 1547 \cdot 1 + 182$.

$1547 = 182 \cdot 8 + 91$.

$182 = 91 \cdot 2$.

Имеем $q_1 = 1, q_2 = 8$, НОД $(1729, 1547) = 91$. Составим таблицу для нахождения u, v (табл. 13).

Таблица 13

n	1	2
q_n	1	8
u_n	1	-8
v_n	-1	9

Из таблицы находим $u = -8$, $v = 9$. Итак, $d = 91$ и $91 = = 1729(-8) + 1547 \cdot 9$.

Заметим, что при вычислении u_n, v_n рекуррентные формулы не понадобились.

Пример 2. Найти $d =$ НОД$(2539,1837)$ и такие целые числа u, v, чтобы $2539u + 1837v = d$.

Решение.

$$2539 = 1837 \cdot 1 + 702$$

$$1837 = 702 \cdot 2 + 433$$

$$702 = 433 \cdot 1 + 269$$

$$433 = 269 \cdot 1 + 164$$

$$269 = 164 \cdot 1 + 105$$

$$164 = 105 \cdot 1 + 59$$

$$105 = 59 \cdot 1 + 46$$

$$59 = 46 \cdot 1 + 13$$

$$46 = 13 \cdot 3 + 7$$

$$13 = 7 \cdot 1 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6$$

Откуда $d = 1, (q_n) = (1,2,1,1,1,1,1,1,3,1,1)$ и последовательности u_n, v_n имеют 11 членов, т. е. $u = u_{11}, v = v_{11}$.

Составим снова таблицу (табл. 14).

Таблица 14

n	1	2	3	4	5	6	7	8	9	10	11
q_n	1	2	1	1	1	1	1	1	3	1	1
u_n	1	2	3	5	8	13	1	34	123	-157	280
v_n	1	3	4	7	11	8	29	7	-170	217	-387

Ответ: $d = 1$ и $d = 2539 \cdot 280 - 1837 \cdot 387$.

Упражнения для самостоятельной подготовки

Найти наибольший общий делитель следующих пар чисел a и b и такие целые числа u, v, чтобы выполнялось $au + bv = d$.

1) $a = 4608, b = 5517$;
2) $a = 7817, b = 4321$.

§ 2. Взаимно простые числа

Определение. Два ненулевых целых числа a называются *взаимно простыми*, если их наибольший общий делитель равен 1.

Теорема. Справедливы следующие утверждения:

1) Ненулевые целые числа a и b взаимно просты $\Leftrightarrow$ $\exists\, u, v \in \mathbb{Z}$, что $au + bv = 1$.

2) Если ab делится на c и b, c взаимно просты, то a делится на c.

3) Если a делится на b, a делится на c и b, c взаимно просты, то a делится на bc.

Доказательство.

1) Необходимость следует из теоремы 5 § 1. Пусть дано, что $au + bv = 1$, $u, v \in \mathbb{Z}$. Предположим, что $d \in \mathbb{N}$, $d|a, d|b$. Тогда d делит $au + bv$, т. е. $d|1$, откуда $d = 1$. Достаточность доказана.

2) Так как b и c взаимно просты, по теореме 5 существуют целые u, v такие, что $bu + cv = 1$. Умножим это равенство на a: $abu + acv = a$. Так как abu делится на c, ac делится на c, то и a делится на c. Пункт 2 доказан.

3) Так как b и c взаимно просты, то из теоремы 3 следует, что $b = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $c = q_1^{\beta_1} \dots q_m^{\beta_m}$, где p_i, q_j –

простые числа, причем $p_i \neq q_j$ при любых i, j, и все $\alpha_i, \beta_j \geq 1$. Тогда в силу теоремы 3

$a = p_1^{\alpha_1'} \ldots p_k^{\alpha_k'} q_1^{\beta_1'} \ldots q_m^{\beta_m'} \cdot M$, где $\alpha_i' \geq \alpha_i, \beta_j' \geq \beta_j$ для всех i, j и $M \in \mathbb{Z}$. Пункт третий доказан. ■

§ 3. Теория сравнений

Определение. Пусть $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Мы пишем $a \equiv b (\mathrm{mod}\, n)$ и говорим, что a сравнимо с b по модулю n, если $a - b$ делится на n.

Предложение 1. $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow$ классы вычетов $a + n\mathbb{Z}$ и $b + n\mathbb{Z}$ в кольце $\mathbb{Z}/n\mathbb{Z}$ (фактор-кольце кольца $\mathbb{Z}$ по главному идеалу $n\mathbb{Z}$) совпадают.

Доказательство. $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow (a - b)$ делится на $n \Leftrightarrow$ $\exists q \in \mathbb{Z}$, что $a - b = nq \Leftrightarrow \exists q \in \mathbb{Z}$, $a = b + nq \Leftrightarrow a \in b + n\,\mathbb{Z} \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z}$, что и требовалось доказать.

Заметим, что последняя равносильность вытекает из того, что различные классы вычетов кольца по идеалу не пересекаются.

Следствие. Отношение сравнения по модулю n является эквивалентностью на $\mathbb{Z}$, и классы этой эквивалентности совпадают с классами вычетов по модулю идеала $n\mathbb{Z}$, т. е. с элементами фактор-кольца $\mathbb{Z}/n\mathbb{Z}$.

Предложение 2.

1) Для любого целого: a $a + n\,\mathbb{Z} = r + u\mathbb{Z}$, где r – остаток от деления a на n;
2) $|\mathbb{Z}/n\mathbb{Z}| = n$, причем

$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$.

Доказательство.

1) Поделим a на n с остатком: $a = nq + r$, $q, r \in \mathbb{Z}$, $0 \le r \le n - 1$. Тогда $a \in r + n\mathbb{Z}$, откуда $a + n\mathbb{Z} = r + n\mathbb{Z}$ в силу соответствующего свойства классов вычетов произвольного кольца.

2) Пусть $0 \le i \le j \le n - 1$ и $i + n\mathbb{Z} = j + n\mathbb{Z}$. Тогда $j - i$ делится на n и $0 \le j - i \le n - 1$, откуда $i = j$. Следовательно, классы вычетов, перечисленные в фигурных скобках выше, попарно различны. Применяя пункт первый, получаем второй.

Замечание. Если n фиксировано, то удобно вместо $a + n\mathbb{Z}$ писать просто $\bar{a}$.

Теорема 1. $\mathbb{Z}/n\mathbb{Z}$ является коммутативным ассоциативным кольцом относительно сложения и умножения, определенных по формулам $\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a} \cdot \bar{b} = \overline{ab}$. При этом роль нуля выполняет нулевой класс $n\mathbb{Z}$, а роль единицы – $(1 + n\mathbb{Z})$.

Доказательство теоремы следует из общих результатов о фактор-кольцах.

Теорема 2. $\mathbb{Z}/n\mathbb{Z}$ – поле $\Leftrightarrow$ n – простое число.

Доказательство.

При $n = 1$ $|\mathbb{Z}/n\mathbb{Z}| = 1$ и, значит, $\mathbb{Z}/n\mathbb{Z}$ – не поле.

Пусть теперь $n > 1$. Необходимость докажем от противного.

Предположим, что $n = pq$, $1 < p < n$, $1 < q < n$. Тогда $\bar{0} = \bar{n} = \overline{pq}$, где $\bar{p}, \bar{q} \neq \bar{0}$, т. е. $\bar{p}$ и $\bar{q}$ – делители нуля, чего не может быть в поле. Необходимость доказана.

Предположим теперь, что n – простое число и $j + n\,\mathbb{Z}$, где $1 \leq j \leq n - 1$ – произвольный ненулевой класс вычетов из $\mathbb{Z}/n\mathbb{Z}$. Тогда j и n взаимно просты и по теореме шестой предыдущего параграфа существуют целые числа u и v такие, что $ju + nv = 1$ и, следовательно, $\bar{j}\,\bar{u} = 1$, $\bar{j}$ имеет обратный элемент в $\mathbb{Z}/n\mathbb{Z}$. Значит, $\mathbb{Z}/n\mathbb{Z}$ – поле. Теорема доказана.

Таким образом, при простом p $\mathbb{Z}/p\mathbb{Z}$ – поле порядка p. Оно называется полем Галуа и обозначается F_p или $GF(p)$.

Теорема 3. $\bar{a}$ обратим в $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ a взаимно просто с n.

Доказательство совершенно аналогично доказательству теоремы 2.

Определение. *Функцией Эйлера* называется функция φ такая, что для любого натурального n $\varphi(n)$ равно числу натуральных чисел, меньших n и взаимно простых с n.

Предложение. $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, где $(\mathbb{Z}/n\mathbb{Z})^*$ – группа обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.

Предложение следует сразу из теоремы 3.

Теорема 4 (Эйлера). Если a взаимно просто с n, то $a^{\varphi(n)} \equiv$ $\equiv 1 \bmod n$.

Доказательство.

В силу предыдущего предложения мультипликативная группа $(\mathbb{Z}/n\mathbb{Z})^*$ кольца $\mathbb{Z}/n\mathbb{Z}$ имеет порядок $\varphi(n)$, а также по теореме 3 $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Тогда в силу следствия к теореме 2 параграфа о циклических группах $\overline{a^{\varphi(n)}} = \bar{1}$, откуда следует справедливость теоремы.

Теорема 5 (мультипликативность функции Эйлера). Если a и b взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство.

Выпишем представителей всех классов $\mathbb{Z}/(a \cdot b)\mathbb{Z}$ в прямоугольную таблицу (табл. 15):

Таблица 15

0	1	…	j	…	$a-1$
a	$1+a$	…	$j+a$	…	$(a-1)+a=2a-1$
			…		
$(b-1)\,a$	$1+(b-1)\,a$	…	$j+(b-1)\,a$	…	$(a-1)+(b-1)\,a$ $= ab-1$

Необходимо выяснить, сколько в таблице чисел, взаимно простых с ab, т. е. и с a, и с b одновременно.

Выясним, сколько чисел, взаимно простых с a. Числа в j-столбце взаимно просты с a тогда и только тогда, когда j взаимно просто с a. Таких столбцов $\varphi(a)$ штук. Таким образом, чисел, взаимно простых с a, $\varphi(a)b$ штук.

Рассмотрим любой столбец, где j взаимно просто с a, перейдем в нем к классам вычетов по модулю b. Докажем, что все классы вычетов в этом столбце разные. Предположим, что $\overline{j+ka} = \overline{j+la}$, $0 \le k,l \le b-1$ в $\mathbb{Z}/b\mathbb{Z}$. Тогда $\bar{j} + \overline{ka} = \bar{j} + \overline{la}$ и, следовательно, $\overline{ka} = \overline{la}$. Так как a взаимно просто с b, то в $\mathbb{Z}/b\mathbb{Z}$ существует $(\bar{a})^{-1}$. Преобразуем полученное равенство: $\overline{ka}(\bar{a})^{-1} = \overline{la}(\bar{a})^{-1} \Rightarrow \bar{k} = \bar{l}$, причем $0 \le k,l \le b-1$, следовательно, $k = l$.

Доказали, что в столбце все классы по модулю b разные. Поэтому по определению функции Эйлера, среди чисел $j, j+a, \dots, j+(b-1)a$ точно $\varphi(b)$ чисел, взаимно простых с b.

В итоге, получаем $\varphi(a)$ столбцов, в которых все числа взаимно просты с a и в каждом $\varphi(b)$ чисел, взаимно простых с b. Общее количество чисел, взаимно простых и с a, и с b, равно $\varphi(a)\varphi(b)$. Теорема доказана.

В вычислениях функции Эйлера используется также следующий факт.

Предложение. $\varphi(p^n) = p^{n-1}(p-1)$.

Доказательство. При $n = 1$ имеем очевидно верное утверждение: $\varphi(p) = (p-1)$. Если $n > 1$, то ряд натуральных чисел, меньших p^n и делящихся на p, имеет вид $p, 2p, \dots, (p^{n-1}-1)p$, т. е. количество таких чисел равно $p^{n-1}-1$. Тогда $\varphi(p^n) = (p^n-1) - (p^{n-1}-1) = p^n - p^{n-1}$, что и требовалось доказать. ■

§ 4 Китайская теорема об остатках

Рассмотрим систему сравнений $\begin{cases} x \equiv x_1 \bmod n_1 \\ x \equiv x_2 \bmod n_2 \\ \quad \ldots \\ x \equiv x_k \bmod n_k \end{cases}$ (1)

где x – неизвестное целое, числа n_i попарно взаимно простые.

Аналогично систему можно рассмотреть для многочленов над полем F:

$$\begin{cases} f(x) \equiv \varphi(x_1) \bmod \psi_1(x) \\ f(x) \equiv \varphi(x_2) \bmod \psi_2(x) \\ \quad \ldots \\ f(x) \equiv \varphi(x_k) \bmod \psi_k(x), \end{cases}$$

Где $\psi_i(x), \psi_j(x)$ – взаимно просты при $i \neq j$ над полем F.

По аналогии с теорией чисел $f(x) \equiv \varphi(\mathrm{x}) \bmod \psi(x) \Leftrightarrow f(x) - \varphi(x)$ делится на $\psi(x)$.

Пусть $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$,

$m_j = \frac{N}{n_j} = n_1 \cdot \ldots \cdot n_{j-1} \cdot n_{j+1} \cdot \ldots \cdot n_k$.

Например, пусть $n_1 = 2, n_2 = 3, n_3 = 5$. Тогда $N = 30, m_1 = 15, m_2 = 10, m_3 = 6$.

Теорема 1. Пусть x_0 – любое частное решение системы (1). Тогда все числа из $x_0 + N\mathbb{Z}$ тоже частные решения системы (1).

Доказательство. $\hat{x} \in x_0 + N\mathbb{Z} \Rightarrow \hat{x} \equiv x_0 \bmod N \Rightarrow \hat{x} \equiv x_0 \bmod n_j \ \forall j = \overline{1,k}$, т.к. $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$. Учитывая, что $x_0 \equiv x_j \bmod n_j$, в силу (1) имеем $\hat{x} \equiv x_j \bmod n_j \ \forall j = \overline{1,k}$. Значит, $\hat{x}$ – частное решение. Теорема доказана.

Теорема 2. Пусть $\hat{x}$ и $\tilde{x}$ − частные решения системы (1). Тогда $\hat{x} \equiv \tilde{x} \bmod N$.

Доказательство.

$\forall j = \overline{1,k}\ \ \hat{x} \equiv x_j \bmod n_j,\ \ \tilde{x} \equiv x_j \bmod n_j \ \Rightarrow\ \hat{x} \equiv \tilde{x} \bmod n_j,$ т. е. $\hat{x}$-$\tilde{x}$ делится на n_j. Т. к. числа n_j попарно взаимно простые, то по 3-му свойству взаимно простых чисел $\hat{x}$-$\tilde{x}$ делится на $n_1 \cdot n_2 \cdot \ldots \cdot n_k = N$, откуда $\hat{x} \equiv \tilde{x} \bmod N$.

Теорема доказана. ■

Следствие. Множество всех решений системы (1), если она совместна, представляет собой класс вычетов по модулюN, причем единственный.

Теорема 3. Обозначим как y_j любое целое число, удовлетворяющее сравнению $m_j y_j \equiv x_j \bmod n_j\ \ \forall j = \overline{1,k}$ (y_j существует, т. к. m_j взаимно просто с n_j). Тогда $x_0 = m_1 y_1 + m_2 y_2 + \cdots + + m_k y_k$ − частное решение системы (1).

Доказательство. Фиксируем $j = \overline{1,k}$. Требуется доказать $x_0 \equiv x_j \bmod n_j$, т. е. $\overline{x_0} = \overline{x_j}$ в $\mathbb{Z}/n_j\mathbb{Z}$. Имеем $\overline{x_0} = \overline{m_1 y_1} + \overline{m_2 y_2} + + \cdots + \overline{m_k y_k} = \overline{x_j}$, т. к. в каждом $m_s y_s$ при $s \neq j$ присутствует n_j.

Теорема доказана. ■

Совокупность теорем 1–3 называется *Китайской теоремой об остатках.*

Обобщение китайской теоремы об остатках

Теорема 4. $\begin{cases} x \equiv x_1 \bmod n_1 \\ x \equiv x_2 \bmod n_2 \\ \quad\ldots \\ x \equiv x_k \bmod n_k \end{cases}$ совместна $\Leftrightarrow$

$\forall i,j \quad x_i \equiv x_j \bmod \text{НОД}\,(n_i, n_j)$.

Теорема 5. Если система $\begin{cases} x \equiv x_1 \bmod n_1 \\ x \equiv x_2 \bmod n_2 \\ \quad\ldots \\ x \equiv x_k \bmod n_k \end{cases}$ совместна, то при любом частном решении x_0 ее общее решение имеет вид $x = x_0 + N\mathbb{Z}$, где $N = \text{НОК}(n_1, n_2, \ldots, n_k)$.

Примеры к §§ 3, 4.

1. Решить уравнение в целых числах: $17x - 13y = 1$.

Решение.

В обеих частях уравнения перейдем к классам вычетов по модулю 13: $\overline{17}\bar{x} - \overline{13}\bar{y} = \bar{1}$ в $\mathbb{Z}/13\mathbb{Z}$.

Так как $\overline{13}=\bar{0}$, то $\bar{4}\bar{x} = \bar{1}$.

Подбором находим $\bar{x} = \overline{-3}$, т. е. $x = -3 + 13k$.

Подставляя найденное выражение для x в исходное уравнение, получим $17(-3 + 13k) - 13y = 1$, откуда $13y = -52 + 17 \cdot 13k$, т. е. $y = -4 + 17k$.

Ответ:

$\begin{cases} x = -3 + 13k \\ y = -4 + 17k, k \in \mathbb{Z} \end{cases}$

2. Решить уравнение в целых числах: $13x + 19y + 23z = 3$.

Решение. Перейдем в обеих частях равенства к классам вычетов по модулю 13: $\overline{13}\bar{x} + \overline{19}\bar{y} + \overline{23}\bar{z} = \bar{3}$, т.е. $\bar{6}\bar{y} + \overline{10}\bar{z} = \bar{3}$ в $\mathbb{Z}/13\mathbb{Z}$.

Далее имеем $\bar{6}\bar{y} = \overline{3 - 10z}$.

Подбором находим $\bar{6}^{-1}$ в $\mathbb{Z}/13\mathbb{Z}$: $\bar{6}^{-1} = \overline{-2}$.

Умножим обе части уравнения с $\bar{y}$ на $\overline{-2}$, после чего получим $\bar{y} = \overline{-6 + 20z} = \overline{7 + 7z}$, т. е. $y = 7 + 7z + 13k, k \in \mathbb{Z}$.

Подставив полученное выражение для y в исходное уравнение, получим выражение x через z и k:

$$13x + 19(7 + 7z + 13k) + 23z = 3 \Rightarrow$$

$$13x = -130 - 156z - 19 \cdot 13k \Rightarrow$$

$$x = -10 - 12z - 19k$$

Ответ: $\begin{cases} x = -10 - 12z - 19k \\ y = 7 + 7z + 13k, k \in \mathbb{Z} \end{cases}$

3. Какой остаток имеет число 2012^{2013} при делении на 17?

Решение. Посчитаем $\overline{2012^{2013}}$ в $\mathbb{Z}/17\mathbb{Z}$.

Поделим 2012 на 17 с остатком: $2012 = 17 \cdot 118 + 6$, а 2013 поделим на $\varphi(17) = 16$ с остатком: $2013 = 16 \times \times 125 + 13$.

Учитывая, что по теореме Эйлера $\bar{6}^{16} = \bar{1}$ в $\mathbb{Z}/17\mathbb{Z}$, имеем $\overline{2012^{2013}} = \bar{6}^{16 \cdot 125 + 13} = \bar{6}^{13}$.

Далее $\bar{6}^3 = \overline{216} = \overline{12}$, $\bar{6}^6 = \overline{144} = \bar{8}$, $\bar{6}^9 = \overline{96} = \overline{11}$, $\bar{6}^4 = \overline{72} = \bar{4}$, $\bar{6}^{13} = \bar{6}^9 \cdot \bar{6}^4 = \overline{44} = \overline{10}$, откуда получаем ответ: искомый остаток равен 10.

4. С помощью функции Эйлера решить уравнение $37x \equiv 18 \bmod 57$.

Решение. Данное сравнение равносильно уравнению $\overline{37}\bar{x} = \overline{18}$ в $\mathbb{Z}/57\mathbb{Z}$, откуда $\bar{x} = \overline{37}^{-1} \cdot \overline{18}$. Найдем $\overline{37}^{-1}$ с учетом того, что $\overline{37}^{56} = \bar{1}$, т.к. $56 = \varphi(57)$.

Имеем $\overline{37}^{-1} = \overline{37}^{55} = \overline{37}^{2^5+2^4+2^2+2+1}$, $\overline{37}^2 = \overline{(-20)}^2 =$ $= \overline{400} = \bar{1}$, откуда $\overline{37}^{-1} = \overline{37}$.

Окончательно имеем $\bar{x} = \overline{37} \cdot \overline{18} = \overline{39}$.

Ответ: $x = 39 + 57k$, $k \in \mathbb{Z}$

5. Решить сравнение $189x \equiv 1 \bmod 512$ с помощью алгоритма Евклида.

Решение. Данную задачу можно свести к нахождению таких целых u, v, при которых $512u + 189v = 1 =$ $=$ НОД$(189,512)$. Такую задачу мы рассматривали в первом параграфе. Применяем алгоритм Евклида к паре $a = 512, b = 189$:

$$a = 512 = 189 \cdot 2 + 134$$

$$b = 189 = 134 \cdot 1 + 55$$

$$r_1 = 134 = 55 \cdot 2 + 24$$

$$r_2 = 55 = 24 \cdot 2 + 7$$

$$r_3 = 24 = 7 \cdot 3 + 3$$

$$r_4 = 7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3$$

Имеем $r_6 = 1 = \text{НОД}(a, b)$, следовательно, искомые u, v равны u_6 и v_6 соответственно, где последовательности u_n и v_n считаются с помощью таблицы, как показано в предыдущем параграфе, причем $u_1 = 1$, $v_1 = -q_1 = -2$, $u_2 = -q_2 = -1$, $v_2 = 1 + q_1 q_2 = 3$. Однако для решения поставленной задачи достаточно считать лишь v_n по рекуррентной формуле $v_n = v_{n-2} - v_{n-1} q_n$ (табл. 16).

Таблица 16

n	1	2	3	4	5	6
q_n	2	1	2	2	3	2
v_n	-2	3	-8	19	-65	149

Так, что искомое $v = v_6 = 149$.

Ответ: $x = 149 + 512k$, $k \in \mathbb{Z}$.

6. Решить систему сравнений $\begin{cases} \mathbf{x \equiv 2 \bmod 13} \\ \mathbf{x \equiv 7 \bmod 17.} \\ \mathbf{x \equiv 9 \bmod 15} \end{cases}$

Решение. Эта задача на китайскую теорему.

$N = 13 \cdot 17 \cdot 15$, $m_1 = 17 \cdot 15 = 255$, $m_2 = 13 \cdot 15 = 195$, $m_3 = 13 \cdot 17 = 221$.

Находим частные решения сравнений:

$m_i y_i \equiv x_i \, mod \, n_i$, где $x_1 = 2$, $x_2 = 7$, $x_3 = 9$,

$n_1 = 13$, $n_2 = 17$, $n_3 = 15$.

Имеем $255y_1 \equiv 2 \bmod 13$, что равносильно $-5y_1 \equiv$ $\equiv 2 \bmod 13$, откуда $y_1 = -3$. Далее, $195y_2 \equiv 7 \bmod 17$,

что равносильно $8y_2 \equiv 7 \bmod 17$, откуда $y_2 = 3$. И, наконец, из сравнения $221y_3 \equiv 9 \bmod 15$, которое равносильно $11y_3 \equiv 9 \bmod 15$, находим $y_3 = -6$. Тогда $m_1y_1 + m_2y_2 + m_3y_3 = 255(-3) + 195 \cdot 3 + 221(-6) = = -1506$ – частное решение исходной системы сравнений.

Ответ: $x = -1506 + 2315k$, $k \in \mathbb{Z}$.

6. Какие остатки может иметь число вида $\mathbf{2015n^{1008} - - 1009n^{2015}}$ при делении на 9.

Решение. Поскольку $2015 \equiv -1 \bmod 9$, а $1009 \equiv \equiv 1 \bmod 9$, то данное выражение можно заменить на $f(n) = -n^{1008} - n^{2015}$. Далее, при n, взаимно простом с 9, по теореме Эйлера $n^{\varphi(9)} \equiv 1 \bmod 9$, т. е. $n^6 \equiv \equiv 1 \bmod 9$. Тогда для решения нашей задачи при n, взаимно простом с 9, можно $f(n)$ заменить на $g(n) = -n - -n^5$, т. к. $2015 = 335 \cdot 6 + 5$.

Натуральные числа n, взаимно простые с 9 и меньшие 9, исчерпываются числами $1, 2, 4, 5, 7, 8$.

Имеем в $\mathbb{Z}/9\mathbb{Z}$:

$g(\overline{1}) = -\overline{2} = \overline{7}$,

$g(\overline{2}) = -\overline{34} = \overline{2}$,

$g(\overline{4}) = -\overline{4} - \overline{4}^5 = -\overline{4} - (-\overline{2})^2 \cdot \overline{4} = -\overline{4} - \overline{16} = -\overline{20} = \overline{7}$,

$g(\overline{5}) = -\overline{5} - \overline{5}^5 = -\overline{5} - (-\overline{2})^2 \cdot \overline{5} = -\overline{25} = \overline{2}$,

$g(\overline{7}) = g(-\overline{2}) = \overline{2} + \overline{2}^5 = \overline{34} = \overline{7}$,

$g(\overline{8}) = g(-\overline{1}) = \overline{1} + \overline{1} = \overline{2}$.

Итак, при n, взаимно простом с 9, исходное выражение может иметь остатки лишь 7 и 2.

При $\bar{n} = \bar{3}$, $\bar{n} = \bar{6}$, $\bar{n} = \bar{0}$ в $\mathbb{Z}/9\mathbb{Z}$ $\overline{f(n)} = \bar{0}$.

Ответ: Исходное выражение при делении на 9 может иметь следующие остатки: 0, 2, 3, 6, 7.

Упражнения для самостоятельной подготовки

1. Решить следующие уравнения в целых числах:
   а) $19x - 26y = 1$;
   б) $17x + 41y = 1$;
   в) $11x + 14y + 17z = 1$;
   г) $13x - 21y + 15z = 1$.
2. Какие остатки имеют указанные числа x на указанные числа y:

а) $x = 1945^{1961}, y = 17$;

б) $x = 1917^{2017}, y = 23$?

3. С помощью функции Эйлера решить сравнения:
   а) $29x \equiv 13 \bmod 61$;
   б) $31x \equiv 48 \bmod 59$.
4. Решить сравнения с помощью алгоритма Евклида:
   а) $547x \equiv 1 \bmod 1024$;
   б) $343x \equiv 1 \bmod 729$.

5. Решить следующие системы сравнений:

а) $\begin{cases} x \equiv 9 \bmod 13; \\ x \equiv -10 \bmod 21; \\ x \equiv 2 \bmod 17. \end{cases}$

б) $\begin{cases} x \equiv 1 \bmod 7; \\ x \equiv 2 \bmod 9; \\ x \equiv 3 \bmod 13; \\ x \equiv 4 \bmod 17. \end{cases}$

§ 5. Элементарная теория многочленов

Напомним, что $F[x]$ – кольцо многочленов над полем F. Это кольцо коммутативно, ассоциативно и с единицей.

Аналогом простого числа в $F[x]$ является неприводимый многочлен.

Определение. Многочлен $f(x)$ из $F[x]$ *неприводим* над F, если его нельзя представить в виде $f(x) = g(x)h(x)$, где $1 \leq \deg g(x) < \deg f(x)$, $1 \leq \deg h(x) < \deg f(x)$.

Из определения следует, что любой многочлен степени 1 неприводим. Имеет место аналог теоремы 1 параграфа 1.

Теорема 1. Даже, если F – конечное поле, число неприводимых многочленов над F бесконечно.

Доказательство этой теоремы гораздо сложнее, чем доказательство аналогичной теоремы в теории чисел, и мы его опустим.

Теорема 2 (о делении с остатком в $F[x]$). Для любых многочленов $f(x), g(x) \in F[x]$ при $g(x) \neq 0$ существуют однозначно определенные многочлены $g(x)$ и $r(x)$ из $F(x)$ такие, что $f(x) = g(x)q(x) + r(x)$, где $\deg r(x) < \deg g(x)$ ($q(x)$ называется частным, $r(x)$ называется остатком при делении $f(x)$ на $g(x)$).

Доказательство проводится стандартной индукцией по степени $f(x)$, и мы его здесь не приводим.

Теорема 3 (о разложении многочлена на неприводимые множители). Любой многочлен $f(x)$ из $F[x]$ степени ≥ 1 представим в виде произведения $\alpha p_1(x) \dots p_k(x)$, где $\alpha \in F^*$, $p_1(x), \dots, p_k(x)$ – неприводимые многочлены над F, и данное представление $f(x)$ однозначно с точностью до перестановки сомножителей $p_i(x)$ и их умножения, а также скаляра α перед ними на элементы из F^*.

Пример. $2x^2 + 5x + 2 = 2\left(x + \frac{1}{2}\right)(x + 2) =$

$= 2(x + 2)\left(x + \frac{1}{2}\right) = (x + 2)(2x + 1)$ и т. д.

Полезным является следующий результат.

Следствие к теореме 2 (Теорема Безу). Если $\alpha \in F$ – корень многочлена $f(x) \in F[x]$, то $f(x)$ делится на $(x - \alpha)$ без остатка.

Доказательство. $f(x) = q(x)(x - \alpha) + r(x)$,

где $\deg r(x) < 1$ по теореме 2 для некоторых

$q(x), r(x) \in F[x]$.

Так как $\deg r(x) < 1$, то $r(x) = r$ – константа из F. Подставив α в обе части равенства для $f(x)$, получим $f(x) = r$, т. е. $r = 0$. Следствие доказано.

Предложение 1.

1) Если $\deg f(x) > 1$, $f(x) \in F[x]$ и $f(x)$ имеет корень в F, то $f(x)$ приводим над F;
2) Если $\deg f(x) = 2$ или 3, $f(x) \in F[x]$ и $f(x)$ приводим над F, то $f(x)$ имеет корень в F.

Доказательство.

1) Следует сразу из теоремы Безу.

Докажем пункт 2. Если $f(x)$ приводим над F, то $f(x) = g(x)h(x)$, где $g(x)$ или $h(x)$ имеет степень 1. Пусть, например, $g(x) = ax + b$, $a, b \in F$, $a \neq 0$.

Тогда $g(x)$ имеет корень $(-\frac{b}{a})$, который является корнем и $f(x)$.

Предложение доказано.

Следствие. Если $f(x) \in F[x]$ и $\deg[f(x)] = 2$ или 3, то $f(x)$ неприводим над $F \Leftrightarrow f(x)$ не имеет корней в F.

Пример 1. Найдем все неприводимые многочлены над $F_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$.

Пусть $f(x) = x^2 + \alpha x + \beta$ неприводим над F_2. Тогда $\beta \neq 0$, а значит, $\beta = 1$, т. е. $f(x) = x^2 + \alpha x + 1$. Если $f(x)$ имеет корень в F, то этот корень может быть только единицей. Подставив 1 в выражение для $f(x)$, получим $1 + \alpha + 1 = \alpha$, т.е. 1 – корень $f(x) \Leftrightarrow \alpha = 0$. Следовательно, над F_2 имеется единственный неприводимый многочлен степени 2: $x^2 + x + 1$.

Пример 2. Найдем все неприводимые многочлены над F_2 степени 3.

Рассмотрим $f(x)$ из $F_2[x]$ вида $x^3 + \alpha x^2 + \beta x + 1$. Если $f(1) = 0$, то $1 + \alpha + \beta + 1 = 0$, т.е. $\alpha = \beta$. Поэтому $f(x)$ неприводим над $F_2 \Leftrightarrow \alpha \neq \beta$.

Таким образом, над F_2 имеется два неприводимых многочлена $x^3 + x + 1$, $x^3 + x^2 + 1$.

Пример 3. Найдем все неприводимые многочлены над F_2 степени 4.

Пусть снова $f(x)$ из $F_2[x]$ имеет вид $x^4 + \alpha x^3 + \beta x^2 + \gamma x + 1$. $f(1) = 0 \Leftrightarrow \alpha + \beta + \gamma = 0$. Имеется четыре варианта для наборов (α, β, γ), удовлетворяющих данному равенству (табл. 17).

Таблица 17

α	β	γ
0	0	0
0	1	1
1	0	1
1	1	0

Таким образом, многочлены $x^4 + 1$, $x^4 + x^2 + x + 1$, $x^4 + x^3 + x + 1$, $x^4 + x^3 + x^2 + 1$ приводимы. Поэтому кандидатами на неприводимый многочлен над F_2 степени 4 остаются многочлены: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^2 + 1$. По построению они все не имеют корней в F_2, но последний из них равен $(x^2 + x + 1)^2$, где $x^2 + x + 1$ – единственный неприводимый многочлен степени 2 над F_2. Так как $x^2 + x + 1$ – единственный неприводимый многочлен степени 2 над F_2, то другие кандидаты из четырех многочленов степени 4, выписанных выше, являются неприводимыми. Таким образом, имеется ровно три неприводимых многочлена степени 4 над F_2: $x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$.

Пример 4. При каких $\alpha \in \{0,1,2,3,4,5,6\}$ многочлен $f(x) = x^3 + \alpha x^2 + 3x + 1$ неприводим над $GF(7)$? (Для любого $i = \overline{0,6}$ мы отождествляем i с соответствующим классом вычетов $\bar{\imath} = i + 7\,\mathbb{Z}$).

Решение. Используем предложение 1.

$f(1) = 5 + 2 = 0 \Leftrightarrow \alpha = 2.$

$f(2) = 8 + 4\alpha + 6 + 1 = 15 + 4\alpha = 1 + 4\alpha = 0 \Leftrightarrow \alpha = 5.$

$f(3) = 27 + 9\alpha + 9 + 1 = 37 + 2\alpha = 2 + 2\alpha = 0 \Leftrightarrow \alpha = 6.$

$f(4) = f(-3) = -27 + 9\alpha - 9 + 1 = -35 + 9\alpha = 0 \Leftrightarrow \alpha = 0.$

$f(5) = f(-2) = -8 + 4\alpha - 6 + 1 = -13 + 4\alpha = 0 \Leftrightarrow \alpha = 5.$

$f(6) = f(-1) = -1 + \alpha - 3 + 1 = 3 - \alpha = 0 \Leftrightarrow \alpha = 3.$

Из проведенных вычислений по модулю 7 делаем вывод, что $f(x)$ неприводим над $GF(7) \Leftrightarrow \alpha = 1$ или $\alpha = 4$, т. е. среди рассматриваемых многочленов только многочлены $x^3 + x^2 + 3x + 1$ и $x^3 + 4x^2 + 3x + 1$ являются неприводимыми.

Пример 5. Разложить $f(x) = x^3 + 3x + 1$ на неприводимые множители над $GF(7)$.

Решение. Из решения примера 4 выше следует, что 4 – единственный корень $f(x)$ над $GF(7)$. Разделим $f(x)$ на $x - 4$, пользуясь схемой Горнера (табл. 18):

Таблица 18

	1	0	3	1
4	1	4	5	0

Отсюда следует, что $f(x) = (x-4)(x^2+4x+5)$. Обозначим $g(x) = x^2+4x+5$. Имеем $g(4) = 37 \neq 0$ в $GF(7)$, следовательно, x^2+4x+5 неприводим над $GF(7)$.

Ответ: $f(x) = (x+3)(x^2+4x+5)$.

Упражнения для самостоятельной подготовки

1. Найти все неприводимые многочлены над $F_3 = \mathbb{Z}/3\mathbb{Z}$ степеней 2 и 3.
2. При каких $\alpha \in \{0,1,2,3,4,5,6\}$ многочлен $f(x) = \alpha x^3 + + 2x^2 + x + 1$ неприводим над $GF(7)$?
3. Разложить $f(x) = x^3 + 2x^2 + x - 5$ на неприводимые множители над $GF(7)$.

§ 6. Теория сравнений для многочленов

Определение. Пусть F – поле, $f(x) \in F[x], f(x) \neq 0$. Тогда многочлен $g(x)$ из $F[x]$ сравним с многочленом $h(x)$ из $F[x]$ по модулю $f(x)$, если $g(x) - h(x)$ делится на $f(x)$ без остатка. Обозначение: $g(x) \equiv h(x) \bmod f(x)$.

Аналогично теории сравнений для чисел имеем следующие результаты:

Теорема 1. Отношение сравнения на $F[x]$ по модулю $f(x)$ является отношением эквивалентности, причем $g(x) \equiv h(x) \bmod f(x) \Leftrightarrow g(x)$ сравним с $h(x)$ по модулю главного идеала $f(x)F[x]$ кольца $F[x]$.

Определение. Пусть $g(x) \in F[x]$. Тогда $\{h(x) \in F[x] | h(x) \equiv g(x) \bmod f(x)\}$ называется классом вычетов по модулю $f(x)$.

Этот класс вычетов обозначается как $\overline{g(x)}$ или в развернутом виде $g(x) + f(x)F[x]$.

Теорема 2. В предыдущих обозначениях имеем:

1) $\forall g(x)\ g(x) \in \overline{g(x)}$;
2) $h(x) \in \overline{g(x)} \Rightarrow \overline{h(x)} = \overline{g(x)}$;
3) различные классы вычетов по модулю $f(x)$ не пересекаются;
4) $\overline{g(x)} = \overline{r(x)}$, где $r(x)$ – остаток от деления $g(x)$ на $f(x)$.

Обозначим множество всех классов вычетов по модулю $f(x)$ $F[x]/(f(x))$.

Как уже было отмечено выше (теорема 1), $F[x]/(f(x))$ – множество классов вычетов кольца $F[x]$ по модулю главного идеала $f(x)F[x]$.

Поэтому справедлива следующая теорема.

Теорема 3. $F[x]/(f(x))$ – ассоциативное коммутативное кольцо с единицей относительно операций:

$\overline{h(x)} + \overline{g(x)} = \overline{h(x) + g(x)}$,

$\overline{h(x)} \cdot \overline{g(x)} = \overline{h(x) \cdot g(x)}$.

Теорема 4. $F[x]/(f(x))$ – поле $\Leftrightarrow$ $f(x)$ не приводим над F.

Следствие. Если многочлен $f(x)$ степени n не приводим над полем F порядка q, то $F[x]/(f(x))$ – поле порядка q^n.

Упражнения для самостоятельной подготовки

Найти порядки $\bar{x}$ в мультипликативных группах полей $F_2[x]/(x^4 + x + 1)$ и $F_2[x]/(x^4 + x^3 + x^2 + x + 1)$ порядка 16.

Список литературы

1. Андерсон Джеймс А. Дискретная математика и комбинаторика / Андерсон, А. Джеймс ; пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 960 с.
2. Ван дер Варден. Алгебра / Ван дер Ваден. – М. : Наука, 1976.
3. Каргаполов М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – М. : Наука, 1972.
4. Клиффорд А. Алгебраическая теория полугрупп / А. Клиффорд, Г. Престон. – М. : Мир, 1972.
5. Кострикин А. И. Введение в алгебру / А. И Кострыкин. – М. : Наука, 1977.
6. Курош А. Г. Лекции по общей алгебре / А. Г. Курош. – М. : Наука, 1973.
7. Ленг С. Алгебра / С. Ленг. – М. : Мир, 1971.
8. Белоногов В. А. Задачник по теории групп / В. А. Белоногов. – М. : Наука, 2000.
9. Ляпин Е. С. Упражнения по теории групп / Е. С. Ляпин, А. Я. Айзенштат, М. М. Лесохин. М. : Наука, 1967.
10. Сборник задач по алгебре : учебник для вузов ; под ред. А. И. Кострикина. – 3-е изд, перераб. и доп. – М. : ФИЗМАТЛИТ, 2001. – 464 с.

Учебное пособие

Веретенников *Борис Михайлович*
Белоусова *Вероника Игоревна*

ДИСКРЕТНАЯ МАТЕМАТИКА
Часть I

Редактор *О. С. Смирнова*

Компьютерный набор *В. И. Белоусовой*
Компьютерная верстка *Я. П. Бояршинова*

Подписано в печать 24.06.2014. Формат 60×90 1/16.
Бумага писчая. Плоская печать. Усл. печ. л. 8,25.
Уч.-изд. л. 6,0. Тираж 100 экз. Заказ № 1432.

Издательство Уральского университета
Редакционно-издательский отдел ИПЦ УрФУ
620049, Екатеринбург, ул. С. Ковалевской, 5
Тел.: 8(343)375-48-25, 375-46-85, 374-19-41
E-mail: rio@urfu.ru

Отпечатано в Издательско-полиграфическом центре УрФУ
620075, Екатеринбург, ул. Тургенева, 4
Тел.: 8(343) 350-56-64, 350-90-13
Факс: 8(343) 358-93-06
E-mail: press-urfu@mail.ru