# Глава 2. Отображения и их свойства

## §2.1. Соответствия, отображения, функции

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

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

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

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

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

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

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

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

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

**Определение 2.1.3.** Соответствие $q$ называется *функциональным* (или *однозначным*), если образом любого элемента $x \in D(q)$ является единственный элемент $y \in E(q)$, что обычно записывается как $q: x \mapsto y$ или $q(x) = y$. Соответствие $q$ между множествами $X$ и $Y$ называется *взаимно однозначным* или *биективным* (*биекцией*, иногда 1-1 *соответствием*), если оно всюду определено, сюръективно и инъективно. Однозначное отображение называется *функ-*

*цией*. Функция называется *инъективной*, если различным $x_1$ и $x_2$ из $X$ соответствуют различные $y_1$ и $y_2$ из $Y$, и *сюръективной*, если она сюръективна как соответствие. Функция называется *биективной*, если она одновременно инъективна и сюръективна.

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

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

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

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

где $Q^{-1} \subseteq Y \times X$. Геометрическое представление обратного соответствия получается путем изменения направления стрелок в геометрическом представлении прямого соответствия. Отсюда следует, что обратным соответствием для обратного соответствия будет прямое соответствие:

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

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

Перечислим основные способы задания функций.

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

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

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

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

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

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

Для вычисления $(n+1)!$ при $n \in \mathbf{N}$ требуется $n-1$ умножение, то есть число вычислительных шагов увеличивается с ростом аргумента.

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

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

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

Аналогично по индукции определяется композиция $n$ отображений для любого натурального числа $n \geq 2$.

Для обратной функции удобно использовать еще одно определение.

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

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

**Теорема 2.1.1 (критерий существования обратной функции).** Функция $f: X \to Y$ имеет обратную тогда и только тогда, когда $f$ – биекция.

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

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

**Свойства функций и их композиций**

**1.** Композиция сюръективных функций сюръективна.

**2.** Композиция инъективных функций инъективна.

**3.** Композиция биективных функций биективна.

**4.** Композиция функций в общем случае не коммутативна.

**5.** Композиция функций ассоциативна.

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

**7.** Обратная к биекции функция сама является биекцией.

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

## Примеры

**1.** Выписать графики всех соответствий между множествами $X = \{1, 2\}$ и $Y = \{3, 5\}$. Какие из соответствий являются отображениями, сюръективными, функциональными, инъективными соответствиями? Какие из отображений являются функциями? Указать инъективные, сюръективные и биективные функции.

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

Отображениями являются соответствия $q_6$–$q_9$, $q_{11}$–$q_{15}$, поскольку $D(q_i) = X$, $i = \overline{6,9}$ и $i = \overline{11,15}$. Сюръективными соответствиями являются $q_5$, $q_7$, $q_8$, $q_{10}$–$q_{15}$, так как $E(q_i) = Y$, $i = 5, 7, 8$ и $i = \overline{10,15}$. Функциональными соответствиями являются $q_1$–$q_4$, $q_6$–$q_9$, поскольку только они однозначны. Инъективные соответствия согласно определению 2.1.2: $q_1$–$q_4$, $q_7$, $q_8$. Функциями являются $q_6$–$q_9$, поскольку только они являются функциональными отображениями. Инъективными, сюръективными и биективными функциями согласно определению 2.1.3 являются $q_7$ и $q_8$.

**2.** Исследовать свойства функции $f\colon \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$, где $p$ – простое число, $f(\bar{a}) = \bar{a}^p$. Получить формулы бинома Ньютона $(\bar{a} + \bar{b})^{28}$, $(\bar{a} + \bar{b})^{44}$ и $(\bar{a} + \bar{b})^{75}$ в $\mathbf{Z}/11\mathbf{Z}$.

При $\bar{a} \neq \bar{0}$ $(a, p) = 1$, поэтому $\bar{a}^{p-1} = \bar{1}$ согласно малой теореме Ферма (теореме 1.6.4). Значит, $\bar{a}^p = \bar{a}$ для $\forall\, \bar{a} \in \mathbf{Z}/p\mathbf{Z}$ и $f = e_{\mathbf{Z}/p\mathbf{Z}}$. Таким образом, $(\bar{a} + \bar{b})^p = \bar{a} + \bar{b}$ для $\forall\, \bar{a}, \bar{b} \in \mathbf{Z}/p\mathbf{Z}$.

Используя теорему 1.1.1 о делении с остатком и свойства функции $f$, получим следующие формулы бинома Ньютона в $\mathbf{Z}/11\mathbf{Z}$:

$$(\bar{a} + \bar{b})^{28} = (\bar{a} + \bar{b})^{11\cdot 2+6} = (\bar{a} + \bar{b})^8 = \bar{a}^8 + \bar{8}\bar{a}^7\bar{b} + \overline{8\cdot 7/2}\bar{a}^6\bar{b}^2 + \overline{8\cdot 7\cdot 6/(2\cdot 3)}\bar{a}^5\bar{b}^3 +$$
$$+ \overline{8\cdot 7\cdot 6\cdot 5/(2\cdot 3\cdot 4)}\bar{a}^4\bar{b}^4 + \overline{8\cdot 7\cdot 6/(2\cdot 3)}\bar{a}^3\bar{b}^5 + \overline{8\cdot 7/2}\bar{a}^2\bar{b}^6 + \bar{8}\bar{a}\bar{b}^7 + \bar{b}^8 = \bar{a}^8 + \bar{8}\bar{a}^7\bar{b} +$$
$$+ \bar{6}\bar{a}^6\bar{b}^2 + \bar{a}^5\bar{b}^3 + \bar{4}\bar{a}^4\bar{b}^4 + \bar{a}^3\bar{b}^5 + \bar{6}\bar{a}^2\bar{b}^6 + \bar{8}\bar{a}\bar{b}^7 + \bar{b}^8;$$

$$(\bar{a} + \bar{b})^{44} = (\bar{a} + \bar{b})^{11\cdot 4} = (\bar{a} + \bar{b})^4 = \bar{a}^4 + \bar{4}\bar{a}^3\bar{b} + \bar{6}\bar{a}^2\bar{b}^2 + \bar{4}\bar{a}\bar{b}^3 + \bar{b}^4;$$

$$(\bar{a} + \bar{b})^{75} = (\bar{a} + \bar{b})^{11\cdot 6+9} = (\bar{a} + \bar{b})^{15} = (\bar{a} + \bar{b})^{11+4} = (\bar{a} + \bar{b})^5 = \bar{a}^5 + \bar{5}\bar{a}^4\bar{b} + \overline{10}\bar{a}^3\bar{b}^2 +$$
$$+ \overline{10}\bar{a}^2\bar{b}^3 + \bar{5}\bar{a}\bar{b}^4 + \bar{b}^5.$$

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

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

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

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

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

$f(x) = f_4(f_3(f_2(f_1(x)))) = f_4f_3f_2f_1(x)$, $D(f) = D(f_1) = \mathbf{R}\backslash\{1\}$, $E(f) = E(f_4f_3f_2f_1) = \mathbf{R}_{\geq 1}$.

**4.** $f: \mathbf{R} \to \mathbf{R}$, $g: \mathbf{R} \to \mathbf{R}$, где $f(x) = \sin x$, $g(x) = \sqrt{x^2 - 5x + 9}$. Доказать что композиция функций $f$ и $g$ не коммутативна.

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

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

$fg(x) = \sin\sqrt{x^2 - 5x + 9}$, при $x = 0$ $gf(0) = \sin 3 \neq 3$, поскольку $|\sin x| \leq 1$.

Итак, $gf \neq fg$.

**5.** Заданы три вещественных функции: $f(x) = 2x - 3$, $g(x) = x^3 - 8$, $h(x) = 2^{x^2+16x}$.

**1)** Найти заданные композиции функций: $fgh$, $hfg$, $ffg$.

**2)** Являются ли $f$, $g$, $h$ инъекциями, сюръекциями, биекциями на $\mathbf{R}$?

**3)** Найти обратные функции к $f$, $g$, $h$. Если функции со своими областями определения обратных не имеют, то найти обратные функции к их сужениям.

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

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

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

$$ffg(x) = 2(fg(x)) - 3 = 2(2x^3 - 19) - 3 = 4x^3 - 41.$$

**2)** Пусть $x_1, x_2 \in \mathbf{R}$, $x_1 \neq x_2$, тогда $2x_1 - 3 \neq 2x_2 - 3$, иначе приходим к противоречию. Следовательно, $f$ – инъекция на $\mathbf{R}$. Пусть $\forall\, y \in \mathbf{R}$, тогда уравнение $2x - 3 = y$ разрешимо относительно $x$ и $x = (y + 3)/2 = f^{-1}(y)$. Значит, $f$ – сюръекция на $\mathbf{R}$. Итак, $f$ – биекция на $\mathbf{R}$.

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

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

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

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

$2^{x^2+16x} = y$, откуда $x^2 + 16x = \log_2 y$. $D/4 = 64 + \log_2 y \geq 0$ при $y \geq 2^{-64}$, поэтому $E(h) = D(h^{-1}) = [2^{-64}; +\infty)$ и $x_{1,2} = -8 \pm \sqrt{\log_2 y + 64}$. Отображение $h^{-1}(x) = -8 \pm$

$\pm\sqrt{log_2 x+64}$ не функционально, так как каждому $x \in D(h^{-1})$, $x \neq 2^{-64}$, ставит в соответствие два различных значения. Но отображения $h_1^{-1}(x) = -8 + \sqrt{log_2 x+64}$ и $h_2^{-1}(x) = -8 - \sqrt{log_2 x+64}$, $D(h_1^{-1}) = D(h_2^{-1}) = [2^{-64}; +\infty)$, являются функциями, обратными соответственно к сужениям функции $h$ на множества $[-8; +\infty) = D(h_1) = E(h_1^{-1})$ и $(-\infty; -8] = D(h_2) = E(h_2^{-1})$.

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

Если $f^{-1}$ существует, то $f^{-1}: V_3(\mathbf{Z}/26\mathbf{Z}) \to V_3(\mathbf{Z}/26\mathbf{Z})$, где $f^{-1}(\bar{c}) = A^{-1} \cdot \bar{c}$. Таким образом, функция обратима тогда и только тогда, когда существует $A^{-1} \in M_3(\mathbf{Z}/26\mathbf{Z})$, для чего необходимо и достаточно, чтобы определитель матрицы $det(A)$ был обратимым классом вычетов в $\mathbf{Z}/26\mathbf{Z}$. $det(A) = \overline{11}$:

$$11 \cdot 23 \cdot 1 + 5 \cdot 7 \cdot 19 + 2 \cdot 25 \cdot 22 - 19 \cdot 23 \cdot 22 - 7 \cdot 25 \cdot 11 - 5 \cdot 2 \cdot 1 \equiv$$
$$\equiv -11 \cdot 3 - 9 \cdot 7 - 44 + 7 \cdot 3 \cdot 4 + 7 \cdot 11 - 10 = -33 - 63 - 54 + 84 + 77 =$$
$$= -150 + 161 = 11 \pmod{26}.$$

Поскольку $(11, 26) = 1$, то по теореме 1.6.1 $det(A)$ обратим в $\mathbf{Z}/26\mathbf{Z}$. Вычислим $det(A)^{-1} = det(A^{-1})$, используя соотношение Безу для чисел 1, 11 и 26 и расширенный алгоритм Евклида.

$$26 = 11 \cdot 2 + 4,\ r_1 = 4 = 26 - 11 \cdot 2;$$
$$11 = 4 \cdot 2 + 3,\ r_2 = 3 = 11 - 4 \cdot 2 = 11 - 26 \cdot 2 + 11 \cdot 4 = 11 \cdot 5 - 26 \cdot 2;$$
$$4 = 3 \cdot 1 + 1,\ r_3 = 1 = 4 - 3 = 26 - 11 \cdot 2 + 26 \cdot 2 - 11 \cdot 5 = 26 \cdot 3 - 11 \cdot 7;$$
$$3 = 1 \cdot 3 + 0,\ r_4 = 0.$$

$(11, 26) = r_3 = 1 = 26 \cdot 3 + 11 \cdot (-7)$. Тогда $11 \cdot (-7) \equiv 1 \pmod{26}$ и $det(A)^{-1} = \overline{11}^{-1} = \overline{-7} = \overline{26-7} = \overline{19}$. Итак, функция $f^{-1}$ существует и имеет указанный выше вид. Вычислим матрицу $A^{-1}$:

$$A^{-1} = \overline{19} \cdot \begin{pmatrix} \begin{vmatrix} 29 & 25 \\ 7 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & 19 \\ 7 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 19 \\ 23 & 25 \end{vmatrix} \\ -\begin{vmatrix} 5 & 25 \\ 22 & 1 \end{vmatrix} & \begin{vmatrix} 11 & 19 \\ 22 & 1 \end{vmatrix} & -\begin{vmatrix} 11 & 19 \\ 5 & 25 \end{vmatrix} \\ \begin{vmatrix} 5 & 23 \\ 22 & 7 \end{vmatrix} & -\begin{vmatrix} 11 & 2 \\ 22 & 7 \end{vmatrix} & \begin{vmatrix} 11 & 2 \\ 5 & 23 \end{vmatrix} \end{pmatrix} = \overline{19} \cdot \begin{pmatrix} \overline{-3+7} & \overline{-(2+49)} & \overline{-2-21} \\ \overline{-(5+22)} & \overline{11-28} & \overline{-(-11+35)} \\ \overline{35-12} & \overline{-(77+8)} & \overline{-33-10} \end{pmatrix} =$$
$$= \overline{-7} \cdot \begin{pmatrix} \bar{4} & \bar{1} & \bar{3} \\ \overline{-1} & \bar{9} & \bar{2} \\ \overline{-3} & \overline{-7} & \bar{9} \end{pmatrix} = \begin{pmatrix} \overline{-2} & \overline{-7} & \overline{-21} \\ \bar{7} & \overline{-11} & \overline{-14} \\ \overline{21} & \overline{23} & \overline{-11} \end{pmatrix} = \begin{pmatrix} \overline{24} & \overline{19} & \bar{5} \\ \bar{7} & \overline{15} & \overline{12} \\ \overline{21} & \overline{23} & \overline{15} \end{pmatrix}.$$

## Задачи

**1.** Выписать графики всех соответствий между множествами $X$ и $Y$. Какие из соответствий являются отображениями, сюръективными, функциональными, инъективными соответствиями? Какие из отображений являются функциями? Указать инъективные, сюръективные и биективные функции.

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

**2.** Получить формулы бинома Ньютона $(\bar{a} + \bar{b})^{38}$, $(\bar{a} + \bar{b})^{51}$ и $(\bar{a} + \bar{b})^{100}$ в $\mathbf{Z}/17\mathbf{Z}$.

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

**4.** $f: \mathbf{R}_{>0} \to \mathbf{R}$, $g: \mathbf{R}_{>0} \to \mathbf{R}$, где $f(x) = \log_2 x$, $g(x) = \log_3 x$. Доказать что композиция функций $f$ и $g$ не коммутативна.

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

**1)** Найти заданные композиции функций: $fgh$, $hfg$, $ffg$.

**2)** Являются ли $f$, $g$, $h$ инъекциями, сюръекциями, биекциями на $\mathbf{R}$?

**3)** Найти обратные функции к $f$, $g$, $h$. Если функции со своими областями определения обратных не имеют, то найти обратные функции к их сужениям.

**6.** $f: V_3(\mathbf{Z}/26\mathbf{Z}) \to V_3(\mathbf{Z}/26\mathbf{Z})$, где $f(\bar{c}) = A \cdot \bar{c}$, $A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{4} & \bar{5} & \bar{6} \\ \bar{7} & \bar{8} & \bar{0} \end{pmatrix} \in M_3(\mathbf{Z}/26\mathbf{Z})$. Обратима ли функция $f$? В случае положительного ответа найти обратную функцию $f^{-1}$.

## Ответы

**1. а)** $Q_0 = \{(\,)\} = \varnothing$, $Q_1 = \{(1, 3)\}$, $Q_2 = \{(2, 3)\}$, $Q_3 = \{(1, 3), (2, 3)\}$, $q_3$ – отображение, сюръективная функция, $q_1$, $q_2$ – сюръективные, функциональные, инъективные соответствия; **б)** $Q_0 = \{(\,)\} = \varnothing$, $Q_1 = \{(1, 3)\}$, $Q_2 = \{(1, 4)\}$, $Q_3 = \{(1, 3), (1, 4)\}$, $q_1$–$q_3$ – отображения, $q_3$ – сюръективное соответствие, $q_1$, $q_2$ – инъективные функции. **2.** $(\bar{a} + \bar{b})^{38} = (\bar{a} + \bar{b})^6 = \bar{a}^6 + \overline{6}\bar{a}^5\bar{b} + \overline{15}\bar{a}^4\bar{b}^2 + \overline{3}\bar{a}^3\bar{b}^3 + \overline{15}\bar{a}^2\bar{b}^4 + \overline{6}\bar{a}\bar{b}^5 + \bar{b}^6$; $(\bar{a} + \bar{b})^{51} = (\bar{a} + \bar{b})^3 = \bar{a}^3 + \overline{3}\bar{a}^2\bar{b} + \overline{3}\bar{a}\bar{b}^2 + \bar{b}^3$; $(\bar{a} + \bar{b})^{100} = (\bar{a} + \bar{b})^4 = \bar{a}^4 + \overline{4}\bar{a}^3\bar{b} + \overline{6}\bar{a}^2\bar{b}^2 + \overline{4}\bar{a}\bar{b}^3 + \bar{b}^4$. **3.** $f(x) = f_4 f_3 f_2 f_1(x)$, где $f_1(x) = 2x$, $f_2(x) = e^x$, $f_3(x) = 1 - x$, $f_4(x) = x^3$. **5. 1)** $D(fgh) = D(hfg) = D(ffg) = \mathbf{R}$, $fgh(x) = 2\left(-5arctg\left(4e^{5x} - 68\right) + 2\right)^9 - 7$, $hfg(x) = e^{5^{2(-5arctg(4x)+2)^9 - 7}} - 17$, $ffg(x) = 2\left(2(-5arctg(4x) + 2)^9 - 7\right)^9 - 7$; **2)** $f$ – биекция на $\mathbf{R}$, $g$, $h$ – инъекции, не сюръекции, не биекции на $\mathbf{R}$; **3)** $f^{-1}(x) = \sqrt[9]{(x + 7)/2}$, $D(f^{-1}) = \mathbf{R}$, $g^{-1}(x) = tg((2 - x)/5)/4$, $D(g^{-1}) = (-5\pi/2 + 2; 5\pi/2 + 2)$, $h^{-1}(x) = \log_5(\ln(x + 17))$, $D(h^{-1}) = (-16; +\infty)$. **6.** $f^{-1}: V_3(\mathbf{Z}/26\mathbf{Z}) \to V_3(\mathbf{Z}/26\mathbf{Z})$, где $f^{-1}(\bar{c}) = A^{-1} \cdot \bar{c}$, $det(A) =$

$= det(A^{-1}) = \bar{1},\ A^{-1} = \begin{pmatrix} \bar{4} & \overline{24} & \overline{23} \\ \overline{16} & \bar{5} & \bar{6} \\ \overline{23} & \bar{6} & \overline{23} \end{pmatrix}.$

## §2.2. Взаимно однозначное соответствие. Мощность множества. Конечные, счетные и континуальные множества

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

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

Очевидно, что $A \leftrightarrow B \ \& \ B \leftrightarrow C \Rightarrow A \leftrightarrow C$ – свойство транзитивности.

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

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

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

**Теорема 2.2.3.** Пусть $A_1,\ldots, A_n$ – конечные множества и $|A_i| = m_i,\ i = \overline{1,n}$. Тогда мощность множества $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2,\ldots, a_n) \mid a_i \in A_i,\ i = \overline{1,n}\}$ равна произведению мощностей множеств $A_1, A_2,\ldots, A_n$:

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

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

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

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

**Теорема 2.2.4.** Для любого конечного множества $A$, $|A| = n \in \mathbf{Z}_{\geq 0}$, число всех его подмножеств равно $2^n$, то есть $|P(A)| = 2^n$.

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

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

Любое бесконечное подмножество множества **N** счетно. Счетными являются множества **Z** и **Q**. Объединение конечного числа счетных множеств, объединение счетного множества конечных множеств и объединение счетного множества счетных множеств счетны.

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

**Теорема 2.2.5 (Г. Кантор).** Множество всех действительных чисел интервала (0; 1) несчетно.

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

Интервал (0; 1) может быть приведен во взаимно однозначное соответствие с полуинтервалами [0; 1), (0; 1], отрезком [0; 1], а также множествами $(a; b)$, $(a; b]$, $[a; b)$, $[a; b]$, где $a, b \in \mathbf{R}$, $a < b$, и всем множеством $\mathbf{R}$. $\mathbf{R}^2 \leftrightarrow \mathbf{R}$ и вообще $\mathbf{R}^n \leftrightarrow \mathbf{R}$ для любого $n \in \mathbf{N}$. В общем случае взаимно однозначное соответствие $f: (c; d) \to (a; b)$, $\forall\, a, b, c, d \in \mathbf{R}$, $a < b$, $c < d$, задается аналитически следующим образом:

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

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

## Примеры

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

Нетрудно видеть, что $\mathbf{R}^2$ равномощно множеству всех точек на действительной плоскости, $A$ равномощно множеству всех точек прямой $2x + y = 1$, $B$ – множеству всех точек прямой $x - y = 0$ на действительной плоскости (рис. 2.2.1). Поскольку коэффициенты при $x$ и $y$ у данных двух прямых не пропорциональны, прямые пересекаются на плоскости в единственной точке с координатами (1/3, 1/3). Для доказательства равномощности $\mathbf{R}^2$ и $A \times B$ достаточно показать равномощность множеств всех точек действительной плоскости и всех упорядоченных пар точек на прямых $2x + y = 1$ и $x - y = 0$.

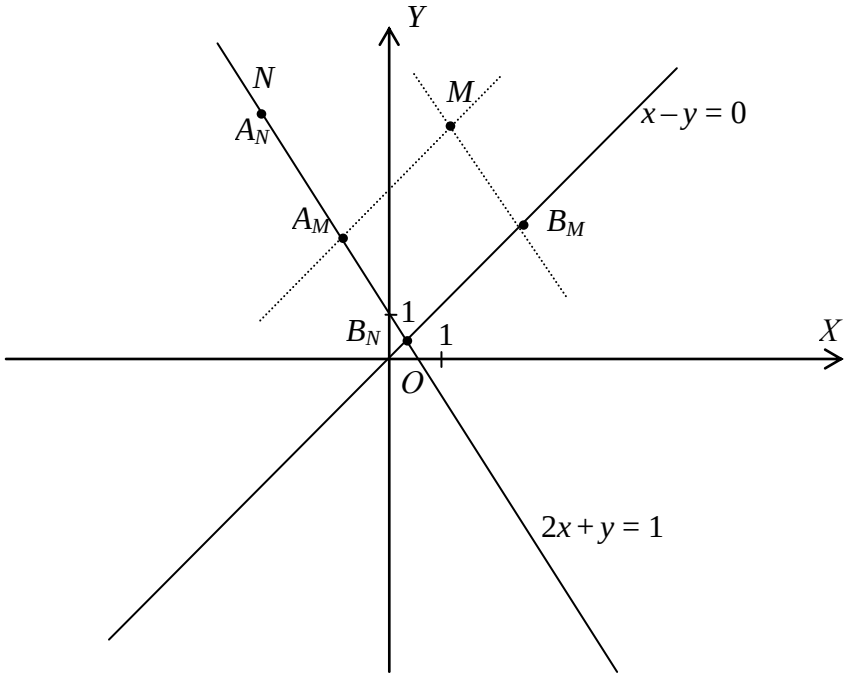


**Рис. 2.2.1**

Каждой точке $M$ на плоскости поставим в соответствие упорядоченную пару точек $(A_M, B_M)$ на прямых $2x + y = 1$ и $x - y = 0$, являющихся точками пересечения этих прямых с прямыми, проходящими через данную точку и парал-

лельными $x-y=0$ и $2x+y=1$ соответственно. Если точка $N$ принадлежит прямой $2x+y=1$ либо $x-y=0$, то первым (вторым) элементом пары точек на прямых будет сама данная точка, а вторым (первым) элементом пары – точка (1/3, 1/3) (см. рис. 2.2.1).

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

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

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

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

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

**1)** Поскольку $A=(A\cap B)\cup(A\setminus B)$ и $(A\cap B)\cap(A\setminus B)=\varnothing$, то получаем, что $|A|=|A\cap B|+|A\setminus B|$, откуда $|A\cap B|=|A|-|A\setminus B|$.

**2)** Так как $A\cup B=A\setminus B\cup B\setminus A\cup(A\cap B)$ и множества в правой части попарно не пересекаются, то $|A\cup B|=|A\setminus B|+|B\setminus A|+|A\cap B|$. Согласно п. 1) имеем $|A\setminus B|=|A|-|A\cap B|$ и $|B\setminus A|=|B|-|A\cap B|$, следовательно, $|A\cup B|=|A|-|A\cap B|+|B|-|A\cap B|+|A\cap B|=|A|+|B|-|A\cap B|$.

**3)** $A\triangle B=A\setminus B\cup B\setminus A$ и $(A\setminus B)\cap(B\setminus A)=\varnothing$. Тогда согласно равенствам из рассуждений п. 2) получаем $|A\triangle B|=|A\setminus B|+|B\setminus A|=|A|+|B|-2|A\cap B|$.

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

$\mathbf{N}^2=\{(m,n)\mid m,n\in\mathbf{N}\}$. Разобьем $\mathbf{N}^2$ на классы. К первому классу $N_2$ отнесем все пары чисел с минимальной суммой, равной 2. Таким образом, $N_2=\{(1,1)\}$. Ко второму классу $N_3$ отнесем все пары чисел с суммой 3: $N_3=\{(1,2),(2,1)\}$. Тогда $N_4=\{(1,3),(2,2),(3,1)\}$. В общем случае $N_i=\{(1,i-1),(2,i-2),(3,i-3),\ldots,(i-1,1)\}$, $i=2,3,\ldots$ Каждый класс $N_i$ содержит ровно $i-1$ пару. Упорядочим классы $N_i$ по возрастанию индексов $i$, а пары внутри класса – по возрастанию первого элемента и занумеруем получившуюся последовательность пар номерами 1, 2, 3,… Легко видеть, что если $m+n=i+1$, то пара $(m,n)$ получит номер $0+1+2+\ldots+(i-1)+m=(i-1)\cdot i/2+m$. Эта нумерация задает взаимно однозначное соответствие $\mathbf{N}^2\leftrightarrow\mathbf{N}$ и доказывает счетность $\mathbf{N}^2$.

**4.** Доказать, что при фиксированном $b\in\mathbf{R}_{>0}$ бесконечное множество равносторонних треугольников, в котором вершинами каждого треугольника являются середины сторон уже построенного треугольника (рис. 2.2.2), является счетным.

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

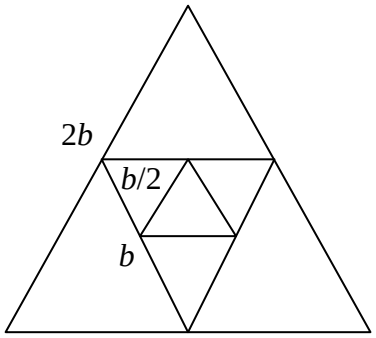


**Рис. 2.2.2**

Рассмотрим взаимно однозначное соответствие $f: T_b \to \mathbf{N}$, представленное на рис. 2.2.3.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $T_b$: … | $2^{-n}b$ | … | $2^{-2}b$ | $2^{-1}b$ | $b$ | $2b$ | $4b$ | … | $2^n b$ | … |
| | ↓ | | ↓ | ↓ | ↓ | ↓ | ↓ | | ↓ | |
| **N**: ... | $2n+1$ | ... | 5 | 3 | 1 | 2 | 4 | … | $2n$ | … |

**Рис. 2.2.3**

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

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

**5.** Показать, что множество всех вещественных чисел интервала $(0; +\infty)$ – континуальное множество.

Известно, что **R** – континуальное множество. Рассмотрим функциональное соответствие $f: \mathbf{R} \to (0; +\infty)$, где $f(x) = e^x$, $\forall\, x \in \mathbf{R}$. Тогда для $\forall\, y \in (0; +\infty)$ существует единственный $x \in \mathbf{R}$, такой, что $f(x) = y$, $x = \ln y$. Итак, $\mathbf{R} \leftrightarrow (0; +\infty)$.

**6.** Доказать, что множество всех точек гиперболы $y = 1/x$ (рис. 2.2.4) на действительной плоскости имеет мощность континуум.

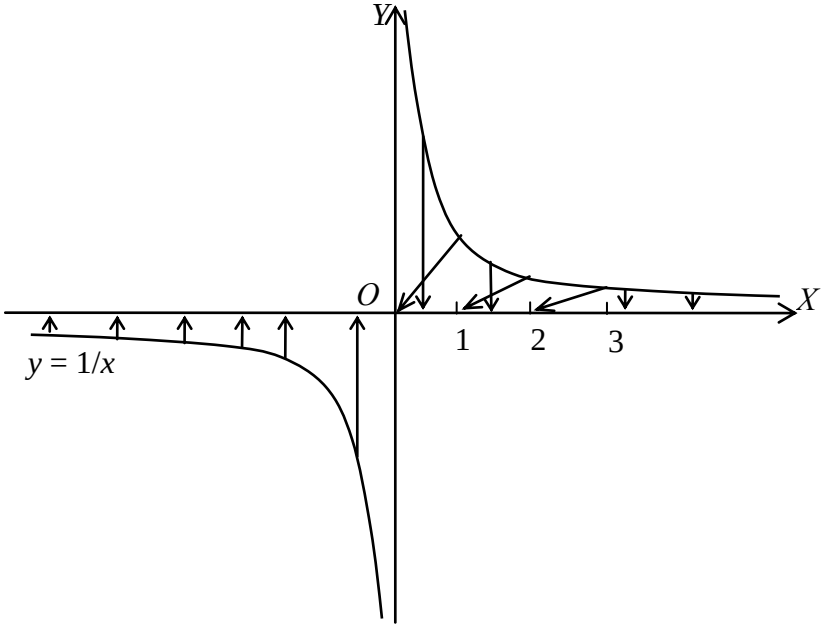


**Рис. 2.2.4**

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

$$f((x, 1/x)) = \begin{cases} x,\ x \in \mathbf{R} \setminus \mathbf{Z}_{\geq 0}; \\ x-1,\ x \in \mathbf{N}. \end{cases}$$

Функция $f: \Gamma \to \mathbf{R}$ действительно является взаимно однозначным соответствием. Графическая иллюстрация представлена на рис. 2.2.4. Итак, $\Gamma \leftrightarrow \mathbf{R}$. Поскольку $\mathbf{R}$ – континуальное множество, $\Gamma$ – также континуальное множество.

**7.** Доказать, что равномощны множества $\mathbf{C}\backslash\{0\}$ и $(0; +\infty) \times (-2\pi;\ \pi)$.

$(-2\pi;\ \pi) \leftrightarrow (0; 2\pi)$, взаимно однозначное соответствие задается согласно (2.2.1) функцией $f(x) = 2\pi(x + 2\pi)/3\pi = 2(x + 2\pi)/3$, $f: (-2\pi;\ \pi) \to (0; 2\pi)$.

Следующая функция $g: (0; 2\pi) \to [0; 2\pi)$ является биекцией и позволяет установить, что $(0; 2\pi) \leftrightarrow [0; 2\pi)$.

$$g(x) = \begin{cases} x,\ x \neq 0,\underbrace{5\ldots5}_{n},\ n \in \mathbf{N}; \\ 0,\ x = 0{,}5; \\ 0,\underbrace{5\ldots5}_{n},\ x = 0,\underbrace{5\ldots5}_{n+1},\ n \in \mathbf{N}. \end{cases}$$

$(-2\pi;\ \pi) \leftrightarrow [0; 2\pi)$, поскольку $gf$ – биекция. Тогда $(0; +\infty) \times (-2\pi;\ \pi) \leftrightarrow$ $\leftrightarrow (0; +\infty) \times [0; 2\pi)$, так как взаимно однозначное соответствие задается функцией $h$: $(0; +\infty) \times (-2\pi;\ \pi) \to (0; +\infty) \times [0; 2\pi)$, где $h((x, y)) = (x, gf(y))$.

Для $\forall\, z \in \mathbf{C}\backslash\{0\}$ $z = \rho e^{i\varphi}$, где $\rho \in (0; +\infty)$, $\varphi \in [0; 2\pi)$ определены однозначно, – показательная форма записи комплексных чисел. Поэтому функция $q$ – биекция $(0; +\infty) \times [0; 2\pi)$ на $\mathbf{C}\backslash\{0\}$, где $q((\rho, \varphi)) = \rho e^{i\varphi} = z$.

Таким образом, $(0; +\infty) \times (-2\pi;\ \pi) \leftrightarrow \mathbf{C}\backslash\{0\}$, поскольку $qh$ – биекция.

**8.** Доказать равномощность множеств $X$ и $Y$, построив взаимно однозначные соответствия между ними.

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

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

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

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

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

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

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

Тогда функция $f\colon X \to Y$ является биекцией, поэтому $X \leftrightarrow Y$:

$$f(x) = \left[\begin{array}{l} g(x),\ x \in [-3;\ 1]; \\ h(x),\ x \in (1;\ 2]. \end{array}\right.$$

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

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

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

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

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

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

$[-2;\ 4] \leftrightarrow [-2;\ 1]$, так как функция $g$, построенная по формуле (2.2.1), является биекцией:

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

Функция $f$, построенная при помощи $g$ и двух последовательностей сдвигов, задает взаимно однозначное соответствие между $X$ и $Y$, поэтому $X \leftrightarrow Y$:

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

**г)** $X = [-3;\ 2]$, $Y = \mathbf{R}$.

$[-3;\ 2] \leftrightarrow [-\pi/2;\ \pi/2]$, так как функция $g_1$, построенная по формуле (2.2.1), является биекцией:

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

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

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

**Задачи**

**1.** Задает ли функция $f$ взаимно однозначное соответствие между множествами?

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

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

**2.** Доказать равномощность множеств $X$ и $Y$, построив взаимно однозначные соответствия между ними:

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

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

**в)** $X = [4; 9] \cup \{10\}$, $Y = \mathbf{R}$ Указание: использовать метод решения примера 8, г).

**Ответы**

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

## §2.3. Классические шифры

**Примеры**

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

OSZJX FXRF YOQJSZ RAYFJ

требуется восстановить отправленное сообщение, если известно, что для использованного (неизвестного) ключа результат шифрования не зависит от порядка выполнения указанных этапов для любого отправленного сообщения.

Пробелы разделяют слова, при зашифровывании пробел остается пробелом. Известно также, что в результате зашифровывания «A» $\mapsto$ «F».

*Решение*.

Занумеруем буквы латинского алфавита от 0 до 23, как указано в таблице 2.3.1.

**Таблица 2.3.1**

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

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

Итак, имеем следующее исходное сообщение:

INTER ARMA SILENT MUSAE

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

*Ответ*. «INTER ARMA SILENT MUSAE».

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

ФВМЁЖТИВФЮ.

*Решение*.

Занумеруем буквы русского алфавита от 0 до 32. Все операции будут выполняться в $\mathbf{Z}/33\mathbf{Z}$. Легко видеть, что $f(x)=(x^2+3x+1)(x^4+x+1)+2$. Отсюда $f(x_1) = f(x_2) = 2$, где $x_1$, $x_2$ – корни $x^2+3x+1$. Итак, мы имеем классический

шифр Цезаря с циклическим сдвигом на 2 позиции вправо. Для расшифровывания сообщения нужно каждую букву циклически сдвинуть на 2 позиции влево (см. таблицу 2.3.2).

**Таблица 2.3.2**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Буква ш. с. | Ф | В | М | Ё | Ж | Т | И | В | Ф | Ю |
| Порядковый номер буквы ш. с. | 21 | 2 | 13 | 6 | 7 | 19 | 9 | 2 | 21 | 31 |
| Порядковый номер буквы и. с. | 19 | 0 | 11 | 4 | 5 | 17 | 7 | 0 | 19 | 29 |
| Буква и. с. | Т | А | К | Д | Е | Р | Ж | А | Т | Ь |

*Ответ*. «ТАКДЕРЖАТЬ».

**3.** Зашифровывание сообщения на русском языке в алфавите без букв «Ё», «Й», «Ъ» осуществляется следующим образом. Пусть сообщение состоит из $n$ букв. Выбирается ключ $K$ – некоторая последовательность из $n$ букв приведенного выше алфавита. Зашифровывание каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Фактически, это шифр Виженера.

Дешифруйте «РБЫНПТСИТСРРЕЗОХ», если известно, что ключевая последовательность не содержит никаких букв, кроме «Б», «В», «Г».

*Решение*.

Каждая буква шифрованного сообщения расшифровывается в трех вариантах, предполагая последовательно, что соответствующая буква шифрованной последовательности есть «Б», «В» или «Г».

**Таблица 2.3.3**

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Шифрованное сообщение | Р | Б | Ы | Н | П | Т | С | И | Т | С | Р | Р | Е | З | О | Х |
| вариант Б | П | А | Щ | М | О | С | Р | З | С | Р | П | П | Д | Ж | Н | Ф |
| вариант В | О | Я | Ш | Л | Н | Р | П | Ж | Р | П | О | О | Г | Е | М | У |
| вариант Г | Н | Ю | Ч | К | М | П | О | Е | П | О | Н | Н | В | Д | Л | Т |

Выбирая из каждой колонки полученной таблицы 2.3.3 ровно по одной букве, находим осмысленное сообщение «НАШКОРРЕСПОНДЕНТ», которое и является искомым.

Можно было найти «НАШМОРОЗПОНОГЕМУ». Если предположить искажение в шифрованном сообщении (в качестве 11-й буквы была бы принята не «Р», а «П»), то получим «НАШМОРОЗПОМОГЕМУ». Число всех различных

вариантов сообщений без ограничений на осмысленность равно $3^{16}$ или 43046721, то есть более 40 миллионов!

*Ответ*. «НАШКОРРЕСПОНДЕНТ».

**4.** Зашифровывание сообщения на русском языке в алфавите без букв «Ё», «Й», «Ъ» и с добавлением знака пробел «_» осуществляется следующим образом. Пусть сообщение состоит из $n$ букв. Выбирается ключ $K$ – некоторая периодическая последовательность из $n$ букв приведенного выше алфавита с периодом 3, в периоде которой все буквы различны. Зашифровывание каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 31, что и эта сумма. Это шифр Виженера с периодической ключевой последовательностью.

Дешифруйте «РБЫВЛРУСЗФРРРЕЗРУ», если известно, что ключевая последовательность не содержит никаких букв, кроме «Б», «В», «Г».

*Решение*.

Количество различных вариантов ключевых периодических последовательностей равно 3! = 6. Из каждой колонки таблицы 2.3.4, построенной по тому же принципу, что и в предыдущем примере, выбираем ровно по одной букве, учитывая вид ключевой периодической последовательности.

**Таблица 2.3.4**

| Шифрованное сообщение | Р | Б | Ы | В | Л | Р | У | С | З | Ф | Р | Р | Р | Е | З | Р | У |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| вариант Б | П | А | Щ | Б | К | П | Т | Р | Ж | У | П | П | П | Д | Ж | П | Т |
| вариант В | О | _ | Ш | А | И | О | С | П | Е | Т | О | О | О | Г | Е | О | С |
| вариант Г | Н | Я | Ч | _ | З | Н | Р | О | Д | С | Н | Н | Н | В | Д | Н | Р |

Далее совершаем перебор шести вариантов, чтобы в качестве исходного сообщения получилось выражение, имеющее смысл:

«БВГ»: «П_ЧБИН…» – нет смысла; «БГВ»: «ПЯШБЗО…» – нет смысла;

«ВБГ»: «ОАЧАК…» – нет смысла; «ВГБ»: «ОЯЩАЗПСО…» – нет смысла;

«ГБВ»: «НАШ_КОРРЕСПОНДЕНТ» – есть смысл;

«ГВБ»: «Н_Щ_ИП…» – нет смысла.

*Ответ*. Ключевая последовательность – «ГБВ», исходное сообщение – «НАШ_КОРРЕСПОНДЕНТ».