В. В. Расин

ЛЕКЦИИ ПО АЛГЕБРЕ

Элементы теории множеств. Натуральные и целые числа. Неравенства. Отображения множеств. Числовые функции

Учебное пособие

Екатеринбург
2011

Министерство науки и образования
Российской Федерации
Уральский федеральный университет
Специализированный учебно-научный центр

В. В. Расин

ЛЕКЦИИ ПО АЛГЕБРЕ

Элементы теории множеств. Натуральные и целые числа. Неравенства. Отображения множеств. Числовые функции

Учебное пособие

Екатеринбург
2011

УДК 512(075.8)
Р 241

Подготовлено на кафедре математики
СУНЦ УрФУ

Расин В. В. Лекции по алгебре: Натуральные и целые числа. Неравенства. Отображения множеств. Числовые функции: Учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2011. 148 с.

В пособии последовательно и подробно обсуждаются свойства натуральных и целых чисел. Большое внимание уделено одному из важнейших понятий современной математики – понятию отображения множеств. Излагается материал, связанный с равномощностью множеств, счетными и несчетными множествами.

Для школьников, учителей и студентов.

Рецензенты: кафедра математики Института развития регионального образования; *А.Г.Гейн*, профессор кафедры алгебры и дискретной математики Уральского государственного университета

Предисловие

Учебное пособие написано на основе лекций, неоднократно читавшихся автором учащимся десятых физико-математических классов Специализированного учебно-научного центра Уральского государственного университета. Оно включает в себя шесть глав: элементы теории множеств (глава 1), натуральные числа (глава 2), целые числа (глава 3), неравенства (глава 4), отображения множеств (глава 5) и числовые функции (глава 6).

В первой главе рассказано о понятии множества и таких теоретико-множественных операциях как объединение, пересечение, разность и прямое (декартово) произведение множеств. Кроме того, обсуждаются свойства этих операций. Знакомство с теоретико-множественными обозначениями полезно при изучении углубленного курса математики. Разумеется, в пособии эти обозначения последовательно используются.

Вторая глава посвящена множеству всех натуральных чисел $\mathbb{N}$. Сначала формулируются аксиомы Пеано. Эти аксиомы фиксируют некоторые свойства числа n', следующего за данным числом n. Далее показывается, что при помощи аксиом Пеано можно определить сложение и умножение двух натуральных чисел и доказать основные свойства этих операций. После этого вводится порядок на множестве всех натуральных чисел и изучаются его свойства. Используя в качестве примера множество $\mathbb{N}$, мы обсуждаем понятия линейно упорядоченного и вполне упорядоченного множеств и доказываем важную теорему о том, что множество всех натуральных чисел вполне упорядочено (теорема 2.1). Кроме того, мы

проверяем (см. раздел 2.5), что множество $\mathbb{N}$ может быть охарактеризовано в терминах порядка.

В третьей главе вводится в рассмотрение множество всех целых чисел $\mathbb{Z}$. Заметим, что здесь (на первых порах) уровень строгости изложения несколько снижен по сравнению со второй главой. Мы, по существу, уточняем известное школьнику понятие целого числа. Некоторые доказательства (например, доказательство ассоциативности сложения) опущены сознательно, дабы не делать изложение слишком громоздким. Здесь мы считаем целесообразным ввести понятие коммутативного кольца с единицей с тем, чтобы школьники начали привыкать к современной математической терминологии. Основой дальнейшего изложения является теорема о делении с остатком. Она позволяет ввести в кольце $\mathbb{Z}$ отношение делимости и получить основные свойства этого отношения. Поскольку на этом этапе появляется возможность ввести в рассмотрение простые числа, мы временно возвращаемся к изучению натуральных чисел и доказываем два важных утверждения: теорему Евклида о бесконечности множества всех простых чисел и теорему о каноническом разложении. Возвращаясь к кольцу $\mathbb{Z}$, мы вводим отношение сравнимости по модулю n и изучаем его свойства. После этого естественно ввести кольцо вычетов по модулю n и доказать, что в кольце вычетов по простому модулю для каждого ненулевого элемента существует обратный. Тем самым предоставляется возможность ввести еще одно важное алгебраическое понятие – понятие поля. Читатель, желающий изучить затронутые в первых двух главах вопросы более глубоко, может воспользоваться книгами [2], [3], [5]–[8].

Четвертая глава содержит сведения о некоторых классических неравенствах. Это прежде всего неравенства между средним геометрическим, средним арифметическим и средним квадратичным. Особое место в дальнейшем изложении занимает неравенство Бернулли. Мы доказываем это неравенство для рационального показателя, поскольку возведение в произвольную действительную степень еще не определено. Этот пробел будет устранен при изучении темы “Действительные числа” (см. [4]). В заключение этой главы вводится понятие среднего степенного порядка α для дан-

ных чисел и устанавливается, что для фиксированного множества положительных чисел их среднее степенное не убывает с ростом порядка. Полезный и интересный дополнительный материал о неравенствах можно найти в книге [1].

Пятая глава посвящена изучению отображений произвольных множеств. Хотя термины "отображение" и "функция" синонимичны, мы резервируем термин "функция" для обозначения числовых функций. Здесь рассматриваются основные типы отображений (инъективные, сюръективные и биективные) и вводятся важные понятия: композиции отображений и отображения, обратного к данному. Понятие биективного отображения естественным образом приводит к понятию равномощности множеств. Как обычно, сначала изучаются счетные множества, т.е. множества, равномощные множеству всех натуральных чисел. Затем доказывается теорема Кантора-Бернштейна и приводятся примеры несчетных множеств.

В шестой главе продолжается изучение отображений для случая числовых функций. Содержание этой главы в целом стандартно и не нуждается в пояснениях. Отметим лишь следующее. Во-первых, мы посчитали естественным наряду с обычным набором свойств функций (четность, нечетность, монотонность, периодичность) ввести в рассмотрение и свойство функции быть выпуклой (вогнутой) вниз на промежутке. В связи с этим важно отметить, что для степенной функции $y = x^r$, $x > 0$, ее выпуклость вниз (при $r > 1$ или $r < 0$) или вверх (при $0 < r < 1$) может быть установлена элементарными средствами, поскольку является простым следствием из неравенства Бернулли. Во-вторых, здесь даются геометрические определения гиперболы и параболы и доказываются теоремы о том, что графики функций $y = ax^2$ ($a \neq 0$) и $y = k/x$ ($k \neq 0$) являются соответственно параболой и гиперболой.

Автор выражает глубокую признательность В. А. Баранскому, М. В. Волкову и А. Г. Гейну, прочитавшим рукопись и высказавшим замечания, способствовавшие ее улучшению.

1. Элементы теории множеств

1.1. Понятие множества. Операции над множествами

В конце девятнадцатого столетия трудами немецкого математика Г. Кантора (1845–1918) была создана теория множеств. С тех пор теоретико-множественный подход с успехом применяется во всех без исключения областях математики. Можно сказать, что язык теории множеств является универсальным языком современной математики. Нашей ближайшей целью является изучение этого языка.

Понятие множества является одним из основных понятий современной математики. Кантор описывал это понятие следующим образом: “Множество – это любое собрание определенных и различимых между собой объектов нашей интуиции или нашей мысли, рассматриваемое как единое целое”. Это описание, разумеется, не является определением. Однако, в нем содержится два следующих важных момента. Во-первых, объекты, составляющие множество, могут иметь какую угодно природу. Во-вторых, само множество полностью определяется составляющими его объектами. Заметим, что синонимами термина “множество” являются термины “совокупность”, “семейство”и др.

Множества обозначаются большими латинскими буквами. Каждое множество состоит из объектов, называемых элементами этого множества. Тот факт, что x является элементом множества X принято обозначать так: $x \in X$. Если же y не является элементом множества X, то пишут $y \notin X$. Для обозначения конечных множеств, содержащих небольшое число элементов, обычно используют фигурные скобки. А именно, запись $\{x_1, x_2, \ldots, x_n\}$ обозначает множество, все элементы которого заключены в фигурные скобки. Например, равенство $A = \{1, 3, 2\}$ означает, что множество X состоит из первых трех натуральных чисел. Высказывание $1 \in A$ является истинным, а высказывание $0 \in A$ ложно.

Два множества A и B называются *равными*, если они состоят из одних и тех же элементов. Иными словами, $x \in A$ тогда и только тогда, когда $x \in B$.

Из этого определения вытекает, что множество не зависит от

того, в каком порядке записаны его элементы. Например, выполнены равенства $\{x, y\} = \{y, x\}$, $\{z, x, y\} = \{y, z, x\}$ и т. п. Отметим также, что одноэлементное множество отлично от своего единственного элемента. Отсюда следуют неравенства $\{x, y\} \neq \neq \{\{x\}, y\}$, $\{x, y, z\} \neq \{\{x\}, \{y, z\}\}$.

Введенное выше обозначение непригодно как для конечных множеств, содержащих большое число элементов, так и для бесконечных множеств. Если для такого множества X известно свойство $P(x)$, которым обладают все элементы множества X и только эти элементы, то используют запись $X = \{x \mid P(x)\}$. Приведем примеры. Если $\mathbb{N}$ – это множество всех натуральных чисел, то множество $\mathbb{E}$ всех четных чисел можно описать следующим образом:

$$\mathbb{E} = \{n \mid n = 2k \text{ для некоторого } k \in \mathbb{N}\}.$$

Пусть $\mathbb{R}$, как обычно, обозначает множество всех действительных чисел, $a, b \in \mathbb{R}$, $a < b$. Тогда множество

$$[a; b] = \{x \mid x \in \mathbb{R} \text{ и } a \leqslant x \leqslant b\}$$

является отрезком с концами a, b.

Довольно часто возникает необходимость в использовании *пустого* множества, т. е. множества, не содержащего ни одного элемента. Например, пустым является множество

$$\{x \mid x \in \mathbb{R} \text{ и } x^2 + 1 = 0\}.$$

Для обозначения пустого множества используется знак $\emptyset$.

Пусть A и B – произвольные множества. Будем говорить, что A является *подмножеством* B (A *включено* в B, B *содержит* A), если каждый элемент множества A принадлежит множеству B. Запись $A \subseteq B$ обозначает, что A является подмножеством B. Отношение $\subseteq$, называемое отношением включения, обладает следующими свойствами:

1) $A \subseteq A$;

2) если $A \subseteq B$ и $B \subseteq A$, то $A = B$;

3) если $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$.

Свойства 1), 2), 3) называются соответственно рефлексивностью, антисимметричностью и транзитивностью отношения включения.

Пусть A – произвольное множество. Рассмотрим множество

$$\mathcal{P}(A) = \{X | X \subseteq A\}.$$

Элементами этого множества являются подмножества исходного множества A. Множество $\mathcal{P}(A)$ часто называют *булеаном* множества A.

Поскольку единственным подмножеством пустого множества является оно само, его булеан одноэлементен. Это означает, что $\mathcal{P}(\emptyset) = \{\emptyset\}$. Одноэлементное множество $\{a\}$ имеет два подмножества: пустое множество и себя самое; следовательно, $\mathcal{P}(\{a\}) = = \{\emptyset, \{a\}\}$. Легко понять, что для двухэлементного множества $\{a, b\}$ имеет место равенство $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Удобно считать, что все множества, возникающие при решении той или иной задачи, являются подмножествами некоторого множества, называемого *универсальным*. Например, при изучении планиметрии универсальным является множество всех точек плоскости. В дальнейшем будем считать, что все рассматриваемые множества содержатся в некотором универсальном множестве U.

Пусть A и B – произвольные множества. Определим следующие операции над множествами.

Объединением множеств A и B называется множество

$$A \cup B = \{x \,|\, x \in A \text{ или } x \in B\}.$$

Пересечением множеств A и B называется множество

$$A \cap B = \{x \,|\, x \in A \text{ и } x \in B\}.$$

Разностью множеств A и B называется множество

$$A \setminus B = \{x \,|\, x \in A \text{ и } x \notin B\}.$$

Дополнением к множеству A называется множество $\overline{A} = = U \setminus A$.

Займемся выяснением свойств введенных выше операций. Из определений объединения и пересечения вытекает двойное включение

$$A \cap B \subseteq A \subseteq A \cup B. \tag{1}$$

Выясним, когда в двойном включении (1) одно из включений превращается в равенство.

Предложение 1.1. *Пусть A и B – произвольные множества. Следующие условия эквивалентны:*

1) $A \subseteq B$;
2) $A = A \cap B$;
3) $B = A \cup B$.

Доказательство. 1) $\Rightarrow$ 2). Поскольку $A \cap B \subseteq A$, убедимся, что выполнено обратное включение. Пусть $a \in A$. Учитывая включение $A \subseteq B$, получаем, что $a \in B$. Следовательно, $a \in A \cap B$.

2) $\Rightarrow$ 3). Из (1) следует, что $B \subseteq A \cup B$. Проверим обратное включение $A \cup B \subseteq B$. Пусть $a \in A \cup B$. Тогда $a \in A$ или $a \in B$. Ясно, что необходимо рассмотреть первую возможнось, когда $a \in$ $\in A$. В силу равенства 2) имеем $a \in A \cap B$ и потому $a \in B$.

3) $\Rightarrow$ 1). Пусть $a \in A$. Тогда $a \in A \cup B$. Используя равенство 3), получаем, что $a \in B$.

В следующем утверждении перечислены основные свойства операций объединения, пересечения и дополнения.

Теорема 1.1. *Пусть A, B и C – произвольные множества. Тогда*

1. $A \cup B = B \cup A$;	1′. $A \cap B = B \cap A$;
2. $(A \cup B) \cup C =$ $= A \cup (B \cup C)$;	2′. $(A \cap B) \cap C =$ $= A \cap (B \cap C)$;
3. $A \cup (B \cap C) =$ $= (A \cup B) \cap (A \cup C)$;	3′. $A \cap (B \cup C) =$ $= (A \cap B) \cup (A \cap C)$;
4. $A \cup \emptyset = A$;	4′. $A \cap U = A$;
5. $A \cup \overline{A} = U$;	5′. $A \cap \overline{A} = \emptyset$.

Доказательство. Все десять равенств, перечисленных в этой теореме, проверяются однотипно. Мы убедимся в справедливости только равенства 3, оставив проверку остальных равенств читателю.

Для доказательства равенства двух множеств, как мы знаем, следует проверить, что каждое из этих множеств является подмножеством другого. Проверим сначала, что выполнено включение

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C). \qquad (2)$$

Пусть $a \in A \cup (B \cap C)$. Тогда $a \in A$ или $a \in B \cap C$. Если $a \in A$, то $a \in A \cup B$ и $a \in A \cup C$, откуда $a \in (A \cup B) \cap (A \cup C)$. Если же $a \in B \cap C$, то опять $a \in A \cup B$ и $a \in A \cup C$, и, следовательно, $a \in (A \cup B) \cap (A \cup C)$.

Убедимся теперь в справедливости включения

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C). \tag{3}$$

Пусть $a \in (A \cup B) \cap (A \cup C)$. Тогда $a \in A \cup B$ и $a \in A \cup C$. Рассмотрим две возможности: $a \in A$ и $a \notin A$. Если $a \in A$, то, очевидно, $a \in A \cup (B \cap C)$. Если же $a \notin A$, то из соотношений $a \in A \cup B$, $a \in A \cup C$ вытекает, что $a \in B$ и $a \in C$. Отсюда $a \in B \cap C$, и потому $a \in A \cup (B \cap C)$.

Равенства, перечисленные в теореме 1.1 обладают следующим важным свойством: любое теоретико-множественное равенство, справедливое для всех значений входящих в него множеств, является следствием этих десяти равенств. Мы не будем доказывать соответствующее утверждение, а лишь продемонстрируем использование равенств из теоремы 1.1 для доказательства следующих двух утверждений.

Предложение 1.2. *Пусть A и B – такие множества, что $A \cup B = U$ и $A \cap B = \emptyset$. Тогда $B = \overline{A}$.*

Доказательство. Используя равенства из теоремы 1.1, получаем

$$B = B \cup \emptyset = B \cup (A \cap \overline{A}) = (B \cup A) \cap (B \cup \overline{A}) = U \cap (B \cup \overline{A}) = B \cap \overline{A},$$

$$\overline{A} = \overline{A} \cup \emptyset = \overline{A} \cup (A \cap B) = (\overline{A} \cup A) \cap (\overline{A} \cup B) = U \cap (\overline{A} \cup B) = \overline{A} \cup B.$$

Отсюда видно, что $B = \overline{A}$.

Теорема 1.2. *Пусть A, B – произвольные множества. Тогда*

6. $\overline{\emptyset} = U$;	6′. $\overline{U} = \emptyset$;
7. $A \cup A = A$;	7′. $A \cap A = A$;
8. $A \cup U = U$;	8′. $A \cap \emptyset = \emptyset$;
9. $A \cup (A \cap B) = A$;	9′. $A \cap (A \cup B) = A$;
10. $\overline{A \cup B} = \overline{A} \cap \overline{B}$;	10′. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Доказательство. Мы проверим только равенства 6 – 10. Равенства $6'$ – $10'$ доказываются аналогично, и их проверка оставляется читателю в качестве упражнения.

Для проверки равенства 6 воспользуемся предложением 1.2. Положив $A = U$, $B = \emptyset$, мы видим, что условие предложения 1.2 выполнено. Отсюда $\overline{U} = \emptyset$.

Равенство 7 вытекает из следующей цепочки равенств

$$A = A \cup \emptyset = A \cup (A \cap \overline{A}) = (A \cup A) \cap (A \cup \overline{A}) = (A \cup A) \cap U = A \cup A.$$

Применяя равенство 7, получаем

$$A \cup U = A \cup A \cup \overline{A} = A \cup \overline{A} = U,$$

откуда следует равенство 8.

Для доказательства равенства 9 заметим, что

$$A = A \cap U = A \cap (B \cup \overline{B}) = (A \cap B) \cup (A \cap \overline{B}).$$

Объединяя первое и последнее множества этой цепочки с множеством $A \cap B$, нетрудно увидеть, что последнее множество цепочки не изменится. Отсюда сразу следует, что $A \cup (A \cap B) = A$.

Равенство 10 вытекает из предложения 1.2. В самом деле,

$$(A \cup B) \cup (\overline{A} \cap \overline{B}) = (A \cup B \cup \overline{A}) \cap (A \cup B \cup \overline{B}) =$$

$$= (B \cup U) \cap (A \cup U) = U \cap U = U.$$

$$(A \cup B) \cap (\overline{A} \cap \overline{B}) = (A \cap \overline{A} \cap \overline{B}) \cup (B \cap \overline{A} \cap \overline{B}) =$$
$$= (\overline{B} \cap \emptyset) \cup (\overline{A} \cap \emptyset) = \emptyset \cup \emptyset = \emptyset.$$

Таким образом,

$$(A \cup B) \cup (\overline{A} \cap \overline{B}) = U, \quad (A \cup B) \cap (\overline{A} \cap \overline{B}) = \emptyset.$$

Применяя предложение 1.2 к множествам $A \cup B$ и $\overline{A} \cap \overline{B}$, получаем, что $\overline{A} \cap \overline{B} = \overline{A \cup B}$.

Определим объединение и пересечение нескольких множеств. Пусть $A_1, A_2, \ldots, A_n$ – произвольные множества. Тогда

$$A_1 \cup A_2 \cup \ldots \cup A_n = \{x \,|\, x \in A_i \ \text{ для некоторого } \ i, 1 \leqslant i \leqslant n\},$$

$$A_1 \cap A_2 \cap \ldots \cap A_n = \{x \,|\, x \in A_i \ \text{ для всех } \ i, 1 \leqslant i \leqslant n\}.$$

Таким образом, объединение (пересечение) n данных множеств состоит из элементов, каждый из которых принадлежит хотя бы одному из этих множеств (всем множествам одновременно).

Для обозначения объединения и пересечения n множеств можно использовать более краткие обозначения $\bigcup\limits_{i=1}^{n} A_i$ и $\bigcap\limits_{i=1}^{n} A_i$, аналогичные обозначениям для суммы и произведения n чисел. Кроме того, если $I = \{1, 2, \ldots, n\}$ – множество, состоящее из первых n натуральных чисел, то вместо $\bigcup\limits_{i=1}^{n} A_i$ и $\bigcap\limits_{i=1}^{n} A_i$ можно использовать обозначения $\bigcup\limits_{i\in I} A_i$ и $\bigcap\limits_{i\in I} A_i$ соответственно. Используя эти обозначения, можно ввести объединение и пересечение произвольного семейства множеств.

Пусть I – произвольное непустое множество. Рассмотрим произвольные множества A_i, где i пробегает множество I. В таком случае будем говорить, что A_i образуют семейство множеств, индексированное множеством I. Тогда

$$\bigcup_{i\in I} A_i = \{x \,|\, x \in I \text{ для некоторого } i \in I\},$$

$$\bigcap_{i\in I} A_i = \{x \,|\, x \in I \text{ для любого } i \in I\}.$$

Тем самым определены объединение и пересечение любого (в том числе и бесконечного) семейства множеств.

Приведем примеры.

1. Пусть $A_i = [i; +\infty)$ – луч с началом в точке i. Тогда

$$\bigcup_{i\in\mathbb{Z}} A_i = \mathbb{R}, \qquad \bigcap_{i\in\mathbb{Z}} A_i = \emptyset.$$

2. Пусть $A_i = [1/i; 3 - 1/i]$, $i \in \mathbb{N}$. Тогда

$$\bigcup_{i\in\mathbb{N}} A_i = (0; 3).$$

Проверим это равенство. Поскольку $0 < 1/i$ и $3 - 1/i < 3$, имеем включение $[1/i; 3 - 1/i] \subseteq (0; 3)$. Отсюда вытекает, что

$$\bigcup_{i\in\mathbb{N}} A_i \subseteq (0; 3).$$

Проверим, что выполнено обратное включение. Пусть $x \in (0;3)$. Убедимся, что $x \in A_m$ для некоторого $m \in \mathbb{N}$. Решая двойное неравенство $1/m < x < 3 - 1/m$, получим $m > 1/x$ и $m > 1/(3-x)$. Ясно, что такое натуральное m всегда найдется. Таким образом, $x \in A_m$, и потому $x \in \bigcup\limits_{i\in\mathbb{N}} A_i$.

3. Пусть $A_i = (1 - 1/i; 2 + 1/i)$. Тогда

$$\bigcap_{i\in\mathbb{N}} A_i = [1;2].$$

Это равенство проверяется аналогично предыдущему. Проверка оставляется читателю в качестве упражнения.

Оказывается, на объединения и пересечения произвольных семейств множеств можно распространить законы дистрибутивности и законы де Моргана.

Предложение 1.3. *Пусть A – произвольное множество, B_i $(i \in I)$ – произвольное семейство множеств. Тогда*

1) $A \cap \bigcup\limits_{i\in I} B_i = \bigcup\limits_{i\in I}(A \cap B_i)$, 1′). $A \cup \bigcap\limits_{i\in I} B_i = \bigcap\limits_{i\in I}(A \cup B_i)$,

2) $\overline{\bigcup\limits_{i\in I} B_i} = \bigcap\limits_{i\in I} \overline{B_i}$, 2′). $\overline{\bigcap\limits_{i\in I} B_i} = \bigcup\limits_{i\in I} \overline{B_i}$.

Доказательство. Докажем равенство 1). Убедимся, что имеет место включение справа налево. Пусть i – произвольный элемент множества I. Тогда выполнены включения $A \cap B_i \subseteq A$ и $A \cap B_i \subseteq B_i$. Отсюда следуют включения

$$\bigcup_{i\in I}(A \cap B_i) \subseteq A, \qquad \bigcup_{i\in I}(A \cap B_i) \subseteq \bigcup_{i\in I} B_i,$$

и потому

$$\bigcup_{i\in I}(A \cap B_i) \subseteq A \cap \bigcup_{i\in I} B_i.$$

Проверим обратное включение. Пусть x – произвольный элемент множества $A \cap \bigcup\limits_{i\in I} B_i$. Тогда $x \in A$ и $x \in B_i$ для некоторого $i \in I$. Следовательно, $x \in A \cap B_i$, и потому $x \in \bigcup\limits_{i\in I}(A \cap B_i)$. Таким образом,

$$A \cap \bigcup_{i\in I} B_i \subseteq \bigcup_{i\in I}(A \cap B_i),$$

и равенство 1) доказано.

Перейдем к доказательству равенства 2). Если $x \in \overline{\bigcup\limits_{i\in I} B_i}$, то $x \notin \bigcup\limits_{i\in I} B_i$. Отсюда следует, что для любого $i \in I$ выполнено условие $x \notin B_i$, т. е. $x \in \overline{B_i}$, и потому $x \in \bigcap\limits_{i\in I} \overline{B_i}$. Тем самым проверено включение слева направо. Для проверки обратного включения достаточно убедиться в том, что приведенные выше рассуждения можно обратить.

Вторая пара равенств может быть доказана совершенно аналогично.

Пусть A – непустое множество, A_i $(i \in I)$ – произвольное семейство его непустых подмножеств. Семейство A_i $(i \in I)$ называется *разбиением* множества A, если выполнены условия:

a) $A = \bigcup\limits_{i\in I} A_i$,

b) $A_i \cap A_j = \emptyset$, если $i \neq j$.

Условия a) и b) означают, что каждый элемент множества A содержится в точности одном подмножестве из разбиения.

Приведем примеры разбиений.

1. Обозначим через A_i $(0 \leqslant i \leqslant 3)$ множество, состоящее из тех натуральных чисел, которые при делении на 4 дают в остатке число i. Ясно, что семейство из четырех множеств A_0, A_1, A_2, A_3 является разбиением множества $\mathbb{N}$ всех натуральных чисел.

2. Семейство полуинтервалов $[m; m+1)$ $(m \in \mathbb{Z})$ является разбиением множества $\mathbb{R}$ всех действительных чисел.

Понятие разбиения множества будет использовано нами при изучении отношений эквивалентности (см. разд. 1.3).

1.2. Прямое произведение множеств

Понятие прямого произведения двух множеств X и Y основывается на понятии упорядоченной пары (x, y) элементов $x \in X$, $y \in Y$. Что же означает прилагательное “упорядоченная” применительно к паре элементов x, y? Прежде всего отметим, что неупорядоченые пары элементов мы, по существу, уже рассматривали. А именно, если $x \in X$, $y \in Y$, то множество $\{x, y\}$ часто называют неупорядоченной парой элементов x, y. Термин “неупорядоченная

пара" подчеркивает тот факт, что $\{x, y\} = \{y, x\}$, т. е. от перемены мест, занимаемых элементами x, y, сама пара не изменяется. Для упорядоченных пар ситуация в корне меняется: если $x \neq y$, то упорядоченные пары (x, y) и (y, x) должны быть различными.

На самом деле упорядоченные пары должны обладать следующим свойством: если $u, x \in X$, $v, y \in Y$, то из равенства $(u, v) = (x, y)$ следуют равенства $u = x$, $v = y$.

Мы поняли, каким свойством должны обладать упорядоченные пары, однако пока еще не дали определение этому понятию. Чтобы прийти к определению, докажем следующее вспомогательное утверждение.

Предложение 1.4. *Пусть $u, x \in X$, $v, y \in Y$. Тогда из равенства*

$$\{\{u\}, \{u, v\}\} = \{\{x\}, \{x, y\}\}$$

следуют равенства $u = x$ и $v = y$.

Доказательство. Предположим сначала, что $u = v$. Тогда $\{u, v\} = \{u\}$, и потому

$$\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\} = \{\{u\}\}.$$

Отсюда

$$\{u\} = \{x\} = \{x, y\},$$

т. е. $u = x = y$. Поскольку $u = v$, имеем $u = x = y = v$.

Пусть теперь $u \neq v$. Из предыдущего рассуждения вытекает, что $x \neq y$. Напомним, что множества $\{\{u\}, \{u, v\}\}$ и $\{\{x\}, \{x, y\}\}$ состоят из одних и тех же элементов. Поскольку $\{u, v\} \neq \{x\}$ и $\{x, y\} \neq \{u\}$, имеем

$$\{u\} = \{x\}, \qquad \{u, v\} = \{x, y\}.$$

Из этих двух равенств вытекает, что $u = x$ и $v = y$.

Из предложения 1.4 следует, что упорядоченную пару (x, y) можно определить как множество $\{\{x\}, \{x, y\}\}$.

Назовем *прямым (декартовым) произведением* непустых множеств X и Y множество $X \times Y$, состоящее из всех упорядоченных пар вида (x, y), где $x \in X$, $y \in Y$.

Приведем примеры прямых произведений.

1. Пусть $X = \{a, b, c, d, e, f, g, h\}$, $Y = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Элементы прямого произведения $X \times Y$ лежат в основе шахматной нотации.

2. Пусть X – множество десятичных цифр, т. е. $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Элементы множества $X \times X$ служат для обозначения однозначных и двузначных десятичных чисел. При этом, как и в примере 1, круглые скобки и запятая опускаются, а лидирующая цифра 0 не пишется.

3. Пусть $\mathbb{R}$ – множество всех действительных чисел. Хорошо известно, что на координатной плоскости каждой точке единственным образом сопоставляется упорядоченная пара действительных чисел, т. е. элемент множества $\mathbb{R} \times \mathbb{R}$.

В примерах 2 и 3 мы встретились с ситуацией, когда множества X и Y совпадают. Прямое произведение $X \times X$ называют *декартовым квадратом* множества X и обозначают X^2.

Опираясь на определение упорядоченной пары можно дать определение упорядоченной тройки. Пусть X_1, X_2, X_3 – произвольные непустые множества, $x_i \in X_i$, $i = 1, 2, 3$. Тогда

$$(x_1, x_2, x_3) = ((x_1, x_2), x_3).$$

Иными словами, упорядоченная тройка, составленная из элементов x_1, x_2, x_3 определена нами как упорядоченная пара, первой компонентой которой является упорядоченная пара (x_1, x_2), а второй компонентой – элемент x_3. Упорядоченные тройки обладают свойством, аналогичным свойству упорядоченных пар: если $(x_1, x_2, x_3) = (y_1, y_2, y_3)$, то $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$.

Множество всех упорядоченных троек (x_1, x_2, x_3), где $x_1 \in X_1$, $x_2 \in X_2$, $x_3 \in X_3$, называют прямым (декартовым) произведением множеств X_1, X_2, X_3 и обозначают $X_1 \times X_2 \times X_3$. Множество $X^3 = X \times X \times X$ – это *декартов* куб множества X.

Пусть теперь дано произвольное $n \geqslant 3$. Если $X_1, X_2, \ldots, X_n$ – произвольные непустые множества, то для любых элементов $x_i \in X_i$ $(1 \leqslant i \leqslant n)$ можно определить упорядоченный набор длины n, составленный из $x_1, \ldots, x_n$, следующим образом:

$$(x_1, x_2, \ldots, x_{n-1}, x_n) = ((x_1, x_2, \ldots, x_{n-1}), x_n).$$

Упорядоченные наборы длины n часто называют кортежами длины n. Можно проверить, что два кортежа длины n равны, если равны их элементы, стоящие на одинаковых местах.

Множество всех кортежей длины n, составленных из элементов множеств $X_1, X_2, \ldots, X_n$ называется прямым (декартовым) произведением этих множеств и обозначается через $X_1 \times X_2 \times \ldots \times X_n$. Множество $X^n = X \times X \times \ldots \times X$ называют *декартовой n-ой степенью* множества X.

1.3. Бинарные отношения

С понятием отношения на данном множестве нам уже приходилось встречаться.

Например, на множестве $\mathbb{Z}$ всех целых чисел можно рассмотреть следующие отношения:

1) x равно y;

2) x меньше или равно y;

3) x нацело делит y;

4) $x - y$ кратно 4.

Если L – множество всех прямых на плоскости, то при изучении планиметрии рассматривались такие отношения:

5) x параллельно y;

6) x перпендикулярно y;

7) x пересекает y.

Пусть A – произвольное множество. На булеане $\mathcal{P}(A)$ множества A можно рассмотреть следующее отношение

8) X является подмножеством Y.

Хотя отношения из примеров 1) – 8) являются различными, все же они похожи друг на друга. Если взять упорядоченную пару (x, y), составленную из элементов данного множества, то x и y могут находиться или не находиться в данном отношении. Так в примере 3) числа 5 и 10 (именно в таком порядке) находятся в указанном отношении, а числа 5 и 8 нет. Удобно говорить, что упорядоченная пара $(5, 10)$ принадлежит отношению из примера 3), а упорядоченная пара $(5, 8)$ этому отношению не принадлежит.

Сопоставим отношениям из примеров 1) – 4) множества всех упорядоченных пар чисел, принадлежащих каждому из этих от-

ношений. Например, отношению из примера 3) соответствует множество $\{(x, y) \mid x$ нацело делит $y\}$, а отношению из примера 4) – множество $\{(x, y) \mid x - y$ кратно $4\}$. Понятно, что данным четырем отношениям будут сопоставлены различные подмножества из декартова квадрата $\mathbb{Z}^2$.

Отсюда вытекает важный вывод: вместо изучения отношений на множестве X можно изучать сопоставленные им подмножества из декартова квадрата X^2. Математики идут еще дальше: они отождествляют отношения с сопоставленными им подмножествами декартова квадрата.

Таким образом, мы приходим к следующему определению.

О п р е д е л е н и е. *Бинарным отношением* на множестве X называется подмножество декартова квадрата множества X.

Иными словами, ρ – бинарное отношение на X, если $\rho \subseteq X^2$.

Заметим, что прилагательное "бинарное" подчеркивает тот факт, что рассмотренные нами отношения связаны с упорядоченными парами элементов. Нетрудно привести пример отношения, связанного с упорядоченными тройками. Пусть P – множество всех точек плоскости. Для любых трех точек x, y, z можно рассмотреть отношение: y лежит между x и z. Ясно, что это отношение состоит из упорядоченных троек. Такое отношение называют тернарным.

Пусть ρ – бинарное отношение на множестве X. Если $(x, y) \in \rho$, то говорят, что x и y находятся в отношении ρ. Вместо записи $(x, y) \in \rho$ мы всегда будем использовать упрощенную запись $x \rho y$.

В разделе 1.1 было отмечено, что отношение включения между множествами обладает свойствами рефлексивности, антисимметричности и транзитивности. Сформулируем эти свойства применительно к произвольному бинарному отношению.

О п р е д е л е н и е. Бинарное отношение ρ на множестве X называется *рефлексивным*, если $x \rho x$ для любого $x \in X$.

О п р е д е л е н и е. Бинарное отношение ρ на множестве X называется *антисимметричным*, если для любых $x, y \in X$ из $x \rho y$ и $y \rho x$ следует $x = y$.

О п р е д е л е н и е. Бинарное отношение ρ на множестве X на-

зывается *транзитивным*, если для любых $x, y, z \in X$ из того, что $x\rho y$ и $y\rho z$ следует $x\rho z$.

Дополним этот список еще одним свойством.

О п р е д е л е н и е. Бинарное отношение ρ на множестве X называется *симметричным*, если для любых $x, y \in X$ из $x\rho y$ следует $y\rho x$.

Обращаясь к примерам 1) – 8), отметим, что отношения 1), 2), 3), 4), 5), 8) рефлексивны, все отношения, кроме отношений 2), 3), 8), симметричны, отношения 1), 2), 3), 8) антисимметричны а отношения 1) – 5), 8) транзитивны.

1.4. Отношения эквивалентности

Этот раздел посвящен изучению бинарных отношений, обладающих тремя свойствами: рефлексивностью, симметричностью и транзитивностью.

О п р е д е л е н и е. Бинарное отношение ρ на множестве X называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Отношения из примеров 1), 4), 5) являются отношениями эквивалентности.

Пусть ρ – отношение эквивалентности на множестве X. Для любого элемента x из X рассмотрим множество

$$[x] = \{y \,|\, x\rho y\}.$$

Это множество называется *классом эквивалентости* элемента x. Оно состоит из всех элементов y, эквивалентных x, т. е. из таких элементов, что $x\rho y$.

Если ρ – отношение из примера 4), то класс эквивалентности числа k состоит из всех чисел вида $4n + k$, $n \in \mathbb{Z}$. Нетрудно сообразить, что в этом случае имеется всего четыре различных класса эквивалентности: [0], [1], [2], [3]. Если же в качестве ρ взять отношение параллельности (пример 5), то класс эквивалентности прямой l – это множество всех прямых, параллельных l. В каждом из двух рассмотренных примеров различные классы эквива-

лентности не имеют общих элементов. Оказывается, это свойство присуще классам любого отношения эквивалентности.

Лемма 1. *Если* $x\rho y$, *то* $[x] = [y]$.

Доказательство. Пусть $z \in [x]$. Тогда $x\rho z$ и, в силу симметричности отношения ρ имеем $y\rho x$. Используя транзитивность этого отношения, получаем $y\rho z$, т. е. $z \in [y]$. Таким образом, $[x] \subseteq [y]$. Так как $y\rho x$, в предыдущем рассуждении x и y можно поменять ролями, и потому $[y] \subseteq [x]$.

Лемма 2. *Если* $[x] \neq [y]$, *то* $[x] \cap [y] = \emptyset$.

Доказательство. Предположим, что $[x] \cap [y]$ непусто. Тогда существует такое z, что $z \in [x]$ и $z \in [y]$, откуда $x\rho z$ и $y\rho z$. Используя лемму 1, получаем $[x] = [z] = [y]$, что противоречит условию.

Из лемм 1 и 2 вытекает следующее утверждение.

Теорема 1.3. *Пусть* ρ *– отношение эквивалентности на множестве* X. *Семейство всех различных классов эквивалентности отношения* ρ *является разбиением множества* X.

Доказательство. Так как в силу рефлексивности отношения ρ выполнено включение $x \in [x]$, объединение всех классов эквивалентности совпадает с множеством X. Различные классы эквивалентности не имеют общих элементов, поэтому и объединение всех различных классов эквивалентности совпадает с множеством X.

Таким образом, каждому отношению эквивалентости на множестве X можно сопоставить разбиение этого множества. Верно и обратное: каждому разбиению множества X можно сопоставить отношение эквивалентности на этом множестве.

Пусть X_i $(i \in I)$ – разбиение множества X. Определим на множестве X бинарное отношение ρ следующим образом: $x\rho y$, если $x, y \in X_j$ для некоторого $j \in I$. Рефлексивность и симметричность такого отношения очевидны. Убедимся, что ρ обладает свойством транзитивности. Предположим, что $x\rho y$ и $y\rho z$. Тогда

$x, y \in X_j$ и $y, z \in X_k$ для некоторых $j, k \in I$. Заметим, что множества X_j, X_k имеют непустое пересечение, поскольку они содержат общий элемент y. Однако различные подмножества из разбиения не пересекаются, поэтому $j = k$. Следовательно, $x, z \in X_j$, т. е. $x\rho z$. Итак, отношение ρ является отношением эквивалентности.

Каковы классы эквивалентности этого отношения? Оказывается, классы эквивалентности в точности совпадают с подмножествами из разбиения. В самом деле, предположим, что $x \in X_j$ для некоторого $j \in I$, и убедимся в том, что $[x] = X_j$. Включение $X_j \subseteq [x]$ очевидно, потому что все элементы из X_j находятся в отношении ρ с элементом X. Пусть $y \in [x]$. Тогда $x, y \in X_k$ для некоторого $k \in I$. Ясно, что $j = k$, откуда $y \in X_j$. Таким образом, $[x] \subseteq X_j$.

2. Натуральные числа

2.1. Аксиомы Пеано

О п р е д е л е н и е. Множество всех натуральных чисел $\mathbb{N}$ – это множество, в котором для каждого элемента n однозначно определен следующий элемент n', причем выполнены свойства:

(P1) множество $\mathbb{N}$ содержит элемент 1, обладающий свойством: $n' \neq 1$ для любого $n \in \mathbb{N}$;

(P2) для любых $m, n \in \mathbb{N}$ из $m' = n'$ следует $m = n$;

(P3) пусть M – произвольное подмножество из $\mathbb{N}$, причем $1 \in$ $\in M$ и из включения $m \in M$ следует включение $m' \in M$; тогда $M = \mathbb{N}$.

Свойства (P1)–(P3) называются *аксиомами Пеано*[1]; аксиома (P3) – это *аксиома индукции.*

Заметим, что аксиомы (P1) – (P3) не отвечают на вопросы: *что такое натуральное число* или *что такое множество всех натуральных чисел ?* Они лишь устанавливают несколько простых и интуитивно понятных свойств множества всех натуральных чисел. Оказывается, однако, что этих свойств достаточно для получения всех сведений о натуральных числах, используемых в математике.

Прежде чем идти дальше, докажем следующее утверждение.

Предложение 2.1. *Произвольное натуральное число n либо равно 1, либо существует такое единственное m, что $n = m'$.*

Д о к а з а т е л ь с т в о. Обозначим через M множество, состоящее из таких натуральных чисел n, что либо $n = 1$, либо $n = m'$ для некоторого $m \in \mathbb{N}$. Проверим сначала, что $M = \mathbb{N}$. Для этого применим аксиому индукции. Ясно, что $1 \in M$. Возьмем произвольное $n \in M$. Тогда элемент n' очевидно лежит в M. Таким образом, M удовлетворяет обоим условиям из аксиомы (P3). Поэтому $M = \mathbb{N}$. Единственность такого элемента m сразу следует из аксиомы (P2).

[1] Дж.Пеано (1858–1922) – видный итальянский математик, областями научных интересов которого являлись математический анализ, геометрия, механика и математическая логика.

При доказательстве предложения 2.1 мы применили *метод математической индукции*. Метод математической индукции основывается на использовании аксиомы (P3).

2.2. Сложение натуральных чисел

Определим сумму $m + n$ натуральных чисел m, n.

Определение. Для произвольных натуральных чисел m, n положим

(1) $m + 1 = m'$;

(2) $m + n' = (m + n)'$.

Анализируя это определение, мы видим, что правило (1) позволяет к любому числу прибавить единицу; правило (2) показывает, что, зная сумму $m + n$, можно найти сумму $m + n'$. На самом деле следовало бы доказать при помощи аксиомы индукции, что таким способом сумма двух натуральных чисел определена однозначно. Соответствующие рассуждения мы опустим, поскольку они достаточно громоздки.

Выведем из этого определения основные свойства операции сложения.

Предложение 2.2. *Операция сложения на множестве* $\mathbb{N}$ *обладает следующими свойствами:*

(A1) $m + (n + p) = (m + n) + p$;

(A2) $m + n = n + m$;

(A3) $m + p = n + p \Rightarrow m = n$.

Свойства (A1) и (A2) называются соответственно *ассоциативностью* и *коммутативностью* сложения, а (A3) – свойством *сократимости*.

Заметим, что наличие у операции сложения свойства ассоциативности позволяет сумму более чем двух слагаемых записывать без использования скобок. Более того, для обозначения суммы вида $a_1 + a_2 + \ldots + a_k$ будет использоваться более короткая запись $\sum_{i=1}^{k} a_i$.

Доказательство свойства (A1). Рассмотрим множество

$$M = \{p \,|\, m + (n + p) = (m + n) + p \text{ для любых } m, n \in \mathbb{N}\}.$$

Поскольку

$$m + (n + 1) = m + n' = (m + n)' = (m + n) + 1,$$

мы видим, что $1 \in M$.

Пусть $p \in M$. Тогда

$$\begin{aligned} m + (n + p') = m + (n + p)' &= (m + (n + p))' = \\ &= ((m + n) + p)' = (m + n) + p'. \end{aligned}$$

Из приведенной цепочки равенств вытекает, что $p' \in M$. Стало быть, условия аксиомы индукции выполнены, и потому $M = \mathbb{N}$. В силу выбора множества M мы видим, что требуемое равенство выполнено при всех $m, n, p \in \mathbb{N}$.

Заметим, что из свойства (A1) вытекает равенство

$$n' + 1 = n + 1'. \tag{4}$$

В самом деле,

$$n' + 1 = (n + 1) + 1 = n + (1 + 1) = n + 1'.$$

Прежде чем проверять свойство (A2), докажем вспомогательное утверждение.

Лемма 1. *Для любого $n \in \mathbb{N}$ выполнено равенство $n + 1 = 1 + n$.*

Доказательство. Применим метод математической индукции. Пусть

$$M = \{n \,|\, n + 1 = 1 + n\}.$$

Ясно, что $1 \in M$. Если $n \in M$, то при помощи равенства (4) получаем

$$n' + 1 = n + 1' = (n + 1)' = (1 + n)' = 1 + n',$$

откуда следует, что $n' \in M$. Применение метода математической индукции показывает, что равенство $n + 1 = 1 + n$ выполнено при всех натуральных n.

Доказательство свойства (A2). Пусть

$$M = \{n \,|\, m + n = n + m \text{ для любого } m \in \mathbb{N}\}.$$

Из леммы 1 следует, что $1 \in M$. Предположим, что $n \in M$. Тогда

$$\begin{aligned} m + n' &= (m + n)' = (n + m)' = (n + m) + 1 = \\ &= n + (m + 1) = n + (1 + m) = (n + 1) + m = n' + m \end{aligned}$$

и потому $n' \in M$. Остается применить аксиому индукции.

Доказательство свойства (A3). Рассмотрим множество

$$M = \{p \,|\, m + p = n + p \Rightarrow m = n\}.$$

Поскольку $m+1 = m'$, $n+1 = n'$, применение к равенству $m+1 = n+1$ аксиомы (P2) показывает, что $m = n$. Отсюда следует, что $1 \in M$. Допустим, что $p \in M$ и предположим, что $m + p' = n + p'$. Используя определение сложения, получаем, что $(m + p)' = (n + p)'$. Используя аксиому (P2), находим, что $m+p = n+p$. Так как $p \in M$, из последнего равенства следует, что $m = n$. Стало быть, проверено, что $p' \in M$. Применение аксиомы индукции завершает рассуждение.

Предложение 2.3. *Если m, n – произвольные натуральные числа, то $m + n \neq m$*

Доказательство. Зафиксируем произвольное натуральное число n и рассмотрим множество

$$M = \{m \,|\, m + n \neq m\}.$$

Из свойства (A2) и аксиомы (P1) следует, что

$$1 + n = n + 1 = n' \neq 1.$$

Отсюда вытекает, что $1 \in M$.

Пусть некоторое число k принадлежит M, т.е. $k + n \neq k$. Рассуждая "от противного", предположим, что $k' + n = k'$. Поскольку $k' + n = (k + n)'$, имеем $(k + n)' = k'$, откуда по аксиоме (P2) получаем равенство $k + n = k$, противоречащее выбору k. Таким образом, из предположения $k + n \neq k$ вытекает, что $k' + n \neq k'$. Применение аксиомы (P3) заканчивает рассуждение.

Пусть m, n – произвольные натуральные числа. Предположим, что существует число p, для которого выполнено равенство

$$m + p = n. \tag{5}$$

В силу свойства (A3) такое число p единственно.

О п р е д е л е н и е. Натуральное число p, удовлетворяющее равенству (5), называется *разностью* чисел n, m и обозначается $n - m$.

Таким образом, на множестве $\mathbb{N}$ определена еще одна операция – вычитание. Правда, в отличие от операции сложения, эта операция применима не к каждой упорядоченной паре натуральных чисел. Поэтому операцию вычитания на множестве $\mathbb{N}$ принято называть *частичной*. К обсуждению свойств операции вычитания мы вернемся в разд. 2.4.

Предложение 2.4. *Если m, n – произвольные натуральные числа, то выполнено в точности одно из трех утверждений:*
(1) $m = n$;
(2) $m = n + p$ для некоторого $p \in \mathbb{N}$;
(3) $n = m + q$ для некоторого $q \in \mathbb{N}$.

Д о к а з а т е л ь с т в о. Зафиксируем натуральное число n, и пусть $P(m)$ обозначает следующее свойство числа m: $m = n$ или $m = n + p$ для некоторого $p \in \mathbb{N}$ или $n = m + q$ для некоторого $q \in \mathbb{N}$. Теперь рассмотрим множество $M = \{m \mid P(m)\}$.

Проверим сначала, что $1 \in M$. Для этого рассмотрим две возможности: $n = 1$ и $n \neq 1$. В случае $n = 1$ истинность высказывания $P(1)$ очевидна. Если же $n \neq 1$, то в силу предложения 2.1 найдется такое q, что $n = q'$. Отсюда $n = q + 1 = 1 + q$.

Возьмем теперь произвольное $m \in M$ и покажем, что $m' \in M$. Так как $P(m)$ истинно, то для m выполнено одно из утверждений (1), (2), (3). Если для m выполняется (1), то $m = n$, откуда $m' = n + 1$; стало быть, для m' имеет место утверждение (2) при $p = 1$. Пусть для m истинно утверждение (2), т. е. $m = n + p$ для некоторого $p \in \mathbb{N}$. Тогда $m' = n + p'$; значит, для m' выполнено утверждение (2). Предположим, наконец, что m обладает свойством (3), т. е. $n = m + q$ для некоторого $q \in \mathbb{N}$. Если $q = 1$, то $n = m'$, и для m' имеет место (1). Если же $q \neq 1$, то $q = r' = r + 1$ для некоторого $r \in \mathbb{N}$. Тогда $n = m + q = m + (r + 1) = (m + 1) + r = m' + r$; отсюда видно, что для m' также выполнено утверждение (3).

Применяя аксиому индукции, мы видим, что $M = \mathbb{N}$, т. е. $P(m)$ истинно при любом m. Так как число n можно взять произвольным, то выполнимость одного из утверждений (1), (2), (3) доказана.

Осталось проверить, что никакие два из этих утверждений одновременно выполняться не могут. Этот факт следует из предложения 2.3; соответствующие рассуждения оставляются читателю.

2.3. Умножение натуральных чисел

О п р е д е л е н и е. Для произвольных натуральных чисел m, n положим

(1) $m \cdot 1 = m$;

(2) $m \cdot n' = m \cdot n + m$.

Заметим, что и здесь следовало бы проверить однозначность определения произведения $m \cdot n$ для произвольных m, n. Эта проверка опускается из тех же соображений, что и аналогичная проверка для суммы.

Предложение 2.5. *Операция умножения на множестве* $\mathbb{N}$ *обладает следующими свойствами:*

(M1) $m \cdot (n \cdot p) = (m \cdot n) \cdot p$;

(M2) $m \cdot n = n \cdot m$;

(M3) $m \cdot (n + p) = m \cdot n + m \cdot p$;

(M4) $m \cdot p = n \cdot p \Rightarrow m = n$.

Свойства (M1), (M2) называются соответственно ассоциативностью и коммутативностью умножения, свойство (M3) – *дистрибутивностью*, а (M4) – свойством сократимости умножения.

Из определения умножения и свойства коммутативности вытекает, что $1 \cdot n = n \cdot 1 = n$ для любого $n \in \mathbb{N}$. Имея в виду это свойство числа 1, говорят, что 1 – *нейтральный* элемент относительно операции умножения. Заметим, что в силу предложения 2.3 множество $\mathbb{N}$ не содержит нейтрального элемента относительно операции сложения

Наличие у операции умножения свойства ассоциативности позволяет произведение более чем двух сомножителей записывать без

использования скобок. Кроме того, обозначения произведения вида $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ будет применяться более короткая запись $\prod_{i=1}^{k} a_i$.

Свойства (M1) – (M4) проверяются аналогично свойствам сложения. Заметим лишь, что сначала следует методом математической индукции доказать свойство (M3); затем проверить справедливость равенства $(m+n) \cdot p = m \cdot p + n \cdot p$ (ведь свойство коммутативности еще не доказано). Проверка ассоциативности и коммутативности умножения совершенно аналогична проверке ассоциативности и коммутативности сложения (разумеется, придется использовать уже доказанную дистрибутивность) (см. разд. 2.2). Детали оставляются читателю в качестве упражнения. Остановимся лишь на доказательстве свойства (M4). Рассуждая "от противного", предположим, что $m \cdot p = n \cdot p$, но $m \neq n$. В силу предложения 2.4 без ограничения общности можно считать, что $m = n + r$ для некоторого $r \in \mathbb{N}$. Отсюда $m \cdot p = n \cdot p + r \cdot p$, и потому $m \cdot p \neq n \cdot p$. Противоречие.

2.4. Сравнение натуральных чисел

В этом разделе мы определим отношение порядка на множестве $\mathbb{N}$ и изучим свойства этого отношения.

О п р е д е л е н и е. Пусть m, n – натуральные числа. Будем говорить, что m меньше n (и обозначим $m < n$), если для некоторого $p \in \mathbb{N}$ выполнено равенство $n = m + p$.

Отношение "меньше" называется *порядком* на множестве $\mathbb{N}$.

Лемма 1. *Порядок на множестве $\mathbb{N}$ обладает свойством транзитивности; это означает, что из $m < n$ и $n < p$ следует $m < p$.*

Д о к а з а т е л ь с т в о. Поскольку $m < n$ и $n < p$, имеем $n = m + r$, $p = n + s$ для некоторых $r, s \in \mathbb{N}$. Отсюда $p = n + (r + s)$; таким образом, $n < p$.

Из предложения 2.4 немедленно вытекает

Лемма 2. *Порядок на множестве $\mathbb{N}$ обладает свойством линейности; это означает, что для любых натуральных чисел m,*

n выполнено в точности одно из трех соотношений: $m = n$, $m < n$, $n < m$.

О п р е д е л е н и е. Число m меньше или равно числа n (обозначаем $m \leqslant n$), если $m = n$ или $m < n$.

Отношение "меньше или равно" часто называют *нестрогим порядком* на множестве $\mathbb{N}$.

Из лемм 1, 2 вытекает

Предложение 2.6. *Пусть m, n, p – произвольные натуральные числа. Тогда выполнены свойства*

(O1) $m \leqslant m$;

(O2) *если* $m \leqslant n$ *и* $n \leqslant m$, *то* $m = n$;

(O3) *если* $m \leqslant n$ *и* $n \leqslant p$, *то* $m \leqslant p$;

(O4) $m \leqslant n$ *или* $n \leqslant m$.

Как мы знаем, свойства (O1), (O2), (O3), (O4) называются соответственно рефлексивностью, антисимметричностью, транзитивностью и линейностью нестрогого порядка.

Предложение 2.7. *Если $n < m'$, то $n \leqslant m$.*

Д о к а з а т е л ь с т в о. Поскольку $n < m'$, имеем $m + 1 = m' = n + q$ для некоторого $q \in \mathbb{N}$. Если $q = 1$, то $m + 1 = n + 1$, откуда $m = n$. Если же $q > 1$, то $q = r + 1$ для некоторого $r \in \mathbb{N}$. Стало быть, $m+1 = n+r+1$ и потому $m = n+r$; таким образом, $n < m$.

Теперь мы можем продолжить обсуждение операции вычитания. По определению разность $n - m$ (если она существует) является решением уравнения

$$m + x = n. \tag{6}$$

В связи с этим интересно изучить вопрос о разрешимости уравнения (6).

Предложение 2.8. *Если $n > m$, то уравнение $m + x = n$ имеет единственное решение.*

Доказательство. Существование решения уравнения (6) сразу вытекает из определения строгого порядка на множестве $\mathbb{N}$. Проверим единственность. Пусть $m + x_1 = n$ и $m + x_2 = n$. Тогда $m + x_1 = m + x_2$. При помощи свойства (А3) операции сложения получаем, что $x_1 = x_2$.

В дальнейшем будут часто встречаться множества, на которых определен порядок, обладающий свойствами (О1)–(О4). Поэтому удобным окажется следующее важное понятие.

Определение. Множество L, на котором задан порядок $\leqslant$, удовлетворяющий свойствам (О1)–(О4), называется *линейно упорядоченным.*

Заметим, что произвольное непустое подмножество линейно упорядоченного множества само является линейно упорядоченным.

Определение. Элемент m линейно упорядоченного множества L называется *наименьшим элементом*, если $m \leqslant l$ для любого $l \in L$.

Наименьшим элементом множества $\mathbb{N}$, очевидно, является элемент 1. В самом деле, из предложения 2.1 следует, что для всякого $n \neq 1$ найдется такое m, что $n = m+1$. Поэтому $1 \leqslant n$ для любого $n \in \mathbb{N}$.

Определение. Элемент m линейно упорядоченного множества L называется *наибольшим элементом*, если $l \leqslant m$ для любого $l \in L$.

Определение. Пусть M – непустое подмножество линейно упорядоченного множества L. Элемент $b \in L$ называется верхней (нижней) гранью подмножества M, если $l \leqslant b$ (соответственно $b \leqslant l$) для любого $l \in M$.

Определение. Подмножество M линейно упорядоченного множества L называется ограниченным сверху (ограниченным снизу), если оно имеет верхнюю (соответственно нижнюю) грань.

Теорема 2.1. *Всякое непустое множество натуральных чисел имеет наименьший элемент.*

Доказательство. Рассуждая "от противного", предположим,

что существует непустое подмножество Q из $\mathbb{N}$, не имеющее наименьшего элемента. Пусть $\mathbb{N}_{\leqslant n}$ обозначает множество всех натуральных чисел, не превосходящих n. Убедимся, что множество Q обладает двумя следующими свойствами:

1) $Q \cap \mathbb{N}_{\leqslant 1} = \emptyset$,

2) если $Q \cap \mathbb{N}_{\leqslant n} = \emptyset$, то $Q \cap \mathbb{N}_{\leqslant n+1} = \emptyset$.

Нетрудно понять, что являясь наименьшим среди натуральных чисел, 1 не может принадлежать множеству Q (иначе множество Q имело бы наименьший элемент, равный 1). Поскольку $\mathbb{N}_{\leqslant 1} = \{1\}$, имеем $Q \cap \mathbb{N}_{\leqslant 1} = \emptyset$. Таким образом, свойство 1) выполнено.

Пусть n – такое натуральное число, что $Q \cap \mathbb{N}_{\leqslant n} = \emptyset$. Ясно, что в этой ситуации число $n+1$ не может принадлежать множеству Q, так как в противном случае $n+1$ было бы наименьшим элементом Q. Учитывая, что

$$\mathbb{N}_{\leqslant n+1} = \mathbb{N}_{\leqslant n} \cup \{n+1\},$$

получаем равенство $Q \cap \mathbb{N}_{\leqslant n+1} = \emptyset$. Следовательно, свойство 2) также выполняется. Пусть

$$M = \{n \mid Q \cap \mathbb{N}_{\leqslant n} = \emptyset\}.$$

Из свойств 1), 2) вытекает, что множество M удовлетворяет условиям аксиомы индукции. Поэтому $M = \mathbb{N}$. Из последнего равенства с очевидностью вытекает, что Q – пустое множество, и мы получили противоречие с выбором Q.

О п р е д е л е н и е. Линейно упорядоченное множество L называется *вполне упорядоченным*, если в нем любое непустое подмножество имеет наименьший элемент.

Таким образом, теорема 2.1 утверждает, что множество $\mathbb{N}$ является вполне упорядоченным.

Разумеется, не всякое непустое множество натуральных чисел имеет наибольший элемент; в частности, это относится к самому множеству $\mathbb{N}$. Тем не менее, справедливо следующее важное утверждение.

Теорема 2.2. *Всякое непустое ограниченное сверху множество натуральных чисел имеет наибольший элемент.*

Доказательство. Пусть M – ограниченное сверху подмножество из $\mathbb{N}$. Обозначим через B множество верхних граней множества M. Ясно, что B непусто. В силу теоремы 2.1 множество B имеет наименьший элемент b. Поскольку b – верхняя грань множества M, достаточно проверить, что $b \in M$. Если $b = 1$, то $M = \{1\}$. Если же $b > 1$, то $b = c'$ для некоторого $c \in \mathbb{N}$. Так как $c < b$, то существует такое $m \in M$, что $c < m$. Кроме того, $m \leqslant c' = b$. Используя предложение 2.7, получаем, что $m = b$, т. е. $b \in M$.

2.5. Характеризация множества $\mathbb{N}$ при помощи порядка

В 2.4 введено отношение нестрогого порядка на множестве $\mathbb{N}$ и из аксиом Пеано выведен ряд свойств этого отношения. В этом разделе мы покажем, что, взяв за основу несколько свойств отношения порядка, можно для каждого натурального n определить следующее за ним число n' и получить аксиомы Пеано.

Рассмотрим следующие три свойства нестрогого порядка на множестве $\mathbb{N}$:

(С1) $\mathbb{N}$ является вполне упорядоченным множеством;

(С2) всякое непустое ограниченное сверху подмножество из $\mathbb{N}$ имеет наибольший элемент;

(С3) множество $\mathbb{N}$ не имеет наибольшего элемента.

Итак, забудем на время определение множества $\mathbb{N}$, данное нами в разд. 2.1. Рассмотрим множество, на котором задан нестрогий линейный порядок, причем выполнены свойства (С1) – (С3).

В качестве элемента 1 возьмем наименьший элемент множества $\mathbb{N}$; существование такого элемента гарантируется свойством (С1).

Пусть $\mathbb{N}_{>n}$ ($\mathbb{N}_{<n}$) обозначает множество всех натуральных чисел, больших (соответственно меньших), чем n. В силу свойства (С3) каждое из множеств $\mathbb{N}_{>n}$ непусто. Поэтому по свойству (С1) при любом $n \in \mathbb{N}$ множество $\mathbb{N}_{>n}$ имеет наименьший элемент; этот элемент обозначим через n'.

Убедимся теперь, что такое определение элемента n', следующего за n, позволяет из свойств (С1) – (С3) вывести аксиомы Пеано (Р1) – (Р3).

Вывод аксиомы (P1). Эта аксиома сразу следует из того, что 1 является наименьшим элементом множества $\mathbb{N}$.

Вывод аксиомы (P2). Будем рассуждать "от противного". Предположим, что существуют такие числа m, n, что $m \neq n$ и $m' = n'$. Поскольку $m \neq n$, одно из этих чисел меньше другого; это сразу вытекает из свойства (C1). Без ограничения общности можно считать, что $m < n$. Из последнего неравенства следует, что $n \in \mathbb{N}_{>m}$, и потому $m' \leqslant n < n'$, что противоречит равенству $m' = n'$.

Вывод аксиомы (P3). Возьмем произвольное множество M, обладающее свойствами: $1 \in M$ и $n \in M \Rightarrow n' \in M$; нам следует убедиться, что $M = \mathbb{N}$. Для этого достаточно проверить, что множество $Q = \mathbb{N} \setminus M$ пусто. Предположим, что $Q \neq \emptyset$. В силу свойства (C1) множество Q имеет наименьший элемент q. Поскольку $1 \notin Q$, выполнено неравенство $1 < q$. Отсюда следует, что множество $\mathbb{N}_{<q}$ непусто; кроме того, это множество ограничено сверху. Значит, по свойству $(C2)$ это множество имеет наибольший элемент r. Ясно, что $r < q$, поэтому $r \in M$. Убедимся теперь, что $r' = q$. Пусть s – такое натуральное число, что $s \in \mathbb{N}_{>r}$, т. е. $r < s$. Неравенство $s < q$ невозможно, поскольку r – наибольший элемент множества $\mathbb{N}_{<q}$. Следовательно, $q \leqslant s$. Тем самым доказано, что q – наименьший элемент множества $\mathbb{N}_{>r}$, т. е. $q = r'$. Осталось заметить, что из включения $r \in M$ должно следовать включение $q = r' \in M$. Последнее включение противоречит тому, что множества M и Q не пересекаются.

2.6. Метод математической индукции

Пусть имеется некоторое свойство натуральных чисел $A(n)$. Вообще говоря, этим свойством могут обладать не все натуральные числа. Рассмотрим, например, следующее свойство: "n^2+n+1 – простое число" (определение простого числа см. в разделе 3.7). Нетрудно видеть, что числа 1, 2, 3, 5, 6 этим свойством обладают, а числа 4 и 7 – не обладают.

Однако, часто возникает следующая задача: доказать, что некоторое свойство $A(n)$ выполняется для всех натуральных чисел.

Например, рассмотрим следующее свойство:

$$1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6}. \qquad (7)$$

Если вместо n в это равенство подставлять конкретные натуральные числа, то всякий раз будет получаться верное числовое равенство; это означает, что подставленное число обладает свойством (7). Однако проверить это свойство при помощи подстановки для всех натуральных чисел мы, разумеется, не сможем – для этого потребовалось бы бесконечное число проверок. Каким же способом можно доказать, что свойством (7) обладают все натуральные числа? Оказывается, это можно сделать при помощи аксиомы индукции.

Итак, пусть нужно доказать, что данным свойством $A(n)$ обладают все натуральные числа. Предположим, что мы умеем доказывать следующие утверждения:

1) $A(1)$ выполняется, т. е. 1 обладает данным свойством (база индукции);

2) для любого $k \geqslant 1$ из того, что выполнено $A(k)$ следует выполнение $A(k+1)$ (шаг индукции).

Оказывается, в таком случае можно утверждать, что $A(n)$ выполняется для всех натуральных чисел.

В самом деле, обозначим через M множество всех натуральных чисел, которые обладают данным свойством. Из утверждения 1) следует, что $1 \in M$. Утверждение 2) означает, что включение $k \in M$ влечет включение $k + 1 = k' \in M$ при любом $k \geqslant 1$. На основании аксиомы индукции мы заключаем, что что $M = \mathbb{N}$.

Метод математической индукции сводится к проверке утверждений 1) и 2) и предназначен для доказательства того факта, что данным свойством $A(n)$ обладают все натуральные числа.

Применим метод математической индукции для доказательства того, что равенство (7) выполнено для всех натуральных чисел.

При $n = 1$ равенство (7), очевидно, выполнено:

$$1 = \frac{1 \cdot 2 \cdot 3}{6}.$$

Пусть при $n = k \geqslant 1$ выполнено равенство

$$1^2 + 2^2 + 3^2 + \ldots + (k-1)^2 + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Тогда

$$1^2+2^2+3^2+\ldots+(k-1)^2+k^2+(k+1)^2 = \frac{k(k+1)(2k+1)}{6}+(k+1)^2 =$$

$$= \frac{(k+1)(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}.$$

Таким образом, из того, что равенство (7) выполнено при $n = k \geqslant 1$ нам удалось доказать, что это равенство выполняется и при $n = k+1$. Поскольку база индукции и шаг индукции проверены, равенство (7) выполнено для всех натуральных чисел.

Доказательства методом математической индукции могут использовать несколько иные схемы рассуждений, чем примененная нами выше. В таких случаях вместо аксиомы индукции используются следующие утверждения.

Предложение 2.9. *Пусть M – произвольное подмножество из $\mathbb{N}$, причем $l \in M$ и для любого $k \geqslant l$ из включения $k \in M$ следует включение $k+1 \in M$; тогда M содержит все натуральные числа n, большие либо равные l.*

Предложение 2.10. *Пусть M – произвольное подмножество из $\mathbb{N}$, причем $1, 2, \ldots, l \in M$ и для любого $k \geqslant l$ из включения $k-l+1, k-l+2, \ldots, k \in M$ следует включение $k+1 \in M$; тогда $M = \mathbb{N}$.*

Предложение 2.11. *Пусть M – произвольное подмножество из $\mathbb{N}$, причем $1 \in M$ и, кроме того, для любого $k > 1$ выполнено свойство: если все числа, меньшие k принадлежат M, то k принадлежит M. Тогда $M = \mathbb{N}$.*

Эти утверждения доказываются однотипными рассуждениями, основанными на использовании теоремы 2.1.

Докажем, например, предложение 2.11. Пусть M – множество натуральных чисел, удовлетворяющее условию этого предложения. Рассуждая "от противного", предположим, что $M \neq \mathbb{N}$. Тогда

множество $Q = \mathbb{N} \setminus M$ непусто. В силу теоремы 2.1 множество Q имеет наименьший элемент q. Поскольку $1 \notin Q$, имеем $q > 1$. В силу выбора q все числа, меньшие q, не принадлежат множеству Q, а потому они лежат во множестве M. Так как $q \notin M$, получили противоречие с условием предложения.

Доказательство двух других предложений читатель может провести самостоятельно.

Рассмотрим несколько доказательств методом математической индукции.

1. Доказать, что неравенство $2^n > n^2$ выполнено при всех натуральных $n \geqslant 5$.

Легко видеть, что при $n = 5$ данное неравенство выполнено. Тем самым проверена база индукции.

Пусть при $n = k \geqslant 5$ выполнено неравенство

$$2^k > k^2.$$

Тогда

$$2^{k+1} = 2 \cdot 2^k > 2k^2.$$

Убедимся теперь, что при $k \geqslant 5$ выполнено неравенство

$$2k^2 > (k+1)^2 \Leftrightarrow k^2 - 2k - 1 > 0.$$

Поскольку

$$k^2 - 2k - 1 > k^2 - 3k = k(k-3) > 0,$$

требуемое неравенство доказано.

Таким образом, из неравенства $2^k > k^2$ следует неравенство $2^{k+1} > (k+1)^2$. Мы проверили шаг индукции, и тем самым завершили доказательство.

Нетрудно понять, что основой для такого доказательства является предложение 2.9.

2. Пусть дана последовательность (u_n), заданная формулами

$$u_1 = 2, \quad u_2 = 8, \quad u_n = 4u_{n-1} - 4u_{n-2} \text{ при } n \geqslant 3.$$

Доказать, что $u_n = n2^n$.

Поскольку $u_1 = 1 \cdot 2^1$, $u_2 = 2 \cdot 2^2$, база индукции проверена. Заметьте, что в данном случае база индукции состоит в проверке двух равенств.

Переходя к доказательству шага индукции, предположим, что при $k \geqslant 2$ выполнены равенства $u_{k-1} = (k-1)2^{k-1}$ и $u_k = k2^k$. Убедимся, что при $n = k+1$ требуемое равенство также выполняется. Поскольку

$$u_{k+1} = 4u_k - 4u_{k-1},$$

с использованием предположения индукции имеем

$$u_{k+1} = 4k2^k - 4(k-1)2^{k-1} = 8k2^{k-1} - 4(k-1)2^{k-1} =$$

$$= 4(k+1)2^{k-1} = (k+1)2^{k+1}.$$

Таким образом, шаг индукции проверен. Заметим, что при проверке шага индукции для доказательства равенства при $n = k+1$ необходимо было предположить истинность соответствующих равенств при $n = k$ и $n = k-1$.

Читатель должен убедиться, что это доказательство основано на применении предложения 2.10 при $l = 2$.

Пример доказательства, основанного на применении предложения 2.11, мы сейчас рассматривать не будем. В дальнейшем такие доказательства будут нам встречаться неоднократно (см., например, раздел 3.8).

3. Целые числа

3.1. Операции над целыми числами

Пусть $\overline{\mathbb{N}}$ – множество, состоящее из элементов $\overline{n}$, где $n \in \mathbb{N}$, причем $\overline{k} \neq \overline{m}$ тогда и только тогда, когда $k \neq m$. Мы предполагаем также, что $\mathbb{N} \cap \overline{\mathbb{N}} = \emptyset$. Пусть 0 – некоторый элемент, не принадлежащий объединению $\mathbb{N} \cup \overline{\mathbb{N}}$.

О п р е д е л е н и е. Множество $\mathbb{Z} = \overline{\mathbb{N}} \cup \{0\} \cup \mathbb{N}$ называется множеством всех целых чисел.

Элементы из $\mathbb{N}$ будут называться *целыми положительными* (или по-прежнему натуральными) числами, элементы из $\overline{\mathbb{N}}$ – это *целые отрицательные* числа; элемент 0, как обычно, называется *нулем.*

Определим на множестве $\mathbb{Z}$ операции сложения и умножения. При определении операций над целыми числами естественно будет использоваться возможность применения соответствующих операций к натуральным числам.

Определение сложения.

(1) $0 + 0 = 0$;

(2) $m + 0 = 0 + m = m, \quad \overline{m} + 0 = 0 + \overline{m} = \overline{m}$;

(3) $\overline{m} + \overline{n} = \overline{m + n}$;

(4) $\overline{m} + n = n + \overline{m} = \begin{cases} 0, & \text{если } m = n, \\ n - m, & \text{если } n > m, \\ \overline{m - n}, & \text{если } m > n. \end{cases}$

Определение умножения.

(1) $0 \cdot 0 = 0$;

(2) $m \cdot 0 = 0 \cdot m = \overline{m} \cdot 0 = 0 \cdot \overline{m} = 0$;

(3) $1 \cdot \overline{m} = \overline{m} \cdot 1 = \overline{m}$;

(4) $\overline{m} \cdot \overline{n} = m \cdot n$;

(5) $\overline{m} \cdot n = m \cdot \overline{n} = \overline{m \cdot n}$.

Необходимые при дальнейшем изложении свойства сложения и умножения перечислены в леммах 1–9.

Лемма 1. *Для произвольного $r \in \mathbb{Z}$ выполнены равенства $r + 0 = 0 + r = r$.*

Доказательство. См. пункты 1, 2 из определения сложения.

Лемма 2. *Для произвольного $r \in \mathbb{Z}$ существует единственное $s \in \mathbb{Z}$, для которого $r + s = s + r = 0$.*

Доказательство. Если $r \in \mathbb{N}$, то $s = \overline{r}$; если $r \in \overline{\mathbb{N}}$, т. е. $r = \overline{n}$ для некоторого $n \in \mathbb{N}$, то $s = n$; если же $r = 0$, то $s = 0$. Единственность такого числа s будет доказана позже (см. лемму 4).

Единственное число s, удовлетворяющее равенствам $r + s = s + r = 0$, называется *противоположным* для числа r и обозначается через $-r$.

Данное нами выше определение операции сложения показывает, что $-0 = 0$ и $-n = \overline{n}$, $-\overline{n} = n$ для любого $n \in \mathbb{N}$.

Лемма 3. *Для любых $r, s, t \in \mathbb{Z}$ выполнены равенства*
(a) $r + s = s + r$,
(b) $(r + s) + t = r + (s + t)$.

Свойство (a) непосредственно вытекает из определения операции сложения. Свойство (b), очевидно, выполнено, если числа r, s, t натуральные или одно из этих чисел равно нулю. Проверка равенства (b) в случае, когда хотя бы одно из чисел r, s, t отрицательно, сводится к несложным, но достаточно длинным вычислениям. Эту проверку мы опускаем.

Итак, операция сложения на множестве $\mathbb{Z}$ коммутативна и ассоциативна (лемма 3), обладает нейтральным элементом 0 (лемма 1) и для каждого целого числа существует противоположное к нему число (лемма 2). Кратко наличие на множестве $\mathbb{Z}$ операции сложения с таким набором свойств выражают словами: $\mathbb{Z}$ является *абелевой*[1] *группой относительно сложения.*

Лемма 4. *Для любых $q, r \in \mathbb{Z}$ уравнение $x + r = q$ имеет единственное решение.*

[1]Название дано в честь замечательного норвежского математика Н. Х. Абеля (1802–1829).

Доказательство. В силу леммы 2 существует такое $s \in \mathbb{Z}$, что $r + s = s + r = 0$. Тогда $q + s + r = q + 0 = q$; стало быть, $x = q + s$ является решением данного уравнения. Перейдем к проверке единственности решения. Пусть $x_1 + r = q = x_2 + r$. Тогда

$$x_1 = x_1 + 0 = x_1 + r + s = x_2 + r + s = x_2 + 0 = x_2.$$

Решение уравнения $x + q = r$ называется разностью чисел r и q и обозначается $r - q$. В частности, число $0 - r$ выше было названо противоположным к r и обозначено через $-r$.

Лемма 5. *Пусть r, s, t, u – произвольные целые числа. Тогда*
(a) $-(r + s) = (-r) + (-s)$,
(b) $(r + s) - (t + u) = (r - t) + (s - u)$.

Доказательство. Проверим, что число $(-r) + (-s)$ является противоположным к силу $r + s$. Используя свойства коммутативности и ассоциативности сложения, получаем

$$r + s + (-r) + (-s) = r + (-r) + s + (-s) = 0 + 0 = 0.$$

Поскольку единственность элемента, противоположного данному, уже доказана, мы получили свойство (a).

Чтобы проверить свойство (b), достаточно убедиться в том, что число $x = (r-t)+(s-u)$ является решением уравнения $(t+u)+x = r+s$. Из определения разности целых чисел имеем $t+(r-t) = r$ и $u + (s - u) = s$. Поэтому

$$(t + u) + (r - t) + (s - u) = (t + (r - t)) + (u + (s - u)) = r + s.$$

Так как уравнение $(t+u)+x = r+s$ имеет единственное решение, свойство (b) также доказано.

Следующие три утверждения связаны со свойствами операции умножения на множестве $\mathbb{Z}$. Доказательства этих свойств мы опускаем.

Лемма 6. *Для произвольного $r \in \mathbb{Z}$ выполнены равенства*
(a) $r \cdot 1 = 1 \cdot r = r$,
(b) $r \cdot 0 = 0 \cdot r = 0$

Лемма 7. *Для любых $r, s, t \in \mathbb{Z}$ выполнены равенства*
(a) $r \cdot s = s \cdot r$,
(b) $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.

Лемма 8. *Для любых $r, s, t \in \mathbb{Z}$ выполнено равенство*

$$r \cdot (s + t) = r \cdot s + r \cdot t.$$

Таким образом, кроме операции сложения, на множестве $\mathbb{Z}$ определена операция умножения, которая обладает нейтральным элементом 1 (лемма 6), является коммутативной и ассоциативной (лемма 7), и, кроме того, выполняется свойство дистрибутивности (лемма 8). Наличие на множестве $\mathbb{Z}$ операций сложения и умножения таких, что относительно сложения $\mathbb{Z}$ – абелева группа, а для умножения выполнены перечисленные выше свойства, кратко выражают следующим образом: $\mathbb{Z}$ является *коммутативным кольцом с единицей*.

Лемма 9. *Для любых $r, s \in \mathbb{Z}$ выполнены равенства*
(a) $r \cdot (-s) = (-r) \cdot s = -(r \cdot s)$,
(b) $(-r) \cdot (-s) = r \cdot s$.

Доказательство. Проверим свойство (a). Используя дистрибутивность, имеем

$$0 = r \cdot 0 = r \cdot (s + (-s)) = r \cdot s + r \cdot (-s).$$

Из этого равенства видно, что число $r \cdot (-s)$ является противоположным к числу $r \cdot s$; это означает, что $r \cdot (-s) = -(r \cdot s)$. Равенство $(-r) \cdot s = -(r \cdot s)$ легко следует из доказанного равенства и коммутативности умножения.

Свойство (b) легко получается из свойства (a). Действительно,

$$(-r) \cdot (-s) = (-(-r)) \cdot s = r \cdot s.$$

Здесь мы использовали единственность элемента, противоположного к данному: в самом деле, элемент $-(-r)$, противоположный к $-r$, в силу единственности совпадает с r.

Следуя сложившейся практике, в дальнейшем знак умножения мы, как правило, будем опускать, т. е. $r \cdot s$ будем записывать в виде rs.

3.2. Порядок на множестве $\mathbb{Z}$

Пусть $r, s \in \mathbb{Z}$. Число r меньше числа s ($r < s$), если разность $s - r$ является натуральным числом.

Введенное нами отношение "меньше" на множестве $\mathbb{Z}$, как и раньше, называется порядком.

Сформулируем основные свойства порядка на множестве $\mathbb{Z}$.

Предложение 3.1. *Пусть r, s, t, u – произвольные целые числа. Тогда*

(1) *если $r < s$ и $s < t$, то $r < t$ (транзитивность);*

(2) *для любых r и s выполнено в точности одно из трех соотношений: либо $r = s$, либо $r < s$, либо $s < r$ (линейность);*

(3) *если $r < s$ и $t < u$, то $r + t < s + u$;*

(4) *если $r < s$ и $0 < t$, то $rt < st$;*

(5) *если $0 < r < s$ и $0 < t < u$, то $rt < su$.*

(6) *если $0 < r < s$, то $r^2 < s^2$.*

Доказательство. Свойства (1), (3), (4) сразу следуют из того, что множество всех натуральных чисел *замкнуто* относительно сложения и умножения (это означает, что сумма и произведение натуральных чисел есть число натуральное). Свойство (2) вытекает из того факта, что разность $r - s$ должна быть либо нулем, либо целым положительным числом, либо целым отрицательным числом.

Проверим свойство (5). Используя дважды свойство (4), имеем $rt < st$ и $st < su$. Используя свойство (1), получаем требуемое неравенство.

Свойство (6) немедленно вытекает из свойства (5).

Нестрогий порядок определяется стандартно: $r \leqslant s$, если $r = s$ или $r < s$. Читателю полезно сформулировать и доказать аналог предложения 3.1 для нестрогого порядка.

3.3. Абсолютная величина целого числа

Абсолютная величина (модуль) целого числа r равна r, если $r \geqslant 0$, и равна $-r$, если $r < 0$.

Как обычно, абсолютная величина r обозначается через $|r|$.

Предложение 3.2. *Пусть r и s – произвольные целые числа. Тогда*

(1) $|-r| = |r|$;
(2) $|r|^2 = r^2$;
(3) $-|r| \leqslant r \leqslant |r|$;
(4) $|rs| = |r||s|$;
(5) $|r + s| \leqslant |r| + |s|$.

Доказательство. Свойства (1)–(3) очевидны. Для проверки свойств (4), (5) воспользуемся следующим легко проверяемым утверждением: если $a \geqslant 0$ и $b \geqslant 0$, то из равенства $a^2 = b^2$ следует равенство $a = b$, а из неравенства $a^2 \leqslant b^2$ следует неравенство $a \leqslant b$. Это утверждение следует из свойств (2) и (6) порядка на множестве целых чисел (см. разд. 3.2).

Равенство (4) проверяется без труда. В самом деле, достаточно проверить, что $|rs|^2 = (|r||s|)^2$. Последнее равенство выполнено, поскольку левая и правая его части равны r^2s^2.

Докажем неравенство (5). Из неравенства $rs \leqslant |r||s|$ следует неравенство $r^2 + 2rs + s^2 \leqslant r^2 + 2|r||s| + s^2$. Это неравенство с использованием свойства (2) можно переписать в виде $|r + s|^2 \leqslant$ $\leqslant (|r|+|s|)^2$. Поскольку $|r+s|$ и $|r|+|s|$ неотрицательны, получаем требуемое неравенство.

3.4. Теорема о делении с остатком

Пусть m и n – целые числа. Говорят, что n *делит* m (обозначение $n \,|\, m$), если $m = un$ для некоторого целого u.

Легко понять, что в кольце целых чисел далеко не всегда одно число делит другое. В связи с этим при изучении свойств целых чисел важное значение имеет следующее утверждение, называемое теоремой о делении с остатком.

Теорема 3.1. *Пусть m, n – произвольные целые числа, причем $n \neq 0$. Тогда существуют такие однозначно определенные числа u, r, что $m = un + r$ и $0 \leqslant r < |n|$.*

Доказательство. Проверим, что такие числа u, r всегда найдутся. Предположим сначала, что m и n – натуральные числа.

Если $m < n$, то, очевидно, $u = 0$, $r = m$. Столь же просто рассматривается случай, когда n делит m. В этом случае $m = un + 0$ для некоторого целого u. Поэтому можно считать, что $m > n$ и n не делит m. Рассмотрим множество

$$R = \{s \mid s \in \mathbb{N} \text{ и } s = m - vn \text{ для некоторого } v \in \mathbb{N}\}.$$

Множество R непусто (ему, например, принадлежит число $m - -n$) и состоит из натуральных чисел. Поэтому в силу теоремы 2.1 множество R имеет наименьший элемент r. Покажем, что $r < n$. Учитывая, что

$$m = un + r \tag{1}$$

для некоторого $u \in \mathbb{Z}$, из предположения $r \geqslant n$ легко получить противоречие. В самом деле, если $r = n$, то из равенства (1) следует, что $m = (u + 1)n$; это невозможно, так как n не делит m. Если допустить, что $r > n$, то $r - n$ – натуральное и $r - n = = m - (u + 1)n$. Таким образом, $r - n \in R$, что противоречит выбору r. Итак, мы нашли числа u, r таким образом, что $m = un + r$ и $0 < r < n$.

Осталось рассмотреть возможность, когда хотя бы одно из чисел m, n не является натуральным. Если $m = 0$, то $u = r = 0$. Пусть $m < 0 < n$. Тогда $-m$ и n – натуральные числа; поэтому $-m = u_1 n + r_1$, $0 \leqslant r_1 < n$. Стало быть,

$$m = -u_1 n - r_1 = (-u_1 - 1)n + (n - r_1). \tag{2}$$

Из равенств (2) видно, что $u = -u_1$, $r = 0$, если $r_1 = 0$, и $u = = -u_1 - 1$, $r = n - r_1$, если $r_1 > 0$.

Пусть $n < 0 < m$. Тогда $m = u_1(-n) + r_1$, $0 \leqslant r_1 < -n$. Легко понять, что $u = -u_1$, $r = r_1$.

Предположим, наконец, что $m, n < 0$. Тогда $-m = u_1(-n) + +r_1$, $0 \leqslant r_1 < -n$. Значит

$$m = u_1 n - r_1 = (u_1 + 1)n + (-n - r_1). \tag{3}$$

Из равенств (3) видно, что $u = u_1$, $r = 0$, если $r_1 = 0$, и $u = u_1 + 1$, $r = -n - r_1$, если $r_1 > 0$.

Проверим единственность требуемых чисел. Пусть

$$m = u_1 n + r_1, \quad m = u_2 n + r_2, \quad 0 \leqslant r_1, r_2 < |n|.$$

Тогда $u_1 n + r_1 = u_2 n + r_2$, откуда $r_1 - r_2 = (u_2 - u_1)n$. Переходя в этом равенстве к абсолютным величинам, получим

$$|r_1 - r_2| = |u_2 - u_1||n|. \tag{4}$$

Если предположить, что $u_1 \neq u_2$, то $|u_2 - u_1| \geqslant 1$; поэтому $|u_2 - -u_1||n| \geqslant |n|$. Нетрудно проверить, что из условия $0 \leqslant \leqslant r_1, r_2 < |n|$ следует неравенство $|r_1 - r_2| < |n|$. Таким образом, предположение $u_1 \neq u_2$ приводит к противоречию: правая часть равенства (4) не меньше $|n|$, а левая строго меньше $|n|$. Стало быть, $u_1 = u_2$, а из равенства (4) следует $r_1 = r_2$.

3.5. Отношение делимости

В 3.4 в кольце $\mathbb{Z}$ было определено отношение делимости: $n \,|\, m$, если $m = un$ для некоторого целого u.

Из определения очевидным образом вытекают следущие свойства отношения делимости.

(D1) $m \,|\, m$;

(D2) если $m \,|\, n$ и $n \,|\, m$, то $|m| = |n|$;

(D3) если $m \,|\, n$ и $n \,|\, p$, то $m \,|\, p$;

(D4) если $m \,|\, n$ и $m \,|\, p$, то $m \,|\, sn + tp$, каковы бы ни были целые s, t;

(D5) если $m \,|\, n_i$, $1 \leqslant i \leqslant k$, то $m \,|\, \sum_{i=1}^{k} s_i n_i$, каковы бы ни были целые s_i, $1 \leqslant i \leqslant k$.

(D6) если $m \,|\, n$, то $|m| \leqslant |n|$.

Особо отметим, что $m \,|\, 0$, каково бы ни было целое число m; с другой стороны, если $0 \,|\, n$, то $n = 0$.

Теперь мы можем обсудить важное для дальнейшего изложения понятие наибольшего общего делителя двух целых чисел.

О п р е д е л е н и е. Число d называется наибольшим общим делителем целых чисел m, n, если выполнены свойства:

(a) $d \,|\, m$ и $d \,|\, n$;

(b) если $c \,|\, m$ и $c \,|\, n$, то $c \,|\, d$.

Нетрудно видеть, что если d – наибольший общий делитель чисел m, n, то тем же свойством обладает и $-d$.

В дальнейшем неотрицательный наибольший общий делитель чисел m, n будет обозначаться (m, n).

Заметим, что из определения наибольшего общего делителя вытекают равенства $(0, n) = (n, 0) = n$, если $n \neq 0$; значение выражения (m, n) при $m = n = 0$ будем считать неопределенным.

Убедимся теперь, что для любых целых $m, n \neq 0$ наибольший общий делитель (m, n) существует. Заметив предварительно, что у взаимно противоположных целых чисел множества делителей совпадают, будем считать, что числа m, n являются натуральными.

Рассмотрим множество

$$D_{m,n} = \{b \,|\, b \in \mathbb{N} \text{ и } b = sm + tn \text{ для некоторых } s, t \in \mathbb{Z}\}.$$

Множество $D_{m,n}$ непусто (почему?) и состоит из натуральных чисел; поэтому оно имеет наименьший элемент d.

Справедливо следующее важное утверждение.

Теорема 3.2. *Для любых натуральных чисел m, n наименьший элемент d множества $D_{m,n}$ равен их наибольшему общему делителю (m, n).*

Доказательство. Проверим сначала, что d является общим делителем чисел m, n. Из того, что $m = 1 \cdot m + 0 \cdot n$, $n = 0 \cdot m + 1 \cdot n$, следуют включения $m, n \in D_{m,n}$. Поэтому достаточно проверить, что d делит любое $a \in D_{m,n}$. По теореме о делении с остатком имеем $a = ud + r$, $0 \leqslant r < d$. Стало быть,

$$r = a - ud. \tag{5}$$

Но $d, a \in D_{m,n}$, поэтому $d = sm + tn$, $a = s_1 m + t_1 n$, где s, t, s_1, t_1 – некоторые целые числа. Подставляя выражения для d и a в равенство (5), получим

$$r = (s_1 - us)m + (t_1 - ut)n. \tag{6}$$

Из равенства (6) видно, что если $r > 0$, то $r \in D_{m,n}$. Полученное включение противоречит выбору числа d поскольку $r < d$. Таким образом, $r = 0$, т. е. $d \,|\, a$.

Пусть теперь $c|m$ и $c|n$. Так как $d = sm+tn$, по свойству (D4) получаем, что $c|d$.

Следствие. *Для любых целых чисел m, n найдутся такие целые числа s, t, что $(m, n) = sm + tn$.*

Отметим следующие свойства наибольшего общего делителя.

Предложение 3.3. *Пусть m, n – произвольные целые числа. Тогда*

(a) $(m, n) = (n, m)$;

(b) $((m, n), p) = (m, (n, p))$;

(c) $(mn, mp) = |m|(n, p)$.

Доказательство. Выполнение свойства (a) очевидно. Проверим свойство (b). Пусть $d = ((m, n), p)$. Тогда d делит все три числа m, n, p, и потому делит m, (n, p); стало быть, d общий делитель этих чисел. Пусть теперь c – произвольный общий делитель чисел m, (n, p). Понятно, что c делит все три числа и, следовательно, делит d. Тем самым показано, что $d = (m, (n, p))$.

Проверку свойства (c) мы оставляем читателю в качестве упражнения.

Замечание. Тот факт, что каждой паре целых чисел ставится в соответствие их наибольший общий делитель, означает, что на $\mathbb{Z}$, кроме операций сложения и умножения, определена еще одна операция – вычисление наибольшего общего делителя. Предложение 3.3 показывает, что эта операция коммутативна и ассоциативна.

Введем важное для дальнейшего изложения понятие взаимно простых чисел.

Определение. Целые числа m, n называются *взаимно простыми*, если $(m, n) = 1$.

Следующее утверждение представляет собой часто используемый критерий взаимной простоты целых чисел.

Теорема 3.3. *Целые числа m, n взаимно просты тогда и только тогда, когда $sm + tn = 1$ для некоторых целых s, t.*

Доказательство. Если m, n взаимно просты, то применяя следствие из теоремы 3.2, сразу получаем равенство $sm + tn = 1$, где s, t – некоторые целые числа

Пусть существуют такие целые s, t, что $sm + tn = 1$. Если $d = (m, n)$, то по свойству (D4) $d \mid sm + tn$; стало быть, $d \mid 1$. Поскольку $d \geqslant 0$, получаем, что $d = 1$. Таким образом, m и n взаимно просты.

Взаимно простые числа обладают рядом полезных свойств. Отметим следующие три свойства.

(1) если $(m, n) = 1$ и $(m, p) = 1$, то $(m, np) = 1$;
(2) если $m \mid n$, $p \mid n$ и $(m, p) = 1$, то $mp \mid n$;
(3) если $m \mid np$ и $(m, n) = 1$, то $m \mid p$.

Доказательство свойств (1) – (3).

Пусть $(m, n) = 1$ и $(m, p) = 1$, тогда $sm + tn = 1$, $um + vp = 1$ для некоторых целых s, t, u, v. Перемножив эти равенства, получим

$$(msu + spv + ntu)m + (tv)np = 1.$$

Так как в скобках стоят целые числа, применение теоремы 3.3 показывает, что числа m и np взаимно просты. Свойство (1) доказано.

Проверим свойство (2). Пусть $m \mid n$, $p \mid n$ и $(m, p) = 1$. Так как m и p взаимно просты, найдутся такие целые s, t, что $sm + tp = 1$, откуда

$$n = s(mn) + t(np). \tag{7}$$

Поскольку $m \mid n$, имеем $mp \mid np$. Аналогично, из $p \mid n$ следует, что $mp \mid mn$. Таким образом, mp делит правую часть равенства (7); следовательно, делит и его левую часть.

Перейдем к доказательству свойства (3). Пусть $m \mid np$ и $(m, n) = 1$. Имеем $sm + tn = 1$, откуда

$$p = smp + tnp. \tag{8}$$

Очевидно, m делит правую часть равенства (8), поэтому делит и левую его часть.

3.6. Алгоритм Евклида

Для отыскания наибольшего общего делителя двух целых чисел используется способ, называемый алгоритмом Евклида[1]. Мы можем ограничиться нахождением наибольшего общего делителя двух натуральных чисел, поскольку взаимно противоположные числа имеют одинаковые наборы делителей.

Рассмотрим натуральные числа m, n. Положим r_1 равным остатку от деления m на n. Если $r_1 > 0$, то пусть r_2 – остаток от деления n на r_1. Допустим теперь, что числа $r_1, r_2, \dots r_i$ уже найдены и $r_i > 0$. Тогда через r_{i+1} обозначим остаток от деления r_{i-1} на r_i. Нетрудно понять, что отличные от нуля остатки образуют убывающую последовательность:

$$r_1 > r_2 > \dots > r_i > r_{i+1} > \dots .$$

Обозначим через R множество таких остатков. Множество R состоит из натуральных чисел, поэтому к нему применима теорема 2.1. Таким образом, в R существует наименьший отличный от нуля остаток r_k. Остаток от деления r_{k-1} на r_k не может принадлежать множеству R, и потому он равен нулю. Следовательно, $r_k \,|\, r_{k-1}$.

Убедимся, что последний отличный от нуля остаток r_k является наибольшим общим делителем чисел m и n. Из теоремы о делении с остаком вытекает, что справедливы следующие равенства

$$\begin{array}{rcl} m & = & u_1 n + r_1, \\ n & = & u_2 r_1 + r_2, \\ r_1 & = & u_3 r_2 + r_3, \\ \dots & \dots & \dots \\ r_{k-2} & = & u_k r_{k-1} + r_k, \\ r_{k-1} & = & u_{k+1} r_k, \end{array} \qquad (9)$$

где $u_1, u_2, \dots, u_k, u_{k+1}$ – некоторые целые числа.

Проверим сначала, что r_k – общий делитель чисел m и n. Используя тот факт, что $r_k \,|\, r_{k-1}$, будем перемещаться по равенствам

[1]Евклид (365 – ок. 300 до н. э.) – выдающийся древнегреческий математик. Автор всемирно известной книги “Начала”, посвященной аксиоматическому изложению геометрии.

(9) снизу вверх начиная с предпоследнего равенства. Перемещаясь по равенствам, мы всякий раз будем находится в одной и той же ситуации: r_k делит каждое из слагаемых в правой части данного равенства, а потому делит его левую часть. Тем самым мы получим, что r_k поочередно делит r_{k-2}, r_{k-3},..., r_2, r_1, n, m.

Пусть теперь c – некоторый общий делитель чисел m, n. Начнем перемещаться по равенствам (9) сверху вниз. Последовательно получаем, что $c|r_1$, $c|r_2$,...,$c|r_{k-1}$, $c|r_k$. Тем самым доказано, что $r_k = (m, n)$.

В качестве примера применим алгоритм Евклида для отыскания наибольшего общего делителя чисел 5967 и 689. Имеем

$$\begin{aligned} 5967 &= 8 \cdot 689 + 455, \\ 689 &= 1 \cdot 455 + 234, \\ 455 &= 1 \cdot 234 + 221, \\ 234 &= 1 \cdot 221 + 13, \\ 221 &= 17 \cdot 13. \end{aligned}$$

Следовательно, наибольший общий делитель чисел 5967 и 689 равен 13.

3.7. Простые числа. Теорема Евклида

В этом разделе мы вернемся к изучению свойств натуральных чисел. Здесь мы сформулируем несколько важных свойств простых чисел и докажем знаменитую теорему Евклида о бесконечности множества всех простых чисел.

Определение. Натуральное число $p > 1$ называется простым, если для любого натурального числа n из соотношения $n|p$ следует, что $n = 1$ или $n = p$.

Таким образом, простое число p имеет в точности два натуральных делителя – 1 и p.

Предложение 3.4. *Пусть p – простое число. Тогда для любого $n \in \mathbb{Z}$ либо p делит n, либо p и n взаимно просты.*

Доказательство. Пусть $d = (p, n)$. Тогда $d \mid p$ и потому $d = p$ или $d = 1$. Если $d = p$, то $p|n$, если же $d = 1$, то $(p, n) = 1$.

Предложение 3.5. *Любое натуральное число $n > 1$ имеет простой делитель.*

Доказательство. Пусть $D = \{q \mid q > 1 \text{ и } q \mid n\}$. Ясно, что D – непустое множество натуральных чисел. В силу теоремы 2.1 множество D имеет наименьший элемент p. Проверим, что p – простое число. Пусть $s \mid p$ и $s > 1$. Так как $p \in D$, имеем $p \mid n$. Стало быть, $s \mid n$, откуда следует включение $s \in D$. Поскольку $s \leqslant p$ и p – наименьший элемент D, получаем равенство $s = p$.

Обозначим через $\mathbb{P}$ множество всех простых чисел. Свойства множества $\mathbb{P}$ интересовали еще математиков Древней Греции. Одним из первых утверждений о свойствах этого множества является следующая теорема, называемая теоремой Евклида.

Теорема 3.4. *Множество $\mathbb{P}$ бесконечно.*

Доказательство. Проверим, что для любого натурального числа $n > 1$ существует простое число p, большее чем n. Пусть $m = n! + 1$ (через $n!$, как обычно, обозначено произведение всех натуральных чисел от 1 до n включительно). Ясно, что $m > 1$; поэтому найдется простое число p, делящее m. Предположим, что $p \leqslant n$. Тогда, очевидно, $p \mid n!$. Стало быть, p является общим делителем чисел $n!$ и $m = n! + 1$. Мы получили противоречие с тем, что эти числа взаимно просты.

Замечание. На самом деле мы доказали, что множество всех простых чисел не является ограниченным сверху. Представляется правдоподобным, что неограниченное сверху множество натуральных чисел бесконечно. Правда, у внимательного читателя может возникнуть вопрос: а что такое бесконечное множество? Ответ на этот вопрос не так прост, как может показаться; к его обсуждению мы еще вернемся.

3.8. Теорема о каноническом представлении

Предложение 3.6. *Любое натуральное число $n > 1$ можно представить в виде произведения простых чисел; такое представление единственно с точностью до перестановки сомножителей.*

Доказательство. Заметим сразу, что предложение очевидным образом выполнено для простых чисел: каждое простое число представляется в виде произведения, состоящего из единственного сомножителя – себя самого.

Для доказательства предложения применим метод математической индукции. При $n = 2$ данное утверждение, разумеется, выполнено, поскольку 2 – простое число.

Пусть $n = k > 2$ и для всех натуральных чисел, меньших k, утверждение выполняется. В силу сделанного выше замечания можно считать, что k – составное число. Пусть p_1 – простой делитель числа k. Тогда $k = p_1 k_1$, причем $1 < k_1 < k$. Применяя предположение индукции, получаем, что

$$k_1 = p_2 p_3 \dots p_s,$$

где $p_2, p_3, \dots, p_s$ – некоторые простые числа. Отсюда следует, что

$$k = p_1 p_2 p_3 \dots p_s.$$

Таким образом, установлена возможность разложения числа k на простые множители.

Убедимся теперь, что такое разложение числа k единственно с точностью до перестановки сомножителей. Пусть

$$k = p_1 p_2 \dots p_s \quad \text{и} \quad k = q_1 q_2 \dots q_t,$$

где $p_1, p_2, \dots p_s, q_1, q_2, \dots, q_t$ – некоторые простые числа. Поскольку k – составное число, в каждом из двух разложений этого числа содержится не менее двух сомножителей, т. е. $s, t \geqslant 2$. Убедимся, что $s = t$ и два указанных выше разложения числа k состоят из одних и тех же сомножителей (возможно, различающихся порядком этих сомножителей). Из равенства

$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_t \tag{10}$$

следует, что простое число p_1 делит произведение $q_1 q_2 \dots q_t$. Отсюда вытекает, что p_1 не является взаимно простым с одним из сомножителей $q_1, q_2, \dots, q_t$. Без ограничения общности можно считать, что p_1 не является взаимно простым с q_1. Тогда p_1 делит

простое число q_1 и, следовательно, $p_1 = q_1$ Поделив обе части равенства (10) на p_1, получим

$$p_2 \dots p_s = q_2 \dots q_t = m.$$

Так как $1 < m < k$, к числу m применимо предположение индукции. В частности, это означает, что разложение числа m на простые множители единственно с точностью до перестановки сомножителей. Следовательно, $s - 1 = t - 1$, откуда $s = t$. Кроме того, $k = p_1 m = q_1 m$, и потому единственность разложения k на простые множители доказана.

В полученном нами разложении натурального числа на простые множители некоторые из множителей могут совпадать. Ясно, произведения совпадающих множителей можно заменить степенями. Таким образом, из предложения 3.6 вытекает утверждение, называемое *теоремой о каноническом представлении.*

Теорема 3.5. *Пусть n – произвольное натуральное число, большее чем 1. Тогда n можно представить в виде произведения натуральных степеней различных простых чисел; такое представление единственно с точностью до перестановки сомножителей.*

3.9. Сравнения

Продолжим изучение свойств целых чисел.

Пусть n – натуральное число и $n > 1$.

Определение. Целые числа a, b *сравнимы по модулю* n, если $n \,|\, a - b$.

Сравнимость чисел a, b по модулю n будет обозначаться одним из двух способов: $a \equiv b \pmod n$ или $a \equiv_n b$; каждая из этих записей называется *сравнением* по модулю n.

Таким образом, для каждого натурального $n > 1$ на множестве $\mathbb{Z}$ определено отношение сравнимости по модулю n.

Свойства сравнений.

(С1) $a \equiv a \pmod n$;

(С2) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$;

(С3) $a \equiv b \pmod n$ и $b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$;
(С4) $a \equiv b \pmod n$ и $c \equiv d \pmod n \Rightarrow a + c \equiv b + d \pmod n$;
(С5) $a \equiv b \pmod n$ и $c \equiv d \pmod n \Rightarrow ac \equiv bd \pmod n$;
(С6) $a \equiv b \pmod n \Leftrightarrow am \equiv bm \pmod{nm}$, $m \in \mathbb{Z}, m \neq 0$;
(С7) если $(m, n) = 1$, то $ma \equiv mb \pmod n \Rightarrow a \equiv b \pmod n$.

Эти свойства легко получаются из определения сравнимости по модулю n.

Непосредственно проверяется и следующее утверждение.

Предложение 3.7. *Целые числа a, b сравнимы по модулю n тогда и только тогда, когда остатки от деления чисел a, b на n совпадают.*

Определение. Пусть A – n-элементное множество. Будем говорить, что A – полная система вычетов по модулю n, если элементы из A попарно несравнимы по модулю n.

Важным примером полной системы вычетов является множество $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Теорема 3.6. *Пусть $A = \{a_1, a_2, \ldots, a_n\}$ – полная система вычетов по модулю n, m – целое число, взаимно простое с n, d – произвольное целое число. Тогда множество*

$$M = \{ma + d \,|\, a \in A\}$$

также является полной системой вычетов по модулю n.

Доказательство. Достаточно проверить, что числа из M попарно несравнимы по модулю n. Предположим, что при $1 \leqslant \leqslant i < j \leqslant n$ выполнено соотношение $ma_i + d \equiv ma_j + d \pmod n$. Отсюда следует, что $n \,|\, m(a_i - a_j)$. Так как m и n взаимно просты, имеем $n \mid a_i - a_j$, т. е. $a_i \equiv a_j \pmod n$. Полученное соотношение противоречит определению полной системы вычетов.

3.10. Кольцо вычетов по модулю n

В предыдущем разделе было введено множество

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Определим на этом множестве операции сложения и умножения. Временно обозначим через $[a]_n$ остаток от деления a на n.

Пусть a, b – произвольные числа из $\mathbb{Z}_n$. Положим $a \oplus b = [a+b]_n$ и $a \odot b = [a \cdot b]_n$.

Прежде чем изучать свойства этих операций при произвольном n, рассмотрим конкретный пример. А именно, построим таблицы сложения и умножения для случая $n = 6$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Обратим внимание читателя на таблицу умножения. Из нее видно, что в $\mathbb{Z}_6$ есть отличные от нуля числа, произведение которых равно нулю (например, $3 \odot 4 = 0$). Такие числа называются *делителями нуля.*

Чтобы получить свойства операции сложения $\oplus$ и операции умножения $\odot$, докажем следующее вспомогательное утверждение.

Лемма 1. *Пусть $a, b \in \mathbb{Z}$. Тогда $[a+b]_n = [a+[b]_n]_n$ и $[a \cdot b]_n = [a \cdot [b]_n]_n$*

Доказательство. Разность $(a+b)-(a+[b]_n)$ равна $b-[b]_n$ и потому делится на n. Из предложения 3.7 следует, что остатки $[a+b]_n$ и $[a+[b]_n]_n$ совпадают. Второе равенство проверяется аналогично.

Теорема 3.7. *Множество $\mathbb{Z}_n$ относительно операций $\oplus$ и $\odot$ является коммутативным кольцом с единицей.*

Доказательство. Проверим, что относительно операции сложения $\oplus$ множество $\mathbb{Z}_n$ является абелевой группой. Коммутативность сложения сразу вытекает из коммутативности сложения на множестве $\mathbb{Z}$. Проверим ассоциативность сложения, т. е. докажем, что

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c.$$

Используя лемму 1, имеем

$$a \oplus (b \oplus c) = [a + [b + c]_n]_n = [a + (b + c)]_n,$$

$$(a \oplus b) \oplus c = [c + [a + b]_n]_n = [c + (a + b)]_n.$$

Таким образом, ассоциативность операции $\oplus$ вытекает из ассоциативности и коммутативности сложения на множестве $\mathbb{Z}$.

Далее, нетрудно понять, что нейтральным элементом для операции $\oplus$ является число 0.

Осталось проверить, что каждый элемент $a \in \mathbb{Z}_n$ имеет противоположный $\ominus a$. Если $a = 0$, то $\ominus a = 0$. Пусть $a \neq 0$. Тогда $\ominus a = n - a$.

Ассоциативность и коммутативность умножения, а также то, что 1 является нейтральным элементом относительно умножения, проверяется аналогично.

Проверку закона дистрибутивности мы также оставляем читателю.

Продолжим изучение операции умножения в кольце $\mathbb{Z}_n$. Из рассмотренного выше примера (кольцо $\mathbb{Z}_6$) видно, что множество ненулевых элементов такого кольца может быть не замкнуто относительно умножения. Выделим в $\mathbb{Z}_n$ подмножество $\mathbb{Z}_n^*$, состоящее из ненулевых элементов и замкнутое относительно умножения.

Пусть $\mathbb{Z}_n^* = \{k \mid k \in \mathbb{Z}_n \text{ и } (k, n) = 1\}$. Иными словами, $\mathbb{Z}_n^*$ состоит из всех элементов кольца $\mathbb{Z}_n$, взаимно простых с n.

Теорема 3.8. *Множество $\mathbb{Z}_n^*$ относительно операции $\odot$ является абелевой группой.*

При доказательстве этой теоремы удобно воспользоваться следующим утверждением.

Предложение 3.8. *Для любого $a \in \mathbb{Z}_n^*$ множество*

$$M == \{a \odot k \mid k \in \mathbb{Z}_n^*\}$$

совпадает с $\mathbb{Z}_n^*$

Доказательство. Пусть k – произвольный элемент из $\mathbb{Z}_n^*$. Поскольку a, k взаимно просты с n, их произведение ak также

взаимно просто с n. Заметим теперь, что $n \mid ak - [ak]_n$. Отсюда немедленно вытекает, что $a \odot k = [ak]_n$ также взаимно просто с n и потому принадлежит $\mathbb{Z}_n^*$. Это рассуждение показывает, что $M \subseteq \mathbb{Z}_n^*$.

Пусть теперь k_1, k_2 – различные элементы из $\mathbb{Z}_n^*$. Проверим, что элементы $a \odot k_1$ и $a \odot k_2$ также различны. Предположим, что $a \odot k_1 = a \odot k_2$; отсюда следует, что $n \mid a(k_1 - k_2)$. Поскольку n и a взаимно просты, имеем $n \mid k_1 - k_2$. Последнее соотношение выполняться не может, так как $0 < |k_1 - k_2| < n$. Тем самым доказано, что множества M и $\mathbb{Z}_n^*$ имеют одно и то же число элементов. Но $M \subseteq \mathbb{Z}_n^*$, поэтому $M = \mathbb{Z}_n^*$.

Доказательство теоремы 3.8. Из предложения 3.8 следует замкнутость множества $\mathbb{Z}_n^*$ относительно умножения $\odot$, а из теоремы 3.7 вытекает его ассоциативность и коммутативность. Легко понять, что $1 \in \mathbb{Z}_n^*$. Осталось проверить, что для любого $a \in \mathbb{Z}_n^*$ найдется такой $b \in \mathbb{Z}_n^*$, что $a \odot b = 1$. Применяя предложение 3.8, мы видим, что умножая элемент a поочередно на элементы из $\mathbb{Z}_n^*$, можно получить все элементы этого множества. Так как $1 \in \mathbb{Z}_n^*$, то для некоторого $b \in \mathbb{Z}_n^*$ получим $a \odot b = 1$.

Начиная с этого места сложение и умножение в кольце вычетов мы будем обозначать обычными символами "$+$" и "$\cdot$". Из контекста всегда будет понятно, идет речь об операциях в кольце $\mathbb{Z}$ или в кольце $\mathbb{Z}_n$.

Пусть p – простое число. Поскольку все числа $1, 2, \ldots, p-1$ в этом случае взаимно просты с p, множество $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ относительно умножения является абелевой группой.

Кольцо с единицей, в котором множество ненулевых элементов относительно операции умножения образует абелеву группу, называется *полем*.

Таким образом, при простом p кольцо $\mathbb{Z}_p$ является полем. Это утверждение имеет многочисленные следствия. Остановися лишь на одном из них.

Теорема 3.9. *Число $p > 1$ является простым тогда и только тогда, когда $p \mid (p-1)! + 1$*

Доказательство. Пусть p – простое число. Докажем, что

$$p \mid (p-1)! + 1. \tag{11}$$

Если $p = 2$ или $p = 3$, то выполнение соотношения (11) очевидно. Поэтому можно считать, что $p \geqslant 5$. Поскольку $\mathbb{Z}_p$ – поле, для каждого числа $x \in \mathbb{Z}_p$ существует такое $y \in \mathbb{Z}_p$, что в $\mathbb{Z}_p$ выполнено равенство $xy = 1$. В кольце $\mathbb{Z}$ этому равенству отвечает сравнение

$$xy \equiv 1 \pmod{p}. \tag{12}$$

Может оказаться, что для некоторых x, $0 \leqslant x \leqslant p-1$, выполнено равенство $y = x$. Найдем все такие x. Если $x^2 \equiv 1 \pmod{p}$, то $p \mid x^2 - 1$, откуда $p \mid (x-1)(x+1)$. Так как p – простое число, имеем $p \mid (x-1)$ или $p \mid (x+1)$. В первом случае имеем равенство $x = 1$, во втором – равенство $x = p-1$. Из доказанного следует, что множество $\{2, 3, \ldots, p-2\}$ разбивается на такие пары, что произведение чисел, входящих в каждую пару, сравнимо с 1 по модулю p. Поэтому

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}. \tag{13}$$

Из равенства (13) немедленно вытекает, что

$$(p-1)! = 1 \cdot (p-1) \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv_p p-1 \equiv_p -1.$$

Стало быть, $p \mid (p-1)! + 1$.

Проверим обратное утверждение. Пусть $p > 1$ и p удовлетворяет соотношению (11). Рассуждая “от противного”, допустим, что p – составное число. Тогда существует такое q, что $1 < q \leqslant p-1$ и $q \mid p$. Ясно, что $q \mid (p-1)!$ и $q \mid (p-1)! + 1$. Но тогда $q \mid 1$, что невозможно. Полученное противоречие доказывает простоту числа p.

Теорему 3.9 часто называют теоремой Вильсона.

3.11. Малая теорема Ферма. Теорема Эйлера

Теорема 3.10. *Если p – простое число и натуральное число a взаимно просто с p, то $a^{p-1} \equiv 1 \pmod{p}$.*

Доказательство. Пусть $r_1, r_2, \ldots, r_{p-1}$ – остатки от деления чисел $1 \cdot a$, $2 \cdot a, \ldots, (p-1) \cdot a$ на p. Ясно, что эти остатки попарно различны, и каждый из них отличен от нуля. Поэтому

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}. \tag{14}$$

Поскольку $k \cdot a \equiv r_k \pmod{p}$ при $1 \leqslant k \leqslant p-1$, перемножая указанные сравнения, получим

$$a^{p-1}(p-1)! \equiv r_1 r_2 \ldots r_{p-1} \pmod{p}. \tag{15}$$

В силу равенства (14) имеем $(p-1)! = r_1 r_2 \ldots r_{p-1}$. Заметим теперь, что числа $(p-1)!$ и p взаимно просты. Поэтому сокращая обе части сравнения (15) на число $(p-1)!$, взаимно простое с модулем, получим $a^{p-1} \equiv 1 \pmod{p}$.

Это утверждение называется малой теоремой Ферма[1]. Обобщением этой теоремы является теорема Эйлера[2]. В формулировке теоремы Эйлера используется функция натурального аргумента, называемая *функцией Эйлера*.

Для натурального числа $n > 1$ обозначим через $\varphi(n)$ количество натуральных чисел, меньших чем n и взаимно простых с n. Если $n = 1$, то положим $\varphi(1) = 1$. Вспоминая определение множества $\mathbb{Z}_n^*$, мы видим, что при $n > 1$ число элементов в $\mathbb{Z}_n^*$ равно $\varphi(n)$.

Таким образом, функция φ определена на множестве всех натуральных чисел; эта функция и называется функцией Эйлера.

Теорема 3.11. *Если a и n – натуральные числа, причем n взаимно просто с a и $n > 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Доказательство. Пусть $k = \varphi(n)$. Рассмотрим множество $\mathbb{Z}_n^* = \{z_1, z_2, \ldots, z_k\}$. Пусть $u_1, u_2, \ldots, u_k$ – остатки от деления на n чисел $az_1, az_2, \ldots, az_k$. Числа $u_1, u_2, \ldots, u_k$ попарно различны, и каждое из них взаимно просто с n. Поэтому $Z_n^* = \{u_1, u_2, \ldots, u_k\}$.

[1] П.Ферма (1601–1665) – выдающийся французский математик, один из основоположников математического анализа и теории вероятностей.

[2] Л.Эйлер (1707–1783) – выдающийся российский математик, один из крупнейших математиков восемнадцатого столетия. Известен своими работами по алгебре, теории чисел, математическому анализу, теоретической механике.

Отсюда следует, что произведения $z_1 z_2 \dots z_k$ и $u_1 u_2 \dots u_k$ совпадают и взаимно просты с n. Перемножая сравнения $az_j \equiv u_j \pmod n$ $(1 \leqslant j \leqslant k)$, получим

$$a^k z_1 z_2 \dots z_k \equiv u_1 u_2 \dots u_k \pmod n. \tag{16}$$

Сократим обе части сравнения (16) на число $z_1 z_2 \dots z_k$. Учитывая, что $k = \varphi(n)$, получим требуемое сравнение.

3.12. Вычисление функции Эйлера

При вычислении значений функции Эйлера принципиально важным является следующее утверждение.

Теорема 3.12. *Если m, n – взаимно простые натуральные числа, то $\varphi(mn) = \varphi(m)\varphi(n)$.*

Доказательство. Из определения функции Эйлера следует, что $\varphi(mn)$ равно числу элементов кольца $\mathbb{Z}_{mn}$, взаимно простых с mn. Расположим элементы кольца $\mathbb{Z}_{mn}$ в виде следующей таблицы:

$$\begin{array}{rrrcr} 0 & 1 & 2 & \dots & m-1 \\ m & m+1 & m+2 & \dots & 2m-1 \\ 2m & 2m+1 & 2m+2 & \dots & 3m-1 \\ \dots & \dots & \dots & \dots & \dots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \dots & nm-1 \end{array} \tag{17}$$

Эта таблица состоит из m столбцов и n строк. Элементы k-го столбца имеют вид $um + k$, где $0 \leqslant u \leqslant n-1$. Легко видеть, что $(um + k, m) = (k, m)$. Отсюда следует, что числа, взаимно простые с m, целиком заполняют столбцы, номера которых взаимно просты с m. Количество таких столбцов равно $\varphi(m)$. Подсчитаем теперь, сколько чисел, взаимно простых с n, содержится в каждом таком столбце. Из теоремы 3.6 следует, что множество $U_k = \{um + k | u \in \mathbb{Z}_n\}$ образует полную систему вычетов по модулю n. Ясно, что количество элементов множества U_k, взаимно простых с n, равно $\varphi(n)$. Таким образом, в таблице содержится

$\varphi(m)\varphi(n)$ чисел, взаимно простых как с m, так и с n. Осталось лишь отметить, что все такие числа и только они взаимно просты с mn.

Пусть $n > 1$. Тогда $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, где $p_1, p_2, \dots p_k$ – различные простые числа. Так как степени различных простых чисел взаимно просты, из теоремы 3.12 получаем

$$\varphi(n) = \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \dots \varphi(p_k^{m_k}).$$

Осталось вычислить $\varphi(p^m)$, где p – простое число. Для этого найдем число элементов множества $\mathbb{Z}_{p^m}$, не являющихся взаимно простыми с p^m. Пусть z такой элемент. Тогда $p \mid z$, т. е. $z = lp$, причем $0 \leqslant l < p^{m-1}$. Стало быть, l принимает p^{m-1} значений. Отсюда следует, что $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$.

Таким образом, окончательно получаем:

$$\varphi(n) = p_1^{m_1-1} p_2^{m_2-1} \dots p_k^{m_k-1}(p_1-1)(p_2-1)\dots(p_k-1) =$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right),$$

где $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$

3.13. Сравнения первой степени

Пусть a, b – целые числа, n – натуральное число, $n > 1$. Рассмотрим сравнение

$$ax \equiv b \pmod{n} \tag{18}$$

и поставим задачу об отыскании всех целочисленных решений этого сравнения.

Прежде всего установим условия, при которых такие решения существуют. Пусть x_0 – решение сравнения (18). Тогда

$$ax_0 = b + nu \tag{19}$$

для некоторого целого u. Обозначим через d наибольший общий делитель чисел a и n. Из равенства (19) видно, что условие $d \mid b$ является необходимым для того, чтобы сравнение (18) имело решения. Как мы увидим позже, это условие является также и достаточным.

Рассмотрим сначала случай, когда $d = 1$, т. е. a и n – взаимно простые числа. Пусть $[b]_n$ – остаток от деления числа b на n. Тогда $[b]_n \in \mathbb{Z}_n$. Из теоремы 3.6 следует, что множество $\{[ax]_n \,|\, x \in \mathbb{Z}_n\}$ совпадает с множеством $\mathbb{Z}_n$, поскольку $\mathbb{Z}_n$, очевидно, является полной системой вычетов. Поэтому найдется такое $x_0 \in \mathbb{Z}_n$, что $[ax_0]_n = [b]_n$. Отсюда

$$ax_0 \equiv b \pmod{n}. \tag{20}$$

Стало быть, сравнение (18) имеет решение x_0. Покажем, что формула

$$x = x_0 + nt,\ t \in \mathbb{Z}, \tag{21}$$

позволяет получить любое решение сравнения (18). В самом деле, если x – решение сравнения (18), то вычитая из (18) сравнение (20), получим $a(x - x_0) \equiv 0 \pmod{n}$, т. е. $n \,|\, a(x - x_0)$. Поскольку a и n взаимно просты, $n \,|\, x - x_0$, откуда следует, что $x = x_0 + nt$ для некоторого целого t. Иными словами, любое решение сравнения (18) имеет вид (21). Проверка обратного утверждения не представляет труда и оставляется читателю.

Решим теперь сравнение (18) в случае, когда $d > 1$. Пусть $a = a_1 d$, $b = b_1 d$ и $n = n_1 d$, причем числа a_1, n_1 взаимно просты. Рассмотрим сравнение

$$a_1 x \equiv b_1 \pmod{n_1} \tag{22}$$

Нетрудно понять, что сравнения (18) и (22) равносильны, т. е. их множества решений совпадают. Сравнение (22) мы уже решать умеем: его множество решений описывается формулой $x = x_0 + n_1 t$, где x_0 – решение сравнения (22), лежащее между 0 и $n_1 - 1$, а t – произвольное целое число.

Приведем пример на решение сравнений. Пусть дано сравнение

$$17x \equiv 55 \pmod{37}. \tag{23}$$

Пользуясь алгоритмом Евклида, найдем такие целые числа u, v, что $17u + 37v = 1$. Имеем

$$37 = 2 \cdot 17 + 3, \qquad 17 = 5 \cdot 3 + 2, \qquad 3 = 1 \cdot 2 + 1.$$

Отсюда

$$1 = 3-1\cdot 2 = 3-1\cdot(17-\cdot 3) = 6\cdot 3-17 = 6(37-2\cdot 17) = 6\cdot 37-13\cdot 17.$$

Таким образом, $17(-13) \equiv 1 \pmod{37}$. Умножая последнее сравнение на 55 и учитывая, что $(-13)55 = -715 \equiv -12 \equiv \equiv 25 \pmod{37}$, получаем, что 25 – единственное решение сравнения (23), принадлежащее $\mathbb{Z}_{37}$. Стало быть, $x = 25 + 37t$, $t \in \mathbb{Z}$.

3.14. Линейные диофантовы уравнения

Пусть a, b, c – произвольные целые числа, причем $a, b \neq 0$. Рассмотрим уранение

$$ax + by = c \tag{24}$$

и поставим задачу о нахождении всех *целочисленных* решений этого уравнения. В этом случае уравнение (24) называется *линейным диофантовым*[1] *уравнением.*

Пусть d – наибольший общий делитель коэффициентов a, b. Ясно, что если уравнение (24) имеет решения, то $d \,|\, c$. Пусть $a = a_1 d$, $b = b_1 d$, $c = c_1 d$. Понятно, что уравнения $a_1 x + b_1 y = c_1$ и $ax + by = c$ равносильны. Поэтому без ограничения можно считать, что в уравнении (24) коэффициенты a, b взаимно просты.

Опишем множество всех решений диофантова уравнения (24)0.

Теорема 3.13. *Пусть $(x_0; y_0)$ – некоторое решение диофантова уравнения $ax + by = c$, причем коэффициенты a, b взаимно просты. Если $(x; y)$ – произвольное решение этого уравнения, то $x = x_0 + bt$, $y = y_0 - at$ для некоторого целого t.*

Доказательство. Подставляя выражения $x_0 + bt$ и $y_0 - at$ вместо x, y в уравнение (24), получим

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 + abt - bat = ax_0 + by_0 = c.$$

Таким образом, числа $x_0 + bt$, $y_0 - at$ образуют решение уравнения (24) при любом целом t.

[1]Одним из первых уравнения с целыми коэффициентами, в которых требуется найти все целочисленные решения, рассматривал древнегреческий математик Диофант (ок. 250 г.).

Пусть $(x; y)$ – произвольное решение диофантова уравнения (24). Тогда $ax + by = c$. Кроме того, $ax_0 + by_0 = c$. Отсюда

$$a(x - x_0) + b(y - y_0) = 0. \tag{25}$$

Поскольку a и b взаимно просты, из равенства (25) видно, что $b \mid x - x_0$, т. е. $x - x_0 = bt$ для некоторого целого t. Из равенства (25) теперь имеем $abt + b(y - y_0) = 0$, откуда $y - y_0 = -at$. Тем самым проверено, что любое решение диофантова уравнения имеет указанный в теореме (3.13) вид.

Решим, например, диофантово уравнение $13x + 41y = 8$. Выражая x через y, получим

$$x = \frac{8 - 41y}{13} = -3y + \frac{8 - 2y}{13}. \tag{26}$$

Так как x, $-3y$ – целые числа, число 13 должно делить $8 - 2y$. Поэтому $8 - 2y = 13z$ для некоторого целого z, откуда

$$y = \frac{8 - 13z}{2} = 4 - 7z + \frac{z}{2}. \tag{27}$$

Из равенства (27) следует, как и выше, что $z = 2t$. Теперь

$$y = 4 - 7(2t) + t = 4 - 13t.$$

Из равенства (26) окончательно получаем

$$x = -3(4 - 13t) + 2t = -12 + 41t.$$

3.15. О числовых системах

Понятие числа является одним из основных в математике. Этим объясняется внимание, которое мы уделили натуральным и целым числам. Напомним, что в первой главе при помощи аксиом Пеано было введено множество всех натуральных чисел и определены операции сложения и умножения на нем. Обе эти операции обладают свойствами коммутативности, ассоциативности и сократимости, умножение имеет нейтральный элемент 1 и дистрибутивно относительно сложения. Оказалось, однако, что во множестве $\mathbb{N}$ не всегда разрешимо уравнение $x + m = n$ (по другому, не для

любых натуральных чисел m, n определена их разность). Чтобы устранить этот недостаток, мы добавили к натуральным числам ноль и целые отрицательные числа, получив, таким образом, множество всех целых чисел $\mathbb{Z}$. На множестве $\mathbb{Z}$ нам пришлось доопределить операции сложения и умножения. Замечательным является тот факт, что сложение и умножение на множестве $\mathbb{Z}$ сохранили все свойства соответствующих операций на множестве $\mathbb{N}$. Итак, *сложение и умножение натуральных чисел могут быть распространены на целые числа с сохранением свойств.* Оказывается, что множество $\mathbb{Z}$ относительно операции сложения является абелевой группой, отсюда, в частности, вытекает разрешимость уравнения $x + m = n$ во множестве $\mathbb{Z}$. Напомним также, что относительно операций сложения и умножения множество $\mathbb{Z}$ образует коммутативное кольцо с единицей.

Следующий шаг, который предстоит сделать, – это переход от целых чисел к рациональным. Необходимость введения рациональных чисел мотивируется тем, что в кольце $\mathbb{Z}$ не для всех m, n разрешимо уравнение $mx = n$. Так же, как и выше, мы определяем новое числовое множество $\mathbb{Q}$, называемое множеством всех рациональных чисел и состоящее из всех обыкновенных дробей, т. е. выражений вида m/n, где $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Пусть k – произвольное целое число. Если $m = kn$, где n – натуральное число, то k представимо дробью m/n. Следовательно, можно считать, что $\mathbb{Z} \subset \mathbb{Q}$. Формулы

$$\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}, \qquad \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$$

позволяют распространить сложение и умножение целых чисел на рациональные чисел с сохранением свойств. В частности, множество $\mathbb{Q}$ относительно операции сложении является абелевой группой. Кроме того, множество $\mathbb{Q}\setminus\{0\}$ – абелева группа относительно операции умножения. Стало быть, множество всех рациональных чисел образует поле. Нетрудно понять, что в поле рациональных чисел разрешимо любое линейное уравнение $ax + b = c$ при $a \neq 0$. Однако легко привести пример квадратного уравнения с положительным дискриминантом, не имеющего решений в поле $\mathbb{Q}$. Например, хорошо известно, что среди рациональных чисел нет тако-

го, квадрат которого был бы равен 2. Это означает, что уравнение $x^2 = 2$ не имеет решений в поле $\mathbb{Q}$. Чтобы получить возможность решать квадратные уравнения с положительным дискриминантом (а на самом деле и уравнения более высоких степеней), следует добавить к рациональным числам новые числа – иррациональные. Но каким образом это можно сделать? Здесь следует вспомнить, что каждую обыкновенную дробь можно представить бесконечной десятичной периодической дробью. Теперь можно ввести в рассмотрение множество $\mathbb{R}$, состоящее из всевозможных (не обязательно периодических) бесконечных десятичных дробей. Множество $\mathbb{R}$ называют множеством всех действительных чисел, а иррациональные числа – это как раз бесконечные непериодические десятичные дроби. Оказывается, операции сложения и умножения на $\mathbb{Q}$ можно распространить с сохранением свойств на множество $\mathbb{R}$ (сейчас мы не будем обсуждать, как это сделать). Таким образом, множество всех действительных чисел является полем относительно операций сложения и умножения. Это поле по сравнению с полем $\mathbb{Q}$ обладает важным дополнительным свойством: в нем любое ограниченное множество имеет точную верхнюю грань. Отсюда, в частности, можно получить следующее утверждение: в поле $\mathbb{R}$ любое уравнение $x^n = a$ ($n \in \mathbb{N}$, $a \in \mathbb{R}$, $a > 0$) имеет решение. Строгое обоснование вопросов, связанных с построением поля $\mathbb{Q}$ и поля $\mathbb{R}$ мы отложим до 11 класса. А пока договоримся, что известными нам свойствами рациональных и действительных чисел мы будем пользоваться без каких-либо оговорок.

4. Неравенства

4.1. Неравенство между средним арифметическим и средним геометрическим

Пусть a_1, a_2 – произвольные положительные числа. Из очевидного неравенства $(\sqrt{a_1} - \sqrt{a_2})^2 \geqslant 0$ легко получить, что

$$\sqrt{a_1 a_2} \leqslant \frac{a_1 + a_2}{2}, \tag{1}$$

причем равенство имеет место тогда и только тогда, когда $a_1 = = a_2$.

В этом разделе неравенство (1) обобщается на случай n положительных чисел.

Итак, пусть $a_1, a_2, \ldots, a_n$ – произвольные положительные числа. Рассмотрим их среднее геометрическое

$$G_n = \sqrt[n]{a_1 a_2 \ldots a_n}$$

и среднее арифметическое

$$A_n = \frac{a_1 + a_2 + \ldots + a_n}{n}.$$

Справедливо следующее утверждение.

Теорема 4.1. *Пусть $a_1, a_2, \ldots, a_n$ – произвольные положительные числа. Тогда*

$$\sqrt[n]{a_1 a_2 \ldots a_n} \leqslant \frac{a_1 + a_2 + \ldots + a_n}{n},$$

причем знак равенства имеет место в том и только том случае, когда $a_1 = a_2 = \ldots = a_n$.

Чтобы доказать теорему 4.1, нам понадобится вспомогательное утверждение.

Предложение 4.1. *Пусть $x_1, x_2, \ldots, x_n$ – такие положительные числа, что $x_1 x_2 \ldots x_n = 1$. Тогда $x_1 + x_2 + \ldots + x_n \geqslant n$, причем равенство выполнено тогда и только тогда, когда $x_1 = = x_2 = \ldots x_n = 1$.*

Доказательство. Применим метод математической индукции.

Если $n = 1$, то утверждение очевидно. Пусть при $n = k \geqslant 1$ утверждение выполнено. Проверим, что оно истинно и при $n = k+$ $+1$. Возьмем произвольные положительные числа $x_1, x_2, \ldots, x_k$, x_{k+1} и предположим, что

$$x_1 x_2 \ldots x_k x_{k+1} = 1. \tag{2}$$

Возможны два случая.

1. Все числа $x_1, x_2, \ldots, x_k, x_{k+1}$ равны между собой. Тогда из равенства (2) вытекает, что все они равны 1; поэтому

$$x_1 + x_2 + \ldots + x_{k-1} + x_k + x_{k+1} = k + 1.$$

2. Среди чисел $x_1, x_2, \ldots, x_k, x_{k+1}$ есть различные. Ясно, что тогда найдутся два числа, одно из которых меньше, а другое больше 1. Без ограничения общности можно считать, что $x_k <$ < 1, а $x_{k+1} > 1$. Применив предположение индукции к числам $x_1, x_2, \ldots, x_{k-1}, x_k x_{k+1}$, приходим к неравенству

$$x_1 + x_2 + \ldots + x_{k-1} + x_k x_{k+1} \geqslant k, \tag{3}$$

откуда следует неравенство

$$x_1 + x_2 + \ldots + x_{k-1} + x_k + x_{k+1} \geqslant k + x_k + x_{k+1} - x_k x_{k+1}. \tag{4}$$

Напомним теперь, что $x_k < 1$ и $x_{k+1} > 1$. Из этих неравенств вытекает, что числа $1 - x_k$ и $x_{k+1} - 1$ положительны. Поэтому

$$(1 - x_k)(x_{k+1} - 1) > 0.$$

Раскрывая в произведении скобки и переставляя слагаемые, получим

$$x_k + x_{k+1} - x_k x_{k+1} - 1 > 0,$$

откуда

$$x_k + x_{k+1} - x_k x_{k+1} > 1. \tag{5}$$

Из неравенств (3) и (5) следует, что

$$x_1 + x_2 + \ldots + x_{k-1} + x_k + x_{k+1} > k + 1.$$

Доказательство теоремы 4.1. Пусть $a_1, a_2, \ldots, a_n$ – произвольные положительные числа, G_n – их среднее геометрическое. Рассмотрим числа $x_i = a_i/G_n$ $(1 \leqslant i \leqslant n)$. Числа x_i положительны и $x_1 x_2 \ldots x_n = 1$. Поэтому $x_1 + x_2 + \ldots + x_n \geqslant n$. Стало быть,

$$\frac{a_1 + a_2 + \ldots + a_n}{G_n} \geqslant n. \tag{6}$$

Из неравенства (6) немедленно следует, что

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \geqslant G_n.$$

4.2. Неравенство Коши–Буняковского

Целью данного раздела является доказательство следующего утверждения.

Теорема 4.2. *Пусть $a_1, a_2, \ldots, a_n,\ b_1, b_2, \ldots, b_n$ – произвольные числа Тогда*

$$|a_1 b_1 + a_2 b_2 + \ldots + a_n b_n| \leqslant \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}\sqrt{b_1^2 + b_2^2 + \ldots + b_n^2}.$$

причем равенство выполнено в том и только том случае, когда либо все числа $a_1, a_2, \ldots, a_n$ равны нулю, либо найдется такое число t, что $b_i = t a_i$ при любом i, $1 \leqslant i \leqslant n$.

Доказательство. Неравенство выполнено, если все числа $a_1, a_2, \ldots, a_n$ равны нулю. Пусть хотя бы одно из чисел $a_1, a_2, \ldots, a_n$ отлично от нуля. Рассмотрим выражение

$$q(x) = (xa_1 - b_1)^2 + (xa_2 - b_2)^2 + \ldots + (xa_n - b_n)^2, \tag{7}$$

где x – переменная.

Введем обозначения:

$$A = a_1^2 + a_2^2 + \ldots + a_n^2,\ B = b_1^2 + b_2^2 + \ldots + b_n^2,\ C = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n.$$

После раскрытия скобок и приведения подобных членов в выражении (7), оно запишется в виде

$$q(x) = Ax^2 - 2Cx + B.$$

Поскольку $A \neq 0$, выражение $q(x)$ является квадратным трехчленом. Замечая, что $q(x)$ записывается в виде суммы квадратов, нетрудно понять, что $q(x)$ принимает неотрицательные значения при всех значениях x. Следовательно, дискриминант $4C^2 - 4AB$ квадратного трехчлена $q(x)$ неположителен, т. е. $C^2 - AB \leqslant 0$. Отсюда $C^2 \leqslant AB$. Извлекая из обеих частей последнего неравенства квадратный корень, получим

$$|C| \leqslant \sqrt{A}\sqrt{B}. \tag{8}$$

Вспоминая введенные выше обозначения, мы видим, что требуемое неравенство доказано.

Если неравенство (8) обращается в равенство, то дискриминант квадратного трехчлена $q(x)$ равен нулю. В этом случае существует такое действительное число t, что $q(t) = 0$. Следовательно,

$$q(t) = (ta_1 - b_1)^2 + (ta_2 - b_2)^2 + \ldots + (ta_n - b_n)^2 = 0.$$

Мы знаем, что сумма квадратов действительных чисел равна нулю тогда и только тогда, когда каждое из этих чисел равно нулю. Таким образом, $ta_i - b_i = 0$, т. е. $b_i = ta_i$ при всех $1 \leqslant i \leqslant n$.

Тот факт, что при выполнении указанного условия неравенство Коши-Буняковского обращается в равенство, читатель без труда проверит самостоятельно.

При $n = 2$ неравенство Коши–Буняковского имеет очень простой геометрический смысл. Пусть $\overrightarrow{a} = (a_1, a_2)$, $\overrightarrow{b} = (b_1, b_2)$ – ненулевые векторы на плоскости. Вычисляя скалярное произведение и длины этих векторов, находим $(\overrightarrow{a}, \overrightarrow{b}) = a_1b_1 + a_2b_2$, $|\overrightarrow{a}| = \sqrt{a_1^2 + a_2^2}$, $|\overrightarrow{b}| = \sqrt{b_1^2 + b_2^2}$. Таким образом, неравенство Коши–Буняковского в этом случае можно записать в виде

$$|(\overrightarrow{a}, \overrightarrow{b})| \leqslant |\overrightarrow{a}||\overrightarrow{b}|. \tag{9}$$

Выполнение неравенства (9) очевидно, поскольку

$$(\overrightarrow{a}, \overrightarrow{b}) = |\overrightarrow{a}||\overrightarrow{b}| \cos\varphi,$$

где φ – угол между векторами $\overrightarrow{a}$ и $\overrightarrow{b}$.

4.3. Неравенство между средним арифметическим и средним квадратичным

Для произвольных чисел $a_1, a_2, \ldots, a_n$ рассмотрим их среднее квадратичное

$$Q_n = \sqrt{\frac{a_1^2 + a_2^2 + \ldots + a_n^2}{n}}.$$

Справедливо следующее утверждение.

Теорема 4.3. *Пусть $a_1, a_2, \ldots, a_n$ – положительные числа. Тогда*

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \leqslant \sqrt{\frac{a_1^2 + a_2^2 + \ldots + a_n^2}{n}}, \tag{10}$$

причем знак равенства имеет место в том и только том случае, когда $a_1 = a_2 = \ldots = a_n$.

Доказательство. Рассмотрим числа $b_i = 1/\sqrt{n}$ $(1 \leqslant i \leqslant n)$ и применим неравенство Коши–Буняковского к наборам чисел $a_1, a_2, \ldots, a_n,\ b_1, b_2, \ldots, b_n$. Поскольку $b_1^2 + b_2^2 + \ldots + b_n^2 = 1$, имеем

$$\frac{a_1 + a_2 + \ldots + a_n}{\sqrt{n}} \leqslant \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}. \tag{11}$$

Из теоремы 4.2 следует, что неравенство (11) обращается в равенство тогда и только тогда, когда $a_1 = a_2 = \ldots = a_n$.

Поделив обе части неравенства (11) на $\sqrt{n}$, получим требуемое неравенство между средним арифметическим и средним квадратичным.

4.4. Неравенство Бернулли

В этом разделе мы докажем неравенство Бернулли[1]. Это неравенство, наряду с неравенством между средним геометрическим и средним арифметическим, часто применяется как при решении задач, так и при получении теоретических результатов.

Сначала рассмотрим один частный случай неравенства Бернулли.

[1]Династия швейцарских математиков, основателями которой были братья Якоб Бернулли (1654–1705) и Иоганн Бернулли (1667–1748). Рассматриваемое неравенство приписывают Якобу Бернулли.

Предложение 4.2. *Пусть $x > -1$ и n – натуральное число, $n \geqslant 2$. Тогда*

$$(1+x)^n \geqslant 1 + nx,$$

причем равенство имеет место только при $x = 0$.

Доказательство. Применим метод математической индукции. Если $n = 2$, то

$$(1+x)^2 = 1 + 2x + x^2 \geqslant 1 + 2x.$$

Ясно, что равенство выполнено только если $x = 0$.

Предположим, что при $n = k \geqslant 2$ утверждение выполнено. Проверим, что оно истинно и при $n = k+1$. Поскольку $1 + x \geqslant 0$, имеем

$$(1+x)^{k+1} = (1+x)^k(1+x) \geqslant (1+kx)(1+x) =$$

$$= 1 + (k+1)x + kx^2 \geqslant 1 + (k+1)x.$$

Осталось заметить, что в этой цепочке нестрогие неравенства становятся равенствами лишь при $x = 0$.

Теперь мы обобщим доказаное неравенство. Пусть $x > -1$, $x \neq \neq 0$, r – произвольное рациональное число.

Лемма 1. *Если $0 < r < 1$, то $(1+x)^r < 1 + rx$.*

Доказательство. Поскольку r – рационально, $r = m/n$, где m, n – натуральные числа и $m < n$. Тогда

$$(1+x)^r = (1+x)^{m/n} = \sqrt[n]{(1+x)^m} =$$

$$= \sqrt[n]{\underbrace{1 \cdot 1 \ldots 1}_{n-m} \cdot \underbrace{(1+x)(1+x)\ldots(1+x)}_{m}}.$$

Мы видим, что $(1+x)^r$ является средним геометрическим n чисел, из которых $n - m$ чисел равно 1, а m чисел совпадает с $1 + x$. Применяя неравенство между средним геометрическим и средним арифметическим, получим

$$(1+x)^r < \frac{(n-m) + (1+x)m}{n} = \frac{n + xm}{n} = 1 + \frac{n}{m}x = 1 + rx.$$

Лемма 2. *Если* $r > 1$, *то* $(1+x)^r > 1 + rx$.

Доказательство. Если $1 + rx \leqslant 0$, то доказываемое неравенство очевидно. Пусть $1 + rx > 0$. Поскольку $0 < 1/r < 1$, в силу леммы 1 получаем

$$(1 + rx)^{1/r} < 1 + x. \tag{12}$$

Возводя неравенство (12) в положительную степень r, получим

$$1 + rx < (1 + x)^r.$$

Лемма 3. *Если* $r < 0$, *то* $(1+x)^r > 1 + rx$.

Доказательство. Если $1+rx \leqslant 0$, то неравенство очевидно. Пусть $1 + rx > 0$. Найдем нечетное натуральное число n так, что выполнено неравенство $-r/n < 1$. В силу леммы 1 получаем

$$(1 + x)^{-r/n} < 1 - \frac{r}{n}x. \tag{13}$$

Заметим теперь, что

$$1 - \frac{r}{n}x > 0.$$

В самом деле, это неравенство очевидно, если $x > 0$. Если же $-1 < x < 0$, то $rx/n > 0$, и потому $rx/n = |r/n||x| < 1$; значит, $1-rx/n > 0$. Возьмем теперь очевидное неравенство $1-r^2x^2/n^2 < < 1$; поделив обе части этого неравенства на положительное число $1 - rx/n$, получим

$$\frac{1}{1 - \dfrac{r}{n}x} > 1 + \frac{r}{n}x. \tag{14}$$

Из неравенств (13) и (14) получаем

$$(1 + x)^{r/n} > \frac{1}{1 - \dfrac{r}{n}x} > 1 + \frac{r}{n}x.$$

Возводя обе части неравенства

$$(1 + x)^{r/n} > 1 + \frac{r}{n}x$$

в нечетную степень n, окончательно имеем

$$(1 + x)^r > \left(1 + \frac{r}{n}x\right)^n > 1 + rx.$$

Из лемм 1 – 3 вытекает

Теорема 4.4. *Пусть $x > -1$ и r – рациональное число. Если $r < 0$ или $r > 1$, то*

$$(1+x)^r \geqslant 1 + rx; \tag{15}$$

если же $0 < r < 1$, то

$$(1+x)^r \leqslant 1 + rx. \tag{16}$$

В обоих случаях равенство имеет место только, если $x = 0$.

Каждое из неравенств (15), (16) называют неравенством Бернулли.

Иногда неравенство Бернулли удобно применять в следующем виде. Пусть $x > 0$. Если $r > 1$ или $r < 0$, то из теремы 4.4 следует, что

$$x^r = (1 + (x-1))^r \geqslant 1 + r(x-1) = 1 - r + rx.$$

Таким образом,

$$x^r \geqslant 1 - r + rx. \tag{17}$$

Аналогично при $0 < r < 1$ получаем

$$x^r \leqslant 1 - r + rx. \tag{18}$$

Ясно, что равенство в обоих случаях имеет место лишь при $x = 1$.

4.5. Неравенства между средними степенными

О п р е д е л е н и е. Пусть $a_1, a_2, \ldots, a_n$ – произвольные положительные числа. Число

$$S_\alpha = \left(\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n} \right)^{\frac{1}{\alpha}}$$

называется *средним степенным* порядка α этих чисел.

Нетрудно видеть, что средние степенные порядков 1 и 2 совпадают со средним арифметическим и средним квадратичным соответственно.

Среднее степенное данного порядка от n положительных чисел легко сравнить с их средним геометрическим. В самом деле,

$$\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n} \geqslant \sqrt[n]{a_1^\alpha a_2^\alpha \ldots a_n^\alpha} \geqslant (\sqrt[n]{a_1 a_2 \ldots a_n})^\alpha \tag{19}$$

Если $\alpha > 0$, то из (19) получаем

$$\left(\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n}\right)^{\frac{1}{\alpha}} \geqslant \sqrt[n]{a_1 a_2 \ldots a_n},$$

если же $\alpha < 0$, то

$$\left(\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n}\right)^{\frac{1}{\alpha}} \leqslant \sqrt[n]{a_1 a_2 \ldots a_n}.$$

Теперь покажем, что при $\alpha > 1$ выполнено неравенство

$$\left(\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n}\right)^{\frac{1}{\alpha}} \geqslant \frac{a_1 + a_2 + \ldots + a_n}{n}. \tag{20}$$

В самом деле, пусть $b_i = \left(\dfrac{a_i}{S_\alpha}\right)^\alpha$. Тогда

$$b_1 + b_2 + \ldots + b_n = \frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{S_\alpha^\alpha} = n. \tag{21}$$

Воспользуемся неравенством (18). Имеем

$$b_i^{\frac{1}{\alpha}} \leqslant 1 - \frac{1}{\alpha} + \frac{b_i}{\alpha} \tag{22}$$

при $1 \leqslant i \leqslant n$. Суммируя неравенства (22) по всем i от 1 до n, с учетом равенства (21) получим

$$b_1^{\frac{1}{\alpha}} + b_2^{\frac{1}{\alpha}} + \ldots + b_n^{\frac{1}{\alpha}} \leqslant \left(1 - \frac{1}{\alpha}\right) n + \frac{n}{\alpha} = n. \tag{23}$$

Вспоминая определение чисел b_i, из (23) находим

$$\frac{a_1 + a_2 + \ldots + a_n}{S_\alpha} \leqslant n,$$

откуда легко следует неравенство (20).

Теперь мы в состоянии доказать следующее утверждение.

Теорема 4.5. *Пусть числа α, β отличны от нуля. Если $\alpha < \beta$, то среднее степенное порядка α не превосходит среднего степенного порядка β.*

Доказательство. В зависимости от знаков чисел α и β возникает три случая.

Если $\alpha < 0 < \beta$, то средние степенные порядков α и β разделены, как было отмечено выше, средним геометрическим.

Предположим, что $0 < \alpha < \beta$. Тогда $\beta/\alpha > 1$, и мы можем применить неравенство (20) к числам $a_1^\alpha, a_2^\alpha, \ldots, a_n^\alpha$ и среднему степенному этих чисел порядка $\beta/\alpha > 1$. Имеем

$$\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n} \leqslant \left(\frac{a_1^\beta + a_2^\beta + \ldots + a_n^\beta}{n} \right)^{\frac{\alpha}{\beta}}.$$

Возводя обе части последнего неравенства в положительную степень $1/\alpha$, получим требуемое неравенство.

Пусть теперь $\alpha < \beta < 0$. В этом случае $\alpha/\beta > 1$, и неравенство (20) следует применить к числам $a_1^\beta, a_2^\beta, \ldots, a_n^\beta$ и среднему степенному этих чисел порядка $\alpha/\beta > 1$. Тогда

$$\frac{a_1^\beta + a_2^\beta + \ldots + a_n^\beta}{n} \leqslant \left(\frac{a_1^\alpha + a_2^\alpha + \ldots + a_n^\alpha}{n} \right)^{\frac{\beta}{\alpha}}.$$

Если обе части этого неравенства возвести в отрицательную степень $1/\beta$, то опять получится нужное неравенство.

4.6. Применение неравенств для отыскания наибольших и наименьших значений

Рассмотрим несколько задач на отыскание наибольших и наименьших значений.

1. Для каждого положительного a найти наибольшее значение выражения $f(x) = ax^2 - x^3$ на отрезке $[0; a]$.

□ Применив неравенство между средним геометрическим и средним арифметическим к трем неотрицательным числам $x/2$, $x/2$ и $a - x$, получим

$$\sqrt[3]{\frac{x}{2} \cdot \frac{x}{2} \cdot (a - x)} \leqslant \frac{a}{3},$$

причем равенство имеет место, когда $x/2 = a - x$, т. е. $x = 2a/3$. Стало быть,

$$ax^2 - x^3 = x^2(a - x) \leqslant \frac{4a^3}{27}.$$

Поскольку $f(2a/3) = 4a^3/27$, имеем $\max\limits_{[0;a]} f(x) = 4a^3/27$. $\square$

2. Для каждого положительного a найти наибольшее значение выражения $g(x) = a^2x - x^3$ на отрезке $[0; a]$.

$\square$ Рассмотрим неотрицательные числа

$$\sqrt{2}x, \quad \sqrt{a^2 - x^2}, \quad \sqrt{a^2 - x^2}$$

и воспользуемся тем, что среднее геометрическое этих чисел не превосходит их среднего квадратичного. Имеем

$$\sqrt[3]{\sqrt{2}x \cdot \sqrt{a^2 - x^2} \cdot \sqrt{a^2 - x^2}} \leqslant \sqrt{\frac{2x^2 + a^2 - x^2 + a^2 - x^2}{3}} = a\sqrt{\frac{2}{3}}.$$

Отсюда

$$g(x) = x(a^2 - x^2) \leqslant \frac{2a^3}{3\sqrt{3}},$$

причем равенство достигается, если $\sqrt{2}x = \sqrt{a^2 - x^2}$, т. е. $x = a/\sqrt{3}$. Таким образом, $\max\limits_{[0;a]} g(x) = 2a^3/(3\sqrt{3})$. $\square$

3. Пусть a, b – произвольные положительные, n, m – натуральные числа. Найдем наименьшее значение выражения

$$h(x) = ax^n + \frac{b}{x^m}$$

на луче $(0; +\infty)$.

$\square$ Определим числа $c_1, c_2, \ldots, c_{m+n}$ следующим образом:

$$c_1 = \ldots = c_m = \frac{ax^n}{m}, \qquad c_{m+1} = \ldots = c_{m+n} = \frac{b}{nx^m}.$$

Тогда

$$h(x) = c_1 + c_2 + \ldots + c_{m+n}$$

и

$$c_1c_2 \ldots c_{m+n} = \frac{a^m b^n}{m^m n^n}.$$

Применяя к числам c_i, $1 \leqslant i \leqslant m+n$, неравенство между средним арифметическим и средним геометрическим, получим

$$h(x) \geqslant (m+n) \sqrt[m+n]{\frac{a^m b^n}{m^m n^n}},$$

причем равенство выполнено, если $ax^n/m = b/(nx^m)$. $\square$

5. Отображения множеств

5.1. Определение отображения

Пусть X, Y – произвольные непустые множества.

О п р е д е л е н и е. Отображение f из множества X во множество Y – это правило, при помощи которого каждому элементу $x \in X$ ставится в соответствие однозначно определенный элемент $y \in Y$.

Множество X называется *областью определения* отображения f; множество Y – его *областью значений*.

Синонимичные записи $f : X \longrightarrow Y$ и $X \xrightarrow{f} Y$ выражают тот факт, что f является отображением из X в Y.

Элемент $y \in Y$, который при помощи отображения f поставлен в соответствие элементу $x \in X$, называется *образом* элемента x и обозначается через $f(x)$; в той же ситуации элемент x называется *прообразом* элемента y. *Полным прообразом* $f^{-1}(y)$ элемента y будем называть множество всех прообразов y. Из определения отображения вытекает, что полные прообразы различных элементов не имеют общих элементов.

Заметим, что в том случае, когда X, Y – числовые множества, отображение f из X в Y назывется числовой функцией; если при этом f задано при помощи алгебраического выражения, то, как правило, используется запись $y = f(x),\ x \in X$.

В дальнейшем часто будет возникать ситуация, когда область определения X и область значений Y данного отображения f совпадают. В таком случае f называют *преобразованием* множества X.

Если A – произвольное подмножество множества X, то множество

$$f(A) = \{y \,|\, y = f(x) \text{ для некоторого } x \in A\}$$

называется *образом* множества A при отображении f.

Образ $f(X)$ всей области определения X называется *множеством значений* отображения f.

Часто область определения и множество значений отображения f мы будем обозначать через $D(f)$ и $E(f)$ соответственно.

Рассмотрим теперь следующие три типа отображений.

О п р е д е л е н и е. Отображение f из X в Y называется *инъективным*, если для любых $x_1, x_2 \in X$ из неравенства $x_1 \neq x_2$ следует неравенство $f(x_1) \neq f(x_2)$.

Заметим, что свойство, высказанное в этом определении, может быть выражено следующим образом: для любых $x_1, x_2 \in X$ из равенства $f(x_1) = f(x_2)$ следует равенство $x_1 = x_2$.

О п р е д е л е н и е. Отображение f из X в Y называется *сюръективным*, если множество значений $f(X)$ совпадает с областью значений Y.

С использованием понятия полного прообраза, это определение можно сформулировать по-другому. А именно, отображение f из X в Y сюръективно, если полный прообраз произвольного элемента $y \in Y$ является непустым множеством.

О п р е д е л е н и е. Отображение f из X в Y называется *биективным*, если оно сюръективно и инъективно одновременно.

Приведем примеры отображений.

1. Пусть T – множество всех треугольников плоскости, $\mathbb{R}^+$ – множество всех положительных чисел. Тогда правило, сопоставляющее каждому треугольнику t его площадь $s(t)$, задает отображение $s : T \longrightarrow \mathbb{R}^+$.

2. Пусть S – множество точек полуокружности с центром O без граничных точек, L – множество точек касательной прямой (рис. 1). Для каждой точки X полукружности обозначим через $f(X)$ такую точку прямой, что O, X, $f(X)$ лежат на одной прямой. Ясно, что $f : S \longrightarrow L$ является отображением.

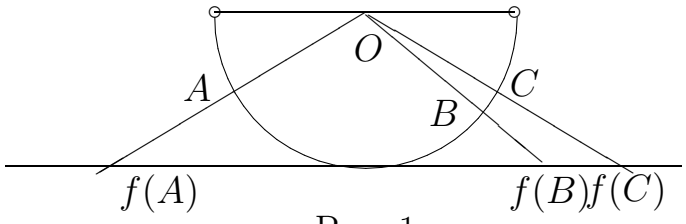

Рис. 1

3. Пусть $X = (-\infty; 3]$. Тогда правило $q(x) = \sqrt{3 - x}$ задает отображение из X в $\mathbb{R}$.

4. Пусть $X = \{1, 2, 3, 4\}$, $Y = \{7, 8, 9\}$. Зададим отображение f

следующим образом:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 9 & 8 & 7 & 8 \end{pmatrix}.$$

Эта запись означает, что $f(1) = 9$, $f(2) = 8$, $f(3) = 7$, $f(4) = 8$. По существу, мы задали указанное отображение таблицей.

5. Пусть X – произвольное непустое множество. Всегда существует тождественное преобразование ε_X множества X, определенное правилом $\varepsilon_X(x) = x$ для любого $x \in X$.

Между свойствами инъективности и сюръективности имеется связь. А именно, справедливо следующее утверждение.

Предложение 5.1. *Пусть X и Y – произвольные непустые множества. Тогда*

1) *если отображение f из X в Y инъективно, то существует сюръективное отображение g из Y на X;*

2) *если отображение f из X в Y сюръективно, то существует инективное отображение g из Y в X;*

Доказательство. Пусть отображение f инъективно. Зафиксируем во множестве X элемент x_0. Правило g определим следующим образом: если $y \in E(f)$ и $f(x) = y$, то $g(y) = x$, если же $y \notin E(f)$, то $g(y) = x_0$. Убедимся сначала, что g является отображением. Пусть $g(y) = x_1$ и $g(y) = x_2$. Предположив, что $y \in E(f)$, имеем $f(x_1) = y$ и $f(x_2) = y$, откуда $f(x_1) = f(x_2)$. Используя инъективность отображения f, получаем, что $x_1 = x_2$. Пусть теперь $y \notin E(f)$. Тогда $g(y) = x_0$, и потому $x_1 = x_0 = x_2$. Таким образом, $g(y)$ однозначно определен, и, следовательно, g является отображением. Сюръективность отображения g очевидна, поскольку для каждого $x \in X$ найдется такой элемент $y \in E(f)$, что $y = f(x)$.

Пусть f – сюръективное отображение. Тогда для каждого $y \in$ $\in Y$ полный прообраз $f^{-1}(y)$ является непустым множеством. Следовательно, для произвольного $y \in Y$ в полном прообразе $f^{-1}(y)$ можно зафиксировать элемент $g(y)$. Тем самым получаем правило g, являющееся, как нетрудно понять, инъективным отображением.

5.2. Композиция отображений

Пусть даны отображения $f : X \longrightarrow Y$ и $g : Y \longrightarrow Z$. Рассмотрим отображение $g \circ f : X \longrightarrow Z$, определенное правилом $g \circ f(x) = g(f(x))$. Это отображение называется *композицией* отображений f и g.

Таким образом, композиция $g \circ f$ определена, если область значений отображения f совпадает с областью определения отображения g. На самом деле, такое требование является излишним: достаточно предполагать, что множество значений отображения f содержится в области определения отображения g.

Приведем примеры композиций отображений.

1. Пусть $X = \{1, 2, 3, 4\}$, $Y = \{6, 7, 8, 9\}$, $Z = \{5, 6, 7\}$. Рассмотрим отображения $f : X \longrightarrow Y$ и $g : Y \longrightarrow Z$, определенные следующим образом

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 9 & 8 & 7 & 8 \end{pmatrix}, \qquad g = \begin{pmatrix} 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 5 \end{pmatrix}.$$

Тогда композиция $g \circ f : X \longrightarrow Z$ задается так

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

2. Рассмотрим отображения $f : \mathbb{R} \longrightarrow \mathbb{R}$ и $g : \mathbb{R} \longrightarrow \mathbb{R}$, заданные формулами $f(x) = x^2$, $g(x) = x - 3$. Тогда $g \circ f(x) = x^2 - 3$. Нетрудно понять, что в этом случае можно рассмотреть и композицию $f \circ g$, причем $f \circ g(x) = (x - 3)^2$.

Пусть даны отображения

$$f : X \longrightarrow Y, \qquad g : Y \longrightarrow Z, \qquad h : Z \longrightarrow T.$$

Тогда определены отображения $(h \circ g) \circ f$ и $h \circ (g \circ f)$. Читатель без труда проверит, что выполнено равенство

$$(h \circ g) \circ f = h \circ (g \circ f). \tag{1}$$

Обозначим через $T(X)$ совокупность всех преобразований непустого множества X. Ясно, что для любых преобразований $f, g \in \in T(X)$ существует композиция $g \circ f$. Из равенства (1) очевидно вытекает

Предложение 5.2. *Операция композиции на множестве* $T(X)$ *ассоциативна.*

Из предложения 5.2 следует, что если $f_1, f_2, \ldots, f_n$ – произвольные преобразования множества X, то однозначно определена их композиция

$$f_1 \circ f_2 \circ \ldots \circ f_n.$$

В частности, если $f_1 = f_2 = \ldots = f_n = f$, то определено преобразование f^n. А именно,

$$f^1 = f, \qquad f^n = f^{n-1} \circ f, \text{ если } n \geqslant 2.$$

В дополнение к предложению 5.2 отметим, что операция композиции на множестве $T(X)$ не является коммутативной, если множество X содержит более одного элемента. Для того чтобы убедиться в этом, достаточно рассмотреть случай, когда множество X состоит из двух элементов. Пусть для определенности $X = \{1, 2\}$. Рассмотрим следующие преобразования:

$$f = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Тогда

$$f \circ g = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \qquad g \circ f = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Видно, что $f \circ g \neq g \circ f$.

Предложение 5.3. *Пусть заданы отображения*

$$f : X \longrightarrow Y \quad \textit{и} \quad g : Y \longrightarrow Z.$$

Тогда

(a) *если* f *и* g *инъективны, то композиция* $g \circ f$ *инъективна;*

(b) *если* f *и* g *сюръективны, то композиция* $g \circ f$ *сюръективна;*

(c) *если* f *и* g *биективны, то композиция* $g \circ f$ *биективна.*

Доказательство. (a) Пусть $x_1, x_2 \in X$, причем $x_1 \neq x_2$. Тогда, используя инъективность отображения f, получаем $f(x_1) \neq \neq f(x_2)$. Из инъективности g теперь следует, что

$$g \circ f(x_1) = g(f(x_1)) \neq g(f(x_2)) = g \circ f(x_2).$$

(b) Пусть z – произвольный элемент из Z. Поскольку g сюръективно, существует такой $y \in Y$, что $z = g(y)$. Но f тоже сюръективно, поэтому $y = f(x)$ для некоторого $x \in X$. Стало быть, $z = g(y) = g(f(x)) = g{\circ}f(x)$, и сюръективность композиции доказана.

(c) следует из доказанного выше.

5.3. Отображение, обратное к данному

Определение отображения, обратного к данному, основывается на следующем утверждении, представляющем и самостоятельный интерес.

Предложение 5.4. *Пусть f – инъективное отображение множества X в множество Y. Тогда существует биективное отображение $g : E(f) \longrightarrow X$, удовлетворяющее равенствам*

$$g(f(x)) = x, \qquad f(g(y)) = y$$

для любых $x \in X$, $y \in E(f)$.

Доказательство. Для произвольного $y \in E(f)$ определим правило g:

$$g(y) = x \Longleftrightarrow y = f(x). \tag{2}$$

Проверим, что правило g задает отображение из $E(f)$ в X. В самом деле, пусть $g(y) = x_1$ и $g(y) = x_2$. Это означает, что $f(x_1) = y$ и $f(x_2) = y$. Стало быть, $f(x_1) = f(x_2)$. Поскольку f – инъективное отображение, из последнего равенства следует, что $x_1 = x_2$.

Теперь покажем, что g – инъективное отображение. Предположим, что $y_1, y_2 \in E(f)$ и $g(y_1) = g(y_2) = x$. Из определения отображения g следует, что $y_1 = f(x)$, $y_2 = f(x)$ и, стало быть, $y_1 = y_2$. Таким образом, g инъективно.

Осталось убедиться в том, что g сюръективно. Пусть x – произвольный элемент из X и $y = f(x)$. Отсюда вытекает, что $x = g(y)$.

Поскольку g одновременно инъективно и сюръективно, оно биективно.

Пусть f – биективное отображение множества X на множество Y. Применяя в этом случае предложение 5.4, мы получим биективное отображение $g : Y \longrightarrow X$, причем равенства $y = f(x)$ и $x = g(y)$ равносильны.

Такое отображение g называется *обратным* к отображению f.

Нетрудно видеть, что если отображение g обратно к биективному отображению f, то и f является обратным к g. В этой ситуации отображения f и g называются *взаимно обратными*.

Сформулируем свойства взаимно обратных отображений.

1. $D(f) = E(g)$;
2. $D(g) = E(f)$;
3. $f \circ g = \varepsilon_Y$;
4. $g \circ f = \varepsilon_X$.

Эти свойства непосредственно вытекают из доказательства предложения 5.4.

Предложение 5.5. *Пусть дано отображение $f : X \longrightarrow Y$. Если существует такое отображение $g : Y \longrightarrow X$, что $f \circ g = \varepsilon_Y$ и $g \circ f = \varepsilon_X$, то f – биективное отображение и g является отображением, обратным к f.*

Доказательство. Пусть $f \circ g = \varepsilon_Y$, $g \circ f = \varepsilon_X$ для некоторого отображения $g : Y \longrightarrow X$. Докажем сначала, что f инъективно. Если $x_1, x_2 \in X$ и $f(x_1) = f(x_2)$, то $g \circ f(x_1) = g \circ f(x_2)$. Поскольку $g \circ f = \varepsilon_X$, имеем $g \circ f(x_1) = x_1$, $g \circ f(x_2) = x_2$. Стало быть, $x_1 = x_2$.

Теперь убедимся, что f сюръективно. Пусть y – произвольный элемент из Y, и $g(y) = x$. Так как $f \circ g = \varepsilon_Y$, получаем

$$f(x) = f(g(y)) = f \circ g(y) = \varepsilon_Y(y) = y.$$

Мы проверили, что f инъективно и сюрьективно. Следовательно, f биективно.

Осталось доказать, что отображение g обратно к f. Пусть x – произвольный элемент из X и $y = f(x)$. Отсюда

$$g(y) = g(f(x)) = g \circ f(x) = \varepsilon_X(x) = x.$$

Таким образом, $y = f(x) \Longrightarrow x = g(y)$. Аналогично проверяется, что $x = g(y) \Longrightarrow y = f(x)$.

Отображение, обратное к данному биективному отображению f, как правило, обозначают через f^{-1}

Из предложений 5.4, 5.5 следует, что биективность данного отображения равносильна наличию у него обратного отображения. По этой причине биективные отображения часто называют обратимыми.

5.4. Множество всех отображений из X в Y

Пусть X, Y – произвольные непустые множества. Обозначим через Y^X множество всех отображений из X в Y. Таким образом, упорядоченной паре непустых множеств X, Y соответствует однозначно определенное множество Y^X, и мы получаем бинарную операцию над множествами. Доказанные ниже утверждения показывают, что имеется некоторая аналогия между свойствами этой операции и свойствами операции возведения в степень на числовых множествах. Этой аналогией отчасти объясняется принятое обозначение для множества всех отображений из X в Y.

Предложение 5.6. *Пусть X_1, X_2, Y – произвольные непустые множества, причем $X_1 \cap X_2 = \emptyset$. Тогда существует биективное отображение из $Y^{X_1 \cup X_2}$ на $Y^{X_1} \times Y^{X_2}$.*

Доказательство. Пусть $f \in Y^{X_1 \cup X_2}$, т. е.

$$f : X_1 \cup X_2 \longrightarrow Y.$$

Определим отображения

$$f_1 : X_1 \longrightarrow Y, \qquad f_2 : X_2 \longrightarrow Y,$$

положив $f_i(x) = f(x)$, если $x \in X_i$, $i = 1, 2$. Нетрудно понять, что правило

$$\varphi(f) = (f_1, f_2)$$

задает отображение φ из $Y^{X_1 \cup X_2}$ в $Y^{X_1} \times Y^{X_2}$.

Докажем, что отображение φ сюръективно. Пусть f_i – произвольные отображения из X_i в Y $(i = 1, 2)$. Так как множества X_1, X_2 не пересекаются, правило

$$f(x) = \begin{cases} f_1(x), & \text{если } x \in X_1, \\ f_2(x), & \text{если } x \in X_2 \end{cases}$$

определяет отображение из $X_1 \cup X_2$ в Y. Ясно, что

$$\varphi(f) = (f_1, f_2)$$

.

Проверка инъективности отображения φ оставляется читателю в качестве упражнения.

Предложение 5.7. *Пусть X, Y, Z – произвольные непустые множества. Тогда существует биективное отображение из $\left(Z^Y\right)^X$ на $Z^{X\times Y}$.*

Доказательство. Пусть $f \in \left(Z^Y\right)^X$, т. е.

$$f : X \longrightarrow Z^Y.$$

Стало быть, для любого $x \in X$ определено отображение

$$f(x) : Y \longrightarrow Z.$$

Построим отображение $\tilde{f}$ из $X \times Y$ в Z. Если $x \in X, y \in Y$, то положим

$$\tilde{f}(x, y) = f(x)(y).$$

Таким образом, правило $\varphi(f) = \tilde{f}$ определяет отображение из $\left(Z^Y\right)^X$ в $Z^{X\times Y}$.

Проверим, что отображение φ инъективно. Пусть $f, g \in \left(Z^Y\right)^X$ и $\tilde{f} = \tilde{g}$. Это означает, что $\tilde{f}(x, y) = \tilde{g}(x, y)$ для любых $x \in X$, $y \in Y$. Поскольку $\tilde{f}(x, y) = f(x)(y)$, $\tilde{g}(x, y) = g(x)(y)$, имеем $f(x) = g(x)$ при любых $x \in X$. Отсюда следует, что $f = g$.

Осталось показать, что φ – сюръективное отображение. Пусть h – произвольное отображение из $Z^{X\times Y}$. Для каждого $x \in$ $\in X$ определим отображение

$$g(x) : Y \longrightarrow Z$$

правилом $g(x)(y) = h(x, y)$. Ясно, что $h = \tilde{g}$.

Предложение 5.8. *Пусть X_1, X_2, Y – произвольные непустые множества. Если существует биективное отображение из X_1 на X_2, то существует и биективное отображение из Y^{X_1} на Y^{X_2}.*

Доказательство. Пусть $f : X_1 \longrightarrow X_2$ – биективное отображение. Тогда, как мы знаем, существует обратное к f отображение f^{-1}. Если g – произвольное отображение из X_1 в Y, то $g \circ f^{-1}$ является отображением из X_2 в Y. Определим отображение

$$\tilde{f} : Y^{X_1} \longrightarrow Y^{X_2}$$

в соответствии с правилом $\tilde{f}(g) = g \circ f^{-1}$ и убедимся, что отображение $\tilde{f}$ является биекцией.

Пусть g_1, g_2 – произвольные отображения из X_1 в Y, причем $\tilde{f}(g_1) = \tilde{f}(g_2)$. Отсюда $g_1 \circ f^{-1} = g_2 f^{-1}$ и потому

$$g_1 \circ f^{-1} \circ f = g_2 \circ f^{-1} \circ f.$$

Поскольку $f^{-1} \circ f = \varepsilon_{X_1}$, получаем, что $g_1 \circ \varepsilon_{X_1} = g_2 \circ \varepsilon_{X_1}$, т. е. $g_1 = g_2$. Тем самым инъективность отображения $\tilde{f}$ доказана.

Проверим, что отображение $\tilde{f}$ сюръективно. Если $h \in Y^{X_2}$, то

$$\tilde{f}(h \circ f) = h \circ f \circ f^{-1} = h \circ \varepsilon_{X_2} = h.$$

Итак, образ отображения $\tilde{f}$ совпадает с множеством Y^{X_2}, т. е. $\tilde{f}$ сюръективно.

Предложение 5.9. *Пусть X, Y_1, Y_2 – произвольные непустые множества. Если существует биективное отображение из Y_1 на Y_2, то существует и биективное отображение из Y_1^X на Y_2^X.*

Доказательство. Пусть f – биективное отображение из Y_1 на Y_2. Для произвольного отображения $g \in Y_1^X$ положим $\tilde{f} = f \circ g$. Ясно, что $\tilde{f}$ – отображение из Y_1^X в Y_2^X. Инъективность и сюръективность этого отображения доказываются при помощи рассуждений, аналогичных использованным при доказательстве предложения 5.9. Соответствующие вычисления оставляются читателю в качестве упражнения.

Следующие два утверждения проверяются аналогично предложениям 5.8 и 5.9. Соответствующие доказательства мы опускаем.

Предложение 5.10. *Пусть X_1, X_2, Y – произвольные непустые множества. Если существует инъективное отображение из X_1 в X_2, то существует и инъективное отображение из Y^{X_1} в Y^{X_2}.*

Предложение 5.11. *Пусть X, Y_1, Y_2 – произвольные непустые множества. Если существует инъективное отображение из Y_1 в Y_2, то существует и инъективное отображение из Y_1^X в Y_2^X.*

Обозначим через 2 множество $\{0,1\}$. Тогда 2^X – множество всех отображений из множества X в двухэлементное множество. Пусть Y – произвольное подмножество из X. Определим функцию

$$h_Y : X \longrightarrow \{0,1\} \tag{3}$$

следующим образом:

$$h_Y(x) = \begin{cases} 1, & \text{если } x \in Y, \\ 0, & \text{если } x \in X \setminus Y. \end{cases}$$

Такое отображение h_Y называется *характеристическим* для подмножества Y. Нетрудно понять, что разным подмножествам отвечают разные характеристические функции. Поэтому справедливо следующее утверждение.

Предложение 5.12. *Существует биективное отображение из булеана $\mathcal{P}(X)$ множества X на множество 2^X.*

Рассмотрим случай, когда $X = \{1, 2, \ldots, n\}$. Если f – отображение из X в Y, то f однозначно определяется конечной последовательностью (кортежем) $(f(1), f(2), \ldots, f(n))$. Отсюда вытекает, что существует биективное отображение из Y^X на Y^n.

5.5. Конечные и бесконечные множества

В этом разделе мы дадим ответ на два вопроса: что такое конечное и что такое бесконечное множество? Существенную помощь при этом нам окажут инъективные отображения. Напомним, что в разделе 2.4 через $\mathbb{N}_{\leqslant n}$ было обозначено множество $\{1, 2, \ldots, n\}$.

Лемма 1. *Пусть n – произвольное натуральное число, f – отображение из $\mathbb{N}_{\leqslant n+1}$ в $\mathbb{N}_{\leqslant n}$. Тогда f не является инъективным.*

Доказательство. Для доказательства этого утверждения применим метод математической индукции.

Если $n = 1$, то f отображает множество $\mathbb{N}_{\leqslant 2} = \{1, 2\}$ в множество $\mathbb{N}_{\leqslant 1} = \{1\}$. Ясно, что такое отображение не является инъективным.

Пусть $k \geqslant 1$. Предположим, что для $n = k$ утверждение выполнено. Убедимся, что оно выполняется и при $n = k + 1$. Пусть f – произвольное отображение из $\mathbb{N}_{\leqslant k+1}$ в $\mathbb{N}_{\leqslant k}$. Возможны два случая:

(a) для любого $i \leqslant k$ справедливо неравенство $f(i) \leqslant k - 1$;

(b) существует такое $j \leqslant k$, что $f(j) = k$.

Рассмотрим случай (a). Тогда существует отображение

$$g : \mathbb{N}_{\leqslant k} \longrightarrow \mathbb{N}_{\leqslant k-1},$$

заданое правилом $g(i) = f(i)$ для каждого $i \leqslant k$. К отображению g применио предположение индукции; поэтому g не является инъективным. Отсюда следует, что f тоже не инъективно.

Предположим, что имеет место случай (b). Если $f(k + 1) = k$, то $f(j) = f(k + 1) = k$ и $j \neq k + 1$. Поэтому f не является инъективным. Пусть $f(k + 1) = l < k$. Можно считать, что кроме чисел j и $k + 1$ в числа k и l никакие другие числа не отображаются (иначе f очевидным образом не обладало бы свойством инъективности). Рассмотрим отображение

$$h : \mathbb{N}_{\leqslant k+1} \longrightarrow \mathbb{N}_{\leqslant k},$$

определенное следующим образом:

$$h(i) = \begin{cases} f(i), & \text{если } i \notin \{j, k + 1\}, \\ l, & \text{если } i = j, \\ n, & \text{если } i = k + 1. \end{cases}$$

Ясно, что отображение h обладает свойстом (a), и потому h, а вслед за ним и f, не является инъективным.

Из леммы 1 очевидным образом вытекает следующее утверждение, называемое принципом Дирихле[1].

[1]П.Л.Дирихле (1805–1859) – один из крупнейших математиков девятнадцатого столетия. Известен работами по теории чисел, математическому анализу, вариационному исчислению.

Пусть f – отображение из $\mathbb{N}_{\leqslant m}$ в $\mathbb{N}_{\leqslant n}$, причем $m > n$. Тогда отображение f не является инъективным.

Лемма 2. *Пусть X – непустое множество, и для некоторого натурального n существует инъективное отображение f из $\mathbb{N}_{\leqslant n}$ в X. Если никакое отображение из $\mathbb{N}_{\leqslant n+1}$ в X не является инъективным, то f – биективное отображение.*

Доказательство. Предположим, что заключение леммы не верно. Это значит, что данное инъективное отображение f не является сюръективным. Тогда существует элемент $x \in X$, не принадлежащий множеству значений отображения f. Определим отображение g из $\mathbb{N}_{\leqslant n+1}$ в X:

$$g(k) = \begin{cases} f(k), & \text{если } k \in \mathbb{N}_{\leqslant n}, \\ x, & \text{если } k = n+1. \end{cases}$$

Легко видеть, что g инъективное отображение из $\mathbb{N}_{\leqslant n+1}$ в X. Существование такого отображения противоречит условию леммы.

Лемма 3. *Предположим, что для некоторого $n \in \mathbb{N}$ существуют инъективные отображения*

$$f_1 : \mathbb{N}_{\leqslant n} \longrightarrow X \quad \text{и} \quad f_2 : \mathbb{N}_{\leqslant n+1} \longrightarrow X.$$

Тогда найдется такое инъективное отображение

$$h : \mathbb{N}_{\leqslant n+1} \longrightarrow X,$$

что $h(k) = f_1(k)$ при любом $k \leqslant n$.

Доказательство. Рассмотрим множества значений $E(f_1)$, $E(f_2)$ отображений f_1 и f_2 соответственно. Проверим, что включение

$$E(f_2) \subseteq E(f_1) \tag{4}$$

невозможно. Рассуждая “от противного”, допустим, что это включение выполнено. Поскольку f_1 – инъективное отображение, из предложения 5.4 следует существование биективного отображения g из $E(f_1)$ на $\mathbb{N}_{\leqslant n}$. Из включения (4) вытекает, что определена

композиция $g \circ f_2$, отображающая $\mathbb{N}_{\leqslant n+1}$ в $\mathbb{N}_{\leqslant n}$. В силу п. (а) предложения 5.3 получаем, что отображение $g \circ f_2$ инъективно. Однако лемма 1 утверждает, что инъективного отображения из $\mathbb{N}_{\leqslant n+1}$ в $\mathbb{N}_{\leqslant n}$ не существует.

Итак, включение (4) не выполняется. Отсюда следует, что найдется такой элемент $x \in X$, что $x \notin E(f_1)$. Определим отображение h:

$$h(k) = \begin{cases} f_1(k), & \text{если } k \in \mathbb{N}_{\leqslant n}, \\ x, & \text{если } k = n+1. \end{cases}$$

Ясно, что h – инъективное отображение из $\mathbb{N}_{\leqslant n+1}$ в X и $h(k) = f_1(k)$ для любого $k \leqslant n$.

Лемма 4. *Пусть для любого $n \in \mathbb{N}$ существует инъективное отображение из $\mathbb{N}_{\leqslant n}$ в множество X. Тогда существует инъективное отображение из $\mathbb{N}$ в X.*

Доказательство. Проверим сначала, что для каждого $n \in \mathbb{N}$ можно определить инъективное отображение

$$f_n : \mathbb{N}_{\leqslant n} \longrightarrow X$$

таким образом, что

$$f_{n+1}(k) = f_n(k) \tag{5}$$

для любого $k \leqslant n$. Существование такой последовательности отображений можно доказать методом математической индукции.

Если $n = 1$, то достаточно выбрать произвольный элемент $x \in X$ и положить $f_1(1) = x$.

Пусть $n \geqslant 1$, и отображение f_n определено. Поскольку существует инъективное отображение из $\mathbb{N}_{\leqslant n+1}$ в X, применение леммы 3 показывает, что найдется инъективное отображение h из $\mathbb{N}_{\leqslant n+1}$ в X, обладающее свойством: $h(k) = f_n(k)$ при любом $k \leqslant n$. Ясно, что $f_{n+1} = h$.

Из доказанного свойства такой последовательности отображений легко получается следующее свойство: если $m < n$, то $f_m(m) = f_n(m)$.

Построим теперь отображение $f : \mathbb{N} \longrightarrow X$, положив $f(n) = f_n(n)$ для любого $n \in \mathbb{N}$. Легко убедиться в том, что f инъективно. В самом деле, пусть m, n – различные натуральные числа.

Без ограничения общности можно считать, что $m < n$. Имеем $f(n) = f_n(n)$, $f(m) = f_m(m) = f_n(m)$. Так как f_n – инъективное отображение, имеем $f_n(n) \neq f_n(m)$, откуда $f(n) \neq f(m)$. Стало быть, f инъективно.

Пусть X – произвольное непустое множество. Тогда выполнено в точности одно из двух утверждений:

1) для любого натурального n существует инъективное отображение из $\mathbb{N}_{\leqslant n}$ в X;

2) существует наибольшее натуральное число n, для которого множество $\mathbb{N}_{\leqslant n}$ инъективно отображается в X.

Поэтому из лемм 2, 4 вытекает

Теорема 5.1. *Пусть X – непустое множество. Тогда выполняется одна из двух возможностей:*

(a) *существует инъективное отображение f из $\mathbb{N}$ в X.*

(b) *существует биективное отображение f из $\mathbb{N}_{\leqslant n}$ на X при некотором $n \in \mathbb{N}$;*

Если реализуется возможность (a), то множество X называется бесконечным; если же имеет место возможность (b), то X называется конечным. В том случае, когда X – конечное множество, определено число $|X|$, называемое числом элементов множества X; а именно, если $|X| = n$, то существует биекция из $\mathbb{N}_{\leqslant n}$ на X. Заметим, что если X – конечное множество и $|X| = n$, то существует биективное отображение $g : X \longrightarrow \mathbb{N}_{\leqslant n}$.

Поскольку $\mathbb{N}_{\leqslant n} \subseteq \mathbb{N}$ при любом n, из определений конечного и бесконечного множеств вытекает

Предложение 5.13. *Если X конечное, а Y – бесконечное множество, то существует инъективное отображение $g : X \longrightarrow Y$.*

Давая определения конечных и бесконечных множеств, мы использовали в качестве "эталонных" множество $\mathbb{N}$ и его подмножества $\mathbb{N}_{\leqslant n}$, $n \in \mathbb{N}$. Оказывается, конечные и бесконечные множества можно охарактеризовать без использования множества $\mathbb{N}$ и его подмножеств.

Теорема 5.2. *Множество X бесконечно тогда и только тогда, когда существует биективное отображение f множества X на его собственное подмножество Y.*

Доказательство. Пусть X бесконечно. Тогда существует инъективное отображение g из $\mathbb{N}$ в X. Множество значений отображения g можно представить в виде

$$E(g) = \{g(i) \mid i \in \mathbb{N}\}.$$

Рассмотрим множество

$$Y_0 = \{g(2i) \mid i \in \mathbb{N}\}.$$

Ясно, что Y_0 – собственное подмножество $E(g)$. Поэтому множество $Y = (X \setminus E(g)) \cup Y_0$ является собственным подмножеством множества X. Определим отображение f из X в Y:

$$f(x) = \begin{cases} x, & \text{если } x \in X \setminus E(g), \\ g(2i), & \text{если } x \in E(g) \text{ и } x = g(i). \end{cases} \tag{6}$$

Проверим, что f – биективное отображение. Пусть $x_1, x_2 \in X$ и $x_1 \neq x_2$. Если $x_1, x_2 \in X \setminus E(g)$, то

$$f(x_1) = x_1 \neq x_2 = f(x_2).$$

Если $x_1, x_2 \in E(g)$, то $x_1 = g(i_1)$, $x_2 = g(i_2)$. Из неравенства $x_1 \neq x_2$, очевидно, вытекает неравенство $i_1 \neq i_2$. Поэтому

$$f(x_1) = g(2i_1) \neq g(2i_2) = f(x_2).$$

Если же $x_1 \in X \setminus E(g)$, $x_2 \in E(g)$, то $f(x_1) = x_1 \in X \setminus E(g)$, $f(x_2) \in E(g)$. Неравенство $f(x_1) \neq f(x_2)$ следует из того, что множества $X \setminus E(g)$ и $E(g)$ не имеют общих элементов. Итак, доказано, что при любых $x_1, x_2 \in X$ из $x_1 \neq x_2$ следует $f(x_1) \neq$ $\neq f(x_2)$. Стало быть, f – инъективное отображение.

Осталось проверить, что f сюръективно. Пусть $y \in Y$. Возможны два случая: 1) $y \in X \setminus E(g)$, 2) $y \in Y_0$. В первом случае, положив $x = y$, получим $y = f(x)$. Если же имеет место второй случай, то $y = g(2i)$ для некоторого $i \in \mathbb{N}$. Тогда $y = f(x)$, где

$x = g(i)$. Мы проверили, что любой элемент из Y является образом некоторого элемента из X; следовательно, f сюръективно.

Проверим обратное утверждение. Пусть Y – собственное подмножество из X, и отображение $f : X \longrightarrow Y$ биективно. Возьмем произвольный элемент $x_0 \in X \setminus Y$. Ясно, что x_0 не содержится в множестве значений отображения f, т. е. для любого $x \in X$ выполнено неравенство $f(x) \neq x_0$. Для произвольного натурального n рассмотрим элемент $x_n = f^n(x_0)$. Проверим, что $x_k \neq x_m$, если $k, m \in \mathbb{N}$ и $k \neq m$. Предположим, что это утверждение не выполняется, т. е. $x_k = x_m$ для некоторых различных k и m. Пусть для определенности $k < m$ и $s = m - k$. Учитывая определение элементов x_k, x_m, имеем

$$f^k(x_0) = f^m(x_0) = f^{k+s}(x_0) = f^k(f^s(x_0)).$$

Из инъективности отображения f вытекает инъективность отображения f^k. Поэтому из равенства $f^k(x_0) = f^k(f^s(x_0))$ следует равенство

$$x_0 = f^s(x_0).$$

Последнее равенство показывает, в частности, что x_0 лежит в образе отображения f. Это противоречит выбору элемента x_0.

Определим отображение

$$g : \mathbb{N} \longrightarrow X$$

при помощи правила $g(n) = x_n$. Доказанное выше утверждение означает, что отображение g инъективно. Стало быть, X – бесконечное множество.

Теорема 5.3. *Множество X конечно тогда и только тогда, когда любое инъективное преобразование f множества X является биективным.*

Эта теорема непосредственно вытекает из теорем 5.2 и 5.1. В самом деле, теорему 5.1 можно переформулировать следующим образом: множество конечно тогда и только тогда, когда оно не является бесконечным. Это означает, что утверждение "X – бесконечное множество" является отрицанием утверждения "X – конечное множество". Нетрудно понять, что для утверждения "существует инъективное отображение множества X на собственное

подмножество" отрицанием служит утверждение "любое инъективное преобразование f множества X является биективным".

Понятие бесконечного множества впервые встретилось в разделе 3.7 при обсуждении теоремы Евклида о множестве всех простых чисел. Там же было высказано предположение, что для произвольного множества натуральных чисел свойства "быть бесконечным" и "быть неограниченным сверху" равносильны. Теперь мы в состоянии доказать, что это действительно так.

Предложение 5.14. *Если множество натуральных чисел бесконечно, то оно неограничено сверху.*

Доказательство. Пусть M – бесконечное подмножество из $\mathbb{N}$. Будем рассуждать "от противного". Предположим, что M ограничено сверху. Это значит, что найдется такое натуральное число n, что $M \subseteq \mathbb{N}_{\leqslant n}$. Поскольку M бесконечно, существует инъективное отображение $f : \mathbb{N} \longrightarrow M$. Ясно, что f является инъективным отображением из $\mathbb{N}$ в $\mathbb{N}_{\leqslant n}$. Так как $\mathbb{N}_{\leqslant n+1} \subset \mathbb{N}$, существование такого отображения f противоречит лемме 1.

Предложение 5.15. *Если множество натуральных чисел неограничено сверху, то оно бесконечно.*

Пусть M не является ограниченным сверху. Построим отображение f из $\mathbb{N}$ в M следующим образом. Из теоремы 2.1 следует, что M имеет наименьший элемент m_1. Положим

$$f(1) = m_1.$$

Предположим теперь, что для некоторого натурального n элементы $f(1), f(2), \ldots, f(n)$ уже определены. Рассмотрим множество

$$M_n = M \setminus \{f(1), f(2), \ldots, f(n)\}.$$

Поскольку M неограничено сверху, множество M_n непусто. Поэтому оно имеет наименьший элемент m_{n+1}. По определению полагаем

$$f(n+1) = m_{n+1}.$$

При помощи метода математической индукции легко придти к выводу, что описанная процедура определит отображение f на всем

множестве $\mathbb{N}$, причем такое f, очевидным образом, инъективно. Стало быть, построено инъективное отображение из $\mathbb{N}$ в M. Поэтому M – бесконечное множество.

Из предложений 5.14 и 5.15 очевидным образом вытекает следующее утверждение.

Предложение 5.16. *Множество натуральных чисел ограничено сверху тогда и только тогда, когда оно конечно.*

Отображение f, построенное при доказательстве предложения 5.15, является, на самом деле биекцией. Проверим справедливость этого утверждения. В самом деле, пусть $E(f) \subset M$, т. е. $E(f)$ – собственное подмножество из M. Тогда $M \setminus E(f)$ – непустое множество натуральных чисел, и потому это множество содержит наименьший элемент m. Рассмотрим множество $E(f) \cap \mathbb{N}_{<m}$. Это множество непусто, поскольку ему принадлежит, например, $f(1)$, являющееся наименьшим элементом множества M. Кроме того, это множество ограничено сверху; следовательно, в силу предложения 5.16 оно конечно. Поэтому существует такое k, что

$$E(f) \cap \mathbb{N}_{<m} = \{f(1), f(2), \ldots, f(k)\}.$$

Из определения числа m вытекает, что m – наименьший элемент множества $M \setminus \{f(1), f(2), \ldots, f(k)\}$, и потому $m = f(k+1)$, т. е. $m \in E(f)$. Последнее включение противоречит выбору числа m.

Эти рассуждения показывают, что справедливо

Предложение 5.17. *Если множество M натуральных чисел бесконечно, то существует биективное отображение f из $\mathbb{N}$ на M.*

5.6. Счетные множества

О п р е д е л е н и е. Множество X называется *счетным*, если существует биективное отображение $f : \mathbb{N} \longrightarrow X$.

В том случае, когда множество X счетно, существует биективное отображение g из X на $\mathbb{N}$; в качестве g можно взять, например, отображение, обратное к f. Нетрудно видеть, что счетность множества X означает возможность *занумеровать* элементы этого

множества, т. е. включить все элементы этого множества в бесконечную последовательность без повторяющихся членов.

Заметим также, что если X, Y – счетные множества, то существует биективное отображение из X на Y. В самом деле, существуют биективные отображения

$$f : X \longrightarrow \mathbb{N}, \qquad g : \mathbb{N} \longrightarrow Y.$$

Ясно, что композиция $g \circ f$ – биективное отображение из X на Y.

В этом разделе мы изучим свойства счетных множеств. Сначала приведем несколько примеров счетных множеств.

1. Множество $\mathbb{E}$ четных натуральных чисел счетно.

В самом деле, рассмотрим отображение $f : \mathbb{N} \longrightarrow \mathbb{E}$, определенное правилом $f(n) = 2n$. Ясно, что f – биективное отображение.

2. Множество $\mathbb{O}$ нечетных натуральных чисел счетно.

Для проверки этого утверждения достаточно рассмотреть отображение $g : \mathbb{N} \longrightarrow \mathbb{O}$, заданное правилом $g(n) = 2n - 1$.

3. Множество $\mathbb{Z}$ всех целых чисел счетно.

Рассмотрим отображение $h : \mathbb{N} \longrightarrow \mathbb{Z}$, заданное следующим образом:

$$h(n) = \begin{cases} n/2, & \text{если } n = 2k, \\ (1-n)/2, & \text{если } n = 2k-1. \end{cases}$$

Читатель без труда проверит, что h – биективное отображение.

Предложение 5.18. *Всякое бесконечное X множество содержит счетное подмножество.*

Доказательство. Поскольку X бесконечно, существует инъективное отображение

$$f : \mathbb{N} \longrightarrow X.$$

Пусть $Y = E(f)$. Тогда Y счетно и $Y \subseteq X$.

Предложение 5.19. *Всякое бесконечное подмножество счетного множества само счетно.*

Доказательство. Пусть Y – бесконечное подмножество счетного множества X. Как мы знаем, существует биективное отображение

$$g : X \longrightarrow \mathbb{N}.$$

Обозначим множество $g(Y)$ через M и рассмотрим отображение

$$h : Y \longrightarrow M,$$

определенное правилом $h(i) = g(i)$ для любого $i \in Y$. Ясно, h – является биективным отображением, и потому из бесконечности множества Y следует бесконечность множества M. Следовательно, M – бесконечное подмножество из $\mathbb{N}$. Применение предложения 5.17 показывает, что M – счетное множество. Поскольку h^{-1} является биективным отображением M на Y, получаем, что Y – также счетное множество.

Из предложения 5.19 вытекает следующее утверждение.

Предложение 5.20. *Пусть X бесконечное, а Y – счетное множество. Если существует инъективное отображение $f : X \longrightarrow Y$, то X – счетное множество.*

Доказательство. Пусть $Z = f(X)$. Тогда Z – бесконечное подмножество счетного множества Y, и потому Z счетно. Легко понять, что существует биективное отображение из Z на X. Следовательно, X – счетное множество.

Предложение 5.20 в дальнейшем часто будет использоваться для доказательства счетности множеств.

Предложение 5.21. *Объединение двух счетных множеств счетно.*

Доказательство. Пусть A_1, A_2 – счетные множества. Справедливо равенство

$$A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1).$$

Заметим, что множество $A_2 \setminus A_1$ является подмножеством счетного множества A_2, и потому либо конечно, либо счетно. Поскольку

множество $\mathbb{E}$ четных натуральных чисел и множество $\mathbb{O}$ нечетных натуральных чисел являются счетными, существуют инъективные отображения

$$f_1 : A_1 \longrightarrow \mathbb{E}, \qquad f_2 : A_2 \setminus A_1 \longrightarrow \mathbb{O}.$$

Определим отображение

$$f : A_1 \cup A_2 \longrightarrow \mathbb{N}$$

при помощи правила

$$f(a) = \begin{cases} f_1(a), & \text{если } a \in A_1, \\ f_2(a), & \text{если } a \in A_2 \setminus A_1. \end{cases}$$

Легко проверяется, что f – инъективное отображение. Так как множество $A_1 \cup A_2$, очевидно, является бесконечным, из предложения 5.20 следует, что это множество счетно.

Теорема 5.4. *Множество $\mathbb{N} \times \mathbb{N}$ является счетным.*

Доказательство. Построим инъективное отображение из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$. Для этого воспользуемся тем, что множество $\mathbb{P}$ всех простых чисел является счетным. Пусть $\mathbb{P} = \{p_i \,|\, i \in \mathbb{N}\}$. Рассмотрим произвольную упорядоченную пару $(m, n) \in \mathbb{N} \times \mathbb{N}$ и положим

$$f(m, n) = p_m^n.$$

Легко проверяется, что из равенства $f(i, j) = f(m, n)$ следует равенство $(i, j) = (m, n)$. В самом деле, пусть $p_i^j = p_m^n$. Из теоремы о каноническом разложении натуральных чисел вытекает, что $i = m$ и $j = n$, т. е. $(i, j) = (m, n)$. Таким образом, отображение f из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$ инъективно. Поскольку $\mathbb{N} \times \mathbb{N}$ бесконечно, оно является счетным.

Из теоремы 5.4 вытекает

Теорема 5.5. *Пусть X, Y – счетные множества. Тогда множество $X \times Y$ является счетным.*

Доказательство. Обозначим через f, g биективные отображения из X и Y на $\mathbb{N}$. Поставим в соответствие каждому элементу $(x, y) \in X \times Y$ элемент $(f(x), g(y)) \in \mathbb{N} \times \mathbb{N}$. Ясно, что указанное правило определяет биективное отображение из $X \times Y$ на $\mathbb{N} \times \mathbb{N}$.

Предложение 5.22. *Объединение счетного семейства счетных множеств является счетным множеством.*

Доказательство. Пусть A_i, $i \in \mathbb{N}$, – произвольное семейство счетных множеств. Определим множества B_i, $i \in \mathbb{N}$, следующим образом:

$$B_1 = A_1, \qquad B_i = A_i \setminus (A_1 \cup A_2 \cup \ldots \cup A_{i-1}) \text{ при } i \geqslant 2.$$

Проверим, что множества B_i попарно не пересекаются. В самом деле, пусть $j < k$ и $b \in B_j$. Поскольку $B_j \subseteq A_j$, элемент b содержится в A_j. Но $B_k \subseteq A_k \setminus A_j$, поэтому $b \notin B_k$.

Покажем теперь, что имеет место равенство

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} B_i. \tag{7}$$

Так как $B_i \subseteq A_i$ при любом $i \in \mathbb{N}$, правая часть равенства (7) содержится в его левой части. Проверим обратное включение. Пусть $a \in \bigcup_{i=1}^{\infty} A_i$ и A_k – множество с наименьшим номером, содержащее a. Тогда $a \notin A_1 \cup A_2 \cup \ldots \cup A_{k-1}$. Поэтому $a \in B_k$, и, следовательно, $a \in \bigcup_{i=1}^{\infty} B_i$.

Каждое из множеств B_i конечно или счетно. Поэтому существует инъективное отображение $f_i : B_i \longrightarrow \mathbb{N}$. Определим отображение

$$f : \bigcup_{i=1}^{\infty} B_i \longrightarrow \mathbb{N} \times \mathbb{N}$$

следующим способом: если $b \in B_i$, то $f(b) = (i, f_i(b)$. Правило f на самом деле задает отображение, поскольку B_i попарно не пересекаются. Кроме того, нетрудно проверить, что это отображение инъективно. Отсюда следует, что $\bigcup_{i=1}^{\infty} B_i$, а потому и $\bigcup_{i=1}^{\infty} A_i$ является счетным множеством.

Предложение 5.23. *Множество $\mathbb{Q}$ всех рациональных чисел счетно.*

Доказательство. Обозначим через $\mathbb{Q}^+$ (соответственно $\mathbb{Q}^-$) множество всех положительных (соответственно отрицательных) рациональных чисел. Всякое положительное рациональное

число можно представить в виде несократимой дроби m/n, где $m, n \in \mathbb{N}$. Поставив в соответствие каждой несократимой дроби m/n упорядоченную пару (m, n), мы получим инъективное отображение из $\mathbb{Q}^+$ в $\mathbb{N} \times \mathbb{N}$. Отсюда вытекает, что Q^+ счетно. Поскольку существует очевидное биективное отображение из $\mathbb{Q}^+$ на $\mathbb{Q}^-$, множество $\mathbb{Q}^-$ также счетно. Так как $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$, получаем, что $\mathbb{Q}$ – счетное множество.

Предложение 5.24. *Если X – счетное множество, то для каждого натурального n множество X^n счетно.*

Доказательство. Применим метод математической индукции. Поскольку $X^1 = X$, при $n = 1$ утверждение выполнено. Пусть $n = k \geqslant 1$ и X^k счетно. Поскольку существует биективное отображение из $X^k \times X$ на X^{k+1}, при помощи теоремы 5.5 получаем, что X^{k+1} также счетно.

Предложение 5.25. *Если X – счетное множество, то множество X_{fin} всех конечных последовательностей, составленных из элементов множества X, счетно.*

Для доказательства этого утверждения достаточно заметить, что множество X_{fin} всех конечных последовательностей равно $\bigcup_{n=1}^{\infty} X^n$. Применение предложения 5.24 и теоремы 5.5 показывает, что это множество счетно.

Определение. Бесконечная последовательность (x_n) называется *периодической*, если существуют такие $k, l \geqslant 1$, что $x_{m+l} = x_m$ при любом $m > k$.

Выберем наименьшие k, l, обладающие свойством, сформулированным в определении. Тогда конечные последовательности $x_1, x_2, \ldots, x_k$ и $x_{k+1}x_{k+2}\ldots x_{k+l}$ называются соответственно непериодической частью и периодом данной бесконечной последовательности. Например, бесконечная последовательность

$$(3, 4, 1, 2, 8, 5, 6, 4, 2, 8, 5, 6, 4, \ldots, 2, 8, 5, 6, 4, \ldots)$$

является периодической, причем $k = 3$, $l = 5$, непериодическая часть равна $(3, 4, 1)$, а период равен $(2, 8, 5, 6, 4)$.

Предложение 5.26. *Если X – счетное множество, то множество всех бесконечных периодических последовательностей, составленных из элементов множества X, счетно.*

Доказательство. Пусть X_p – множество всех бесконечных периодических последовательностей, составленных из элементов множества X. Каждая последовательность (x_n) из X_p однозначно определяет непериодическую часть и период. Тем самым задано отображение из X_p в прямое произведение $X_{fin} \times X_{fin}$. Поскольку непериодическая часть и период определяют последовательность также однозначно, указанное отображение инъективно. Из теоремы 5.5 и предложения 5.25 следует, что $X_{fin} \times X_{fin}$ – счетное множество. Так как построено инъективное отображение из X_p в счетное множество, можно заключить, что X_p также счетно.

5.7. Равномощность множеств

Пусть X, Y – произвольные непустые множества.

Если существует инъективное (соответственно биективное) отображение из X в Y, то говорят, что *мощность X не больше мощности Y* (соответственно *мощность X равна мощности Y*).

Введем обозначения: $|X| \leqslant |Y|$, если мощность X не больше мощности Y, и $|X| = |Y|$, если мощность X равна мощности Y. Если $|X| = |Y|$, то будем также говорить, что множества X и Y равномощны.

Заметим, что из включения $X \subseteq Y$ вытекает неравенство $|X| \leqslant |Y|$. Обратное утверждение, разумеется, неверно.

Пусть X, Y – счетные множества, Z – бесконечное множество. Тогда $|X| = |Y|$ и $|X| \leqslant |Z|$. Последнее неравенство вытекает из известного нам утверждения: всякое бесконечное множество содержит счетное подмножество.

Кроме того, имеет место следующее простое утверждение.

Предложение 5.27. *Пусть X – бесконечное, а Y – счетное множество. Тогда множества $X \cup Y$ и X равномощны.*

Доказательство. Поскольку X бесконечно, оно содержит счетное подмножество Z. Множество $Z \cup Y$ счетно, поэтому су-

ществует биективное отображение g из $Z \cup Y$ на Y. Нетрудно видеть, что отображение

$$f : X \cup Y \longrightarrow X,$$

заданное правилом

$$f(x) = \begin{cases} x, & \text{если } x \in X \setminus Z, \\ g(x), & \text{если } x \in Z \cup Y, \end{cases}$$

также является биективным.

Приведем несколько важных примеров равномощных множеств.

1. Интервалы $(0;1)$ и $(a;b)$ равномощны.

В самом деле, отображение $f : (0;1) \longrightarrow (a;b)$, определенное формулой $f(x) = (b-a)x + a$, очевидно, является биективным.

2. Интервал $(0;1)$ и множество $\mathbb{R}$ равномощны.

Действительно, пусть

$$g(x) = \begin{cases} 2 - 1/x, & \text{если } 0 < x \leqslant 1/2, \\ 1/(1-x) - 2, & \text{если } 1/2 < x < 1. \end{cases}$$

Легко проверить, что g биективное отображение.

3. Интервал $(0;1)$ и полуинтервал $(0;1]$ равномощны.

Положим

$$h(x) = \begin{cases} x/2, & \text{если } x = 1/2^n,\ n \geqslant 0 \\ x, & \text{в противном случае.} \end{cases}$$

Читатель без труда убедится, что h биективно отображает полуинтервал $(0;1]$ на интервал $(0;1)$.

Из свойств инъективных и биективных отображений вытекают следующие утверждения.

Предложение 5.28. *Пусть X, Y, Z – произвольные непустые множества. Тогда*

1) $|X| = |X|$;

2) *если* $|X| = |Y|$, *то* $|Y| = |X|$;

3) *если* $|X| = |Y|$ *и* $|Y| = |Z|$, *то* $|X| = |Z|$.

Предложение 5.29. *Пусть X, Y, Z – произвольные непустые множества. Тогда*

1) $|X| \leqslant |X|$;
2) *если* $|X| \leqslant |Y|$ *и* $|Y| \leqslant |Z|$, *то* $|X| \leqslant |Z|$;
3) *если* $|X| \leqslant |Y|$, *то* $|Z^X| \leqslant |Z^Y|$;
4) *если* $|Y| \leqslant |Z|$, *то* $|Y^X| \leqslant |Z^X|$.

А что будет в том случае, когда одновременно $|X| \leqslant |Y|$ и $|Y| \leqslant |X|$? Оказывается, справедлива

Теорема 5.6. *Если* $|X| \leqslant |Y|$ *и* $|Y| \leqslant |X|$, *то* $|X| = |Y|$.

Эту теорему часто называют теоремой Кантора[1]– Бернштейна[2].

Доказательство теоремы 5.6 основано на следующем вспомогательном утверждении.

Лемма 1. *Пусть X – бесконечное множество, Y – его собственное подмножество, равномощное X. Если $Z_0 \subseteq X \setminus Y$, то множества $Y \cup Z_0$ и Y равномощны.*

Доказательство. Пусть f – биективное отображение из X на Y. Для каждого натурального числа n рассмотрим множество $Z_n = f^n(Z_0)$. Ясно, что

$$f(Z_k) = Z_{k+1} \tag{8}$$

при любом $k \geqslant 0$. Пусть $Z = \bigcup_{n=1}^{\infty} Z_n$. Легко видеть, что

$$f(Z_0 \cup Z) = Z. \tag{9}$$

В самом деле, включение $f(Z_0 \cup Z) \subseteq Z$ вытекает из равенств (8). Проверим обратное включение. Пусть $y \in Z$. Тогда $y \in Z_n$ при некотором $n \geqslant 1$. Стало быть, $y = f(u)$ для некоторого $u \in Z_{n-1}$. Так как $Z_{n-1} \subseteq Z_0 \cup Z$, получаем, что $y = f(u) \in f(Z_0 \cup Z)$.

Рассмотрим отображение g из $Z_0 \cup Y$ в Y, определенное правилом

$$g(y) = \begin{cases} f(y), & \text{если } y \in Z_0 \cup Z, \\ y, & \text{если } y \in Y \setminus Z. \end{cases}$$

[1]Г. Кантор (1845–1918) – немецкий математик, создатель теории множеств.
[2]Ф. Бернштейн (1878–1950) – немецкий математик.

Из равенства (9) сразу вытекает, что g – сюръективное отображение. Проверим, что g инъективно. Пусть $u, v \in Z_0 \cup Y$ и $g(u) = g(v)$. Из равенства (9) и определения отображения g следует, что либо $u, v \in Y \setminus Z$, либо $u, v \in Z_0 \cup Z$. В том случае, когда $u, v \in Y \setminus Z$, имеем

$$u = g(u) = g(v) = v.$$

Если же $u, v \in Z_0 \cup Z$, то

$$f(u) = g(u) = g(v) = f(v),$$

откуда, в силу инъективности f снова получаем $u = v$. Стало быть, из равенства $g(u) = g(v)$ следует равенство $u = v$.

Итак, g – биективное отображение из $Z_0 \cup Y$ на Y; поэтому $Z_0 \cup Y$ и Y равномощны.

Доказательство теоремы 5.6. Поскольку $|X| \leqslant |Y|$ и $|Y| \leqslant |X|$, существуют инъективные отображения

$$f : X \longrightarrow Y, \qquad g : Y \longrightarrow X.$$

Рассмотрим множества $X_0 = g(Y)$ и $X_1 = g \circ f(X)$. Ясно, что $X_1 \subseteq X_0 \subseteq X$ и $|X_1| = |X|$, $|X_0| = |Y|$. Если $X_1 = X_0$, то, в частности, $|X_1| = |X_0|$, и из предложения 5.28 следует равномощность X и Y. Предположим, что $X_1 \subset X_0$. Тогда к множеству X и его подмножествам X_1 и $Z_0 = X_0 \setminus X_1$ применима лемма 1. Поэтому $|X_1| = |X_1 \cup Z_0| = |X_0|$. Поскольку проверена равномощность множеств X_1, X_0, то множества X и Y также равномощны.

5.8. Несчетные множества

В этом разделе мы приведем несколько примеров бесконечных множеств, не являющихся счетными. Такие множества называются *несчетными.*

Пусть X – бесконечное множество. Чтобы убедиться в том, что X несчетно, достаточно установить, что не существует биективного отображения из $\mathbb{N}$ на X. Иными словами, нужно проверить, что $|\mathbb{N}| \neq |X|$. Поскольку в этом случае $|\mathbb{N}| \leqslant |X|$, то естественно сказать, что мощность множества $\mathbb{N}$ строго меньше мощности

множества X. Нетрудно понять, что соответствующее определение можно дать и для более общего случая.

Будем говорить, *мощность множества X строго меньше мощности множества Y* ($|X| < |Y|$), если $|X| \leqslant |Y|$ и $|X| \neq \neq |Y|$. Часто вместо $|X| < |Y|$ пишут $|Y| > |X|$ и говорят, что *мощность Y строго больше мощности X*. Для того чтобы убедиться в справедливости неравенства $|X| < |Y|$, достаточно проверить два утверждения:

1) существует инъективное отображение из множества X во множество Y;

2) не существует сюръективного отображения из X на Y.

Действительно, если выполнено утверждение 1), то $|X| \leqslant |Y|$. Из выполнимости утверждения 2) вытекает, что не существует, в частности, и биективного отображения X на Y, откуда $|X| \neq |Y|$.

Теорема 5.7. *Множество всех бесконечных последовательностей, составленных из элементов множества $\{0, 1\}$, является несчетным.*

Доказательство. Предположим, что рассматриваемое множество счетно. Тогда все последовательности из нулей и единиц можно представить в виде строк бесконечной таблицы

$$\begin{array}{ccccc} a_{11} & a_{12} & \dots & a_{1n} & \dots \\ a_{21} & a_{22} & \dots & a_{2n} & \dots \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n1} & a_{n2} & \dots & a_{nn} & \dots \\ \vdots & \vdots & & \vdots & \ddots \end{array} \qquad (10)$$

Для каждого натурального n определим $b_n = 1 - a_{nn}$ и рассмотрим бесконечную последовательность (b_n). Легко понять, что эта последовательность отлична от каждой из последовательностей, являющихся строками таблицы (10). В самом деле, предположим, что последовательность (b_n) совпадает с k-ой строкой из таблицы (10). Это значит, что равенство $b_n = a_{kn}$ выполнено при любом n. В частности, оно выполнено и при $n = k$. Но равенство $b_k = a_{kk}$ невозможно, поскольку $b_k = 1 - a_{kk}$ и $a_{kk} \in \{0, 1\}$. Таким образом, получено противоречие: с одной стороны, мы предположили, что

каждая последовательность из нулей и единиц является строкой таблицы (10), а с другой – нашли последовательность, не являющуюся строкой этой таблицы.

Другим примером несчетного множества является множество $2^{\mathbb{N}}$, состоящее из всех отображений множества $\mathbb{N}$ в двухэлементное множество. Оказывается, существует биективное отображение из $2^{\mathbb{N}}$ на множество всех бесконечных последовательностей из нулей и единиц. Иными словами, эти два множества равномощны. Проверим это утверждение. Пусть f – произвольное отображение из $\mathbb{N}$ в двухэлементное множество $\{0, 1\}$. Тогда однозначно определена последовательность (a_n), где $a_n = f(n)$. Обратно, если задана последовательность (a_n), то правило $f(n) = a_n$ однозначно определяет отображение $f : \mathbb{N} \longrightarrow 2$.

Множества, равномощные множеству $2^{\mathbb{N}}$, играют важную роль в различных разделах математики.

О п р е д е л е н и е. Всякое множество, равномощное множеству $2^{\mathbb{N}}$, называется *множеством мощности континуум.*

Ниже будут приведены примеры различных множеств мощности континуум. А сейчас мы докажем утверждение, обобщающее утверждение о несчетности множества $2^{\mathbb{N}}$.

Теорема 5.8 (теорема Кантора). *Пусть X – произвольное непустое множество. Тогда $|X| < |2^X|$.*

Д о к а з а т е л ь с т в о. Нетрудно понять, что $|X| \leqslant |2^X|$. В самом деле, для каждого элемента $x \in X$ определено такое отображение

$$h_x : X \longrightarrow 2,$$

что $h_x(y) = 1$ тогда и только тогда, когда $y = x$. Ясно, что тем самым задано отображение

$$\varphi : X \longrightarrow 2^X,$$

определенное правилом $\varphi(x) = h_x$. Нетрудно понять, что отображение φ инъективно.

Осталось убедиться в том, что не существует сюръективного отображения из X на 2^X.

Рассмотрим произвольное отображение

$$\varphi : X \longrightarrow 2^X$$

и проверим, что его образ отличен от множества 2^X. Пусть x – произвольный элемент множества X. Тогда определено отображение

$$\varphi(x) : X \longrightarrow 2.$$

Для удобства будем вместо $\varphi(x)$ писать φ_x. Определим теперь отображение

$$f : X \longrightarrow 2$$

при помощи правила $f(x) = 1 - \varphi_x(x)$, $x \in X$. Легко видеть, что при любом $x \in X$ выполнено неравенство

$$f \neq \varphi_x. \tag{11}$$

В самом деле, предположим, что $f = \varphi_y$ для некоторого $y \in X$. Тогда должно выполняться равенство $f(y) = \varphi_y(y)$. Но по определению $f(y) = 1 - \varphi_y(y)$, и мы получаем противоречивое утверждение $\varphi_y(y) = 1 - \varphi_y(y)$. Итак, мы доказали, что каково бы ни было отображение $\varphi : X \longrightarrow 2^X$, обязательно найдется отображение $f : X \longrightarrow 2$, не принадлежащее образу отображения φ. Иными словами, отображение φ не является сюръективным, а потому оно не может быть и биективным.

Таким образом, проверено, что $|X| \leqslant |2^X|$ и $|X| \neq |2^X|$, откуда следует неравенство $|X| < |2^X|$.

Способ, примененный при доказательстве теорем 5.7 и 5.8, часто называют *диагональным методом Кантора*. Разумеется, такие доказательства используются не только при изучении множеств, но и в других разделах современной математики.

Вернемся к обсуждению множеств мощности континуум.

Теорема 5.9. *Пусть X – произвольное непустое множество, причем $2 \leqslant |X| \leqslant |2^{\mathbb{N}}|$. Тогда множество $X^{\mathbb{N}}$ имеет мощность континуум.*

Доказательство. Так как $2 \leqslant |X| \leqslant |2^{\mathbb{N}}|$, с использованием предложения 5.29 имеем

$$|2^{\mathbb{N}}| \leqslant |X^{\mathbb{N}}| \leqslant |(2^{\mathbb{N}})^{\mathbb{N}}|. \tag{12}$$

Из предложения 5.7 вытекает, что

$$|(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}|. \tag{13}$$

Поскольку множество $\mathbb{N} \times \mathbb{N}$ счетно, выполнено равенство

$$|2^{\mathbb{N}\times\mathbb{N}}| = |2^{\mathbb{N}}|. \tag{14}$$

Из соотношений (12) – (14) легко следует, что $|2^{\mathbb{N}}| \leqslant |X^{\mathbb{N}}|$ и $|X^{\mathbb{N}}| \leqslant$ $\leqslant |2^{\mathbb{N}}|$. Теорема Кантора-Бернштейна показывает теперь, что $|X^{\mathbb{N}}| = |2^{\mathbb{N}}|$.

Из теоремы 5.9 вытекает ряд важных следствий.

Предложение 5.30. *Множество чисел из интервала* $(0; 1)$ *имеет мощность континуум.*

Доказательство. Известно, что каждое действительное число $d \in (0; 1)$ можно однозначно представить в виде бесконечной десятичной дроби $0, d_1 d_2 \ldots d_n \ldots$, не содержащей в периоде цифры 9. Пусть $D = \{0, 1, 2, \ldots, 9\}$ – множество десятичных цифр. Нетрудно понять, множество чисел из полуинтервала $[0; 1)$ равномощно множеству всех бесконечных последовательностей, составленных из элементов множества D и не содержащих 9 в периоде. Множество $D^{\mathbb{N}}$, состоящее из всех бесконечных последовательностей элементов из D, имеет мощность континуум (это следует из теоремы 5.9). Обозначим через X множество всех бесконечных последовательностей, имеющих 9 в периоде. Это множество, очевидно, бесконечно, и потому, в силу предложения 5.26, счетно. Из предложения 5.27 вытекает, что множество $D^{\mathbb{N}} \setminus X$ равномощно множеству $D^{\mathbb{N}}$. Последнее множество континуально, а потому и множество $D^{\mathbb{N}} \setminus X$ имеет мощность континуум. Итак, мы проверили, что множество точек полуинтервала $[0; 1)$ имеет мощность континуум. Осталось заметить, что интервал $(0; 1)$ и полуинтервал $[0; 1)$ равномощны.

Следствие 1. *Любой интервал имеет мощность континуум.*

Следствие 2. *Множество* $\mathbb{R}$ *имеет мощность континуум.*

Эти следствия непосредственно вытекают из примеров 1, 2 разд. 5.7 и теоремы 5.30.

Рассмотрим произвольное числовое множество X, содержащее некоторый интервал $(a; b)$.

Из очевидных включений $(a; b) \subseteq X \subseteq \mathbb{R}$ получаем

$$|(a; b)| \leqslant |X| \leqslant |\mathbb{R}|.$$

Поскольку $|(a; b)| = |\mathbb{R}|$, имеем $|X| = |(a; b)|$. Следовательно, справедлива

Теорема 5.10. *Пусть X – произвольное множество действительных чисел, содержащее некоторый интервал. Тогда множество X имеет мощность континуум.*

Пусть A, B – непересекающиеся счетные множества. Тогда множества 2^A, 2^B имеют мощность континуум. Имеем

$$|2^A \times 2^B| = |2^{A \cup B}|.$$

Ясно, что $A \cup B$ – счетное множество, поэтому $2^{A \cup B}$ имеет мощность континуум.

Стало быть, справедлива

Теорема 5.11. *Прямое произведение двух множеств мощности континуум само имеет мощность континуум.*

Заметим, что на координатной плоскости прямоугольник со сторонами, параллельными осям координат, можно считать прямым произведением двух отрезков. Таким образом, из теоремы 5.11 вытекает

Предложение 5.31. *Множество всех точек любого прямоугольника имеет мощность континуум.*

6. Числовые функции

6.1. Определение числовой функции

Пусть X – числовое множество.

О п р е д е л е н и е. Отображение f из X в $\mathbb{R}$ называется числовой функцией.

Таким образом, числовая функция f каждому числу из множества X ставит в соответствие единственное число $f(x)$. Заметим, что вся терминология и все обозначения, введенные нами при изучении отображений, полностью сохраняются и для числовых функций. В частности, множество X – это область определения функции f. Как и раньше запись $f : X \longrightarrow \mathbb{R}$ означает, что f является функцией с областью определения X.

Как правило, в школьном курсе математики наиболее употребительным является задание функций при помощи формул. А именно, пусть $g(x)$ – некоторое алгебраическое выражение с одной переменной x. Обозначим через D область определения выражения $g(x)$. (Напомним, что область определения выражения $g(x)$ – это множество всех чисел, при подстановке каждого из которых вместо x выражение $g(x)$ имеет смысл.) Рассмотрим функцию $g : D \to R$, заданную правилом: каждому $x \in D$ сопоставляется $y = g(x) \in R$. Множество D называется *естественной областью определения* функции g.

Пусть X – некоторое подмножество множества D. Запись

$$y = g(x), \quad x \in X,$$

обозначает функцию $g : X \longrightarrow \mathbb{R}$, ставящую в соответствие числу $x \in X$ число $y = g(x) \in \mathbb{R}$.

Примеры:

1. $y = x^2$, $x \geqslant 0$.

2. $y = \sqrt{x-1}$.

Графики этих функций представлены на рис. 2.

Пусть $f : X \longrightarrow \mathbb{R}$ – некоторая числовая функция. Ее множеством значений называется множество

$$\{y \in \mathbb{R} | y = f(x) \text{ для некоторого } x \in X\}.$$

Примеры:

1) множество значений функции $y = 2\{x\} - 1$ – полуинтервал $[-1; 1)$;

2) множество значений функции $y = 1 - x^2$ – луч $(-\infty; 1]$.

Для отыскания множества значений функции $y = f(x)$, $x \in X$, можно использовать следующее обстоятельство. Уравнение $y = f(x)$ содержит две переменные. Будем считать, что в этом уравнении x – неизвестная величина, а y – параметр. Нетрудно понять, что число y принадлежит множеству значений функции $y = f(x)$, $x \in X$, тогда и только тогда, когда уравнение $f(x) = y$ имеет хотя бы одно решение на множестве X.

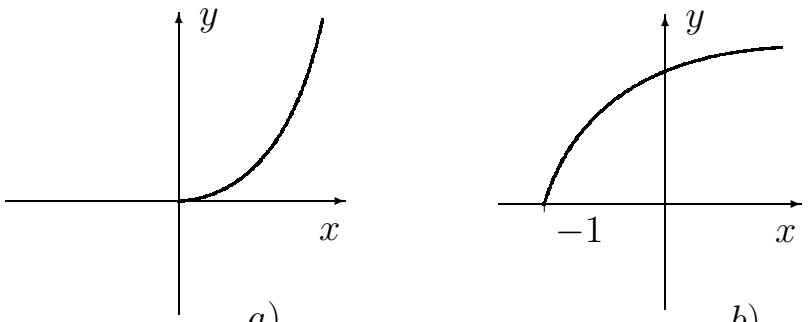

Рис. 2

Рассмотрим несколько задач на отыскание множеств значений функций.

1. Найти множество значений функции $y = 5 - \sqrt{x+2}$.

□ Поскольку $y = 5 - \sqrt{x+2} \Leftrightarrow \sqrt{x+2} = 5 - y$, данное уравнение имеет решение тогда и только тогда, когда $5 - y \geqslant 0$, $y \leqslant 5$.

Ответ: $(-\infty; 5]$. □

2. Найти множество значений функции $y = x - 2\sqrt{x+2}$.

□ В уравнении $x - 2\sqrt{x+2} = y$ сделаем замену $\sqrt{x+2} = t$. Получим уравнение $t^2 - 2t - 2 - y = 0$. Поскольку $t \geqslant 0$, вопрос о разрешимости исходного уравнения сводится к вопросу о разрешимости системы

$$\begin{cases} t^2 - 2t - 2 - y = 0, \\ t \geqslant 0. \end{cases}$$

Дискриминант D квадратного трехчлена $t^2 - 2t - 2 - y$ равен $4y + 12$. Если система имеет решение, то разрешимо уравнение

$t^2 - 2t - 2 - y = 0$, откуда $D \geqslant 0$, т. е. $y \geqslant -3$. Нетрудно видеть, что для всякого $y \geqslant -3$ система разрешима. В самом деле, пусть t_1, t_2 – корни уравнения $t^2-2t-2-y = 0$. Тогда $t_1+t_2 = 2$, поэтому среди чисел t_1, t_2 по крайней мере одно является положительным.

Ответ: $[-3; +\infty)$. □

3. Найти множество значений функции $y = x + 4/x$.

□ Поскольку уравнения $y = x + 4/x$ и $x^2 - xy + 4 = 0$ равносильны, достаточно найти те y, при которых разрешимо уравнение $x^2 - xy + 4 = 0$. Так как $D = y^2 - 16$, то имеем $y^2 - 16 \geqslant 0$, откуда $y \leqslant -4$, $y \geqslant 4$.

Ответ: $(-\infty; -4] \cup [4; +\infty)$. □

4. Найти множество значений функции $y = \dfrac{x}{x^2 + x + 1}$.

□ Уравнение

$$y = \frac{x}{x^2 + x + 1}$$

равносильно уравнению $yx^2 + (y - 1)x + y = 0$. При $y = 0$ это уравнение имеет решение $x = 0$. При $y \neq 0$ уравнение $yx^2 + +(y-1)x+y = 0$ является квадратным (относительно x) и имеет решения, если $D = (y - 1)^2 - 4y^2 \geqslant 0$, т. е. $-3y^2 - 2y + 1 \geqslant 0$, откуда $-1 \leqslant y < 0$, $0 < y \leqslant 1/3$.

Ответ: $[-1; 1/3]$. □

5. Найти множество значений функции $y = \dfrac{1 + \{x\}}{2 - \{x\}}$.

□ Уравнение

$$y = \frac{1 + \{x\}}{2 - \{x\}}$$

равносильно уравнению $2y - y\{x\} = 1 + \{x\}$, или $(y + 1)\{x\} = = 2y - 1$. Замена $t = \{x\}$ приводит к системе

$$\begin{cases} (y + 1)t = 2y - 1, \\ 0 \leqslant t < 1. \end{cases}$$

При $y = -1$ уравнение $(y + 1)t = 2y - 1$ решений не имеет. Пусть $y \neq -1$. Тогда $t = (2y - 1)/(y + 1)$ и из условия $0 \leqslant t < 1$ получаем

$$0 \leqslant \frac{2y - 1}{y + 1} < 1.$$

Решая последнее неравенство методом интервалов, получим

Ответ: $[1/2; 2)$. $\square$

6.2. Свойства числовых функций

В этом разделе мы напоминаем определения изучаемых в школьном курсе математики свойств числовых функций. Такие свойства, как четность, нечетность и ограниченность не нуждаются в особых комментариях. Понятие периодической функции является более сложным, чем предыдущие, и потому заслуживает развернутого комментария. Монотонным функциям посвящен отдельный раздел. В разделе 6.5 вводится важное понятие выпуклой вниз (вверх) функции.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *четной*, если для любого $x \in X$ выполнено условие $-x \in X$ и $f(-x) = = f(x)$.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *нечетной*, если для любого $x \in X$ выполнено условие $-x \in X$ и $f(-x) = = -f(x)$.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *возрастающей на промежутке* $E \subset X$, если для любых $x_1, x_2 \in E$ из неравенства $x_1 < x_2$ следует неравенство $f(x_1) < f(x_2)$.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *убывающей на промежутке* $E \subset X$, если для любых $x_1, x_2 \in E$ из неравенства $x_1 < x_2$ следует неравенство $f(x_1) > f(x_2)$.

О п р е д е л е н и е. Функция называется *монотонной на промежутке* E, если на этом промежутке она либо возрастающая, либо убывающая.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *ограниченной*, если существует такой отрезок $[m; M]$, что $f(x) \in \in [m; M]$ для любого $x \in X$.

О п р е д е л е н и е. Функция $y = f(x)$, $x \in X$, называется *периодической*, если существует такое $T \neq 0$, что для любого $x \in X$ выполнено условие: $x - T \in X$, $x + T \in X$ и $f(x + T) = f(x)$.

Такое число T называется периодом функции $y = f(x)$. Заметим, что если T – период функции, то

$$f(x - T) = f(x - T + T) = f(x),$$

т. е. $-T$ – также период. Более того, для любого целого $k \neq 0$ число kT является периодом. Наименьший положительный период (если такой существует) называется *основным* периодом данной периодической функции. Например, функция $y = \{x\}$ является периодической и ее основной период равен 1, поскольку $\{x\} = \{x + k\}$ для $k \in Z$. Основной период функций $y = \sin x$, $y = \cos x$ равен 2π, а основной период функций $y = \operatorname{tg} x$, $y = \operatorname{ctg} x$ есть π. Заметим, что существуют периодические функции, не имеющие основного периода. Простейший пример доставляет функция $y = a$, где a – фиксированное число. Ясно, что периодом этой функции является любое отличное от нуля число. Менее тривиальным примером периодической функции без основного периода является функция Дирихле $d(x)$, определенная правилом:

$$d(x) = \begin{cases} 1, \text{ если } x \in Q, \\ 0, \text{ если } x \in R \setminus Q. \end{cases}$$

Ее периодом является любое рациональное число $r \neq 0$; это следует из следующего легко проверяемого утверждения:

$$x \in Q \Leftrightarrow x + r \in Q.$$

Рассмотрим несколько задач на изучение свойств функций.

1. Доказать, что функция $y = \sqrt{x}$ является возрастающей.

□ Пусть $f(x) = \sqrt{x}$. Ясно, что $D(f) = [0; +\infty)$. Возьмем произвольные $x_1, x_2 \in [0; +\infty)$, $x_1 < x_2$, и вычислим разность:

$$f(x_1) - f(x_2) = \sqrt{x_1} - \sqrt{x_2} = \frac{x_1 - x_2}{\sqrt{x_1} + \sqrt{x_2}}.$$

Из полученного равенства видно, что $x_1 - x_2 < 0 \Rightarrow f(x_1) - -f(x_2) < 0$, т. е. $y = f(x)$ – возрастающая функция. □

2. Доказать, что функция $y = x^3 - 3x$ убывает на отрезке $[-1; 1]$ и возрастает на каждом из лучей $(-\infty; -1]$ и $[1; +\infty)$.

□ Пусть $x_1 > x_2$. Рассмотрим разность

$$y(x_1) - y(x_2) = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 - 3).$$

Если $x_1, x_2 \in (-\infty; -1]$ или $x_1, x_2 \in [1; +\infty)$, то $x_1^2 \geqslant 1$, $x_2^2 \geqslant 1$, $x_1x_2 > 1$ и потому $x_1^2 + x_1x_2 + x_2^2 > 3$. Стало быть, в этом случае число $x_1^2 + x_1x_2 + x_2^2 - 3$ положительно. Так как $x_1 - x_2 > 0$, имеем $y(x_1) > y(x_2)$, т. е. функция возрастает на каждом из лучей $(-\infty; -1]$ и $[1; +\infty)$.

Пусть $x_1, x_2 \in [-1; 1]$. Тогда выполнены неравенства $|x_1| \leqslant 1$, $|x_2| \leqslant 1$. Если хотя бы одно из этих двух неравенств строгое, то $|x_1x_2| < 1$. Поскольку $x_1^2 \leqslant 1$, $x_2^2 \leqslant 1$, имеем

$$x_1^2 + x_1x_2 + x_2^2 \leqslant |x_1^2 + x_1x_2 + x_2^2| \leqslant x_1^2 + |x_1x_2| + x_2^2 < 3.$$

В противном случае $x_1 = -1$, $x_2 = 1$, откуда следует, что $x_1^2 + {} + x_1x_2 + x_2^2 = 1 < 3$. Стало быть, число $x_1^2 + x_1x_2 + x_2^2 - 3$ отрицательно при любых $x_1, x_2 \in [-1; 1]$. Так как разность $x_1 - x_2$ положительна, получаем, что $y(x_1) < y(x_2)$, т. е. функция убывает на отрезке $x_1, x_2 \in [-1; 1]$. □

3. Доказать, что функция $y = x/(x^2 + 1)$ является ограниченной.

□ Пусть $f(x) = x/(x^2 + 1)$. Поскольку $x^2 + 1 \geqslant 2|x|$ при любом $x \in R$, имеем:

$$|f(x)| = \frac{|x|}{x^2 + 1} \leqslant \frac{x^2 + 1}{2(x^2 + 1)} = \frac{1}{2}.$$

Таким образом, $f(x) \in \left[-\frac{1}{2}; \frac{1}{2}\right]$ для всякого $x \in R$, т. е. $y = {} = f(x)$ – ограниченная функция. □

4. Найти основной период функции $y = \{3x/2\} + \{x/3\}$.

□ Данная функция является периодической, так как

$$\left\{\frac{3(x+6)}{2}\right\} + \left\{\frac{x+6}{3}\right\} = \left\{\frac{3}{2}x + 9\right\} + \left\{\frac{x}{3} + 2\right\} = \left\{\frac{3}{2}x\right\} + \left\{\frac{x}{3}\right\}.$$

Пусть $T > 0$ – основной период. Тогда равенство

$$\left\{\frac{3(x+T)}{2}\right\}+\left\{\frac{x+T}{3}\right\}=\left\{\frac{3}{2}x\right\}+\left\{\frac{x}{3}\right\}.$$

выполнено при всех x. Подставляя в это равенство $x=0$, получим $\{3T/2\}+\{T/3\}=0$. Так как $\{3T/2\}\geqslant 0$, $\{T/3\}\geqslant 0$, то число T одновременно удовлетворяет равенствам $\{3T/2\}=0$, $\{T/3\}=0$, откуда $3T/2=n$, $T/3=m$ для некоторых $n,m\in Z$. Поскольку $T=2n/3$ и $T=3m$, имеем $2n/3=3m$, $2n=9m$. Учитывая, что $n,m\in Z$, из последнего равенства получаем, что m – четно, т. е. $m=2k$, $k\in Z$. Таким образом, $T=6k$. Мы получили, что если T – период, то $T\in Z$ и T кратно шести. Поскольку выше мы проверили, что число 6 – период данной функции, получаем, что 6 – основной период. □

5. Доказать, что функция $y=\{|x|\}$ не является периодической.

□ Доказательство проведем методом "от противного". Пусть $y=\{|x|\}$ – периодическая функция и T – ее период, причем $T>0$. Тогда

$$\{|x+T|\}=\{|x|\} \tag{1}$$

для любого x. Подставляя в это равенство $x=0$, с учетом неравенства $T>0$ получим $T=k$, где $k\in\mathbb{N}$. Положим теперь в равенстве (1) $x=-1/4$. Тогда $\{|T-1/4|\}=1/4$. Поскольку T принимает натуральные значения, $T>1/4$; поэтому $\{(T-1/4)\}=$ $=1/4$, откуда $T-1/4=1/4+m$ для некоторого целого m. Стало быть $T=k=m+1/2$. Противоречие. □

6. Доказать, что функция $y=\{x\}+\{\sqrt{2}x\}$ не является периодической.

□ Как и в предыдущей задаче, для доказательства применим метод "от противного". Пусть данная функция является периодической и $T>0$ – один из ее периодов. Тогда равенство

$$\{x+T\}+\{\sqrt{2}(x+T)\}=\{x\}+\{\sqrt{2}x\}$$

выполнено при всех x. Подставляя $x=0$, получим $y=\{T\}+$ $+\{\sqrt{2}T\}$. Рассуждая далее, как в задаче 4, найдем, что $T=n$ и $\sqrt{2}T=m$, $n,m\in Z$. Так как $T\neq 0$, то, поделив второе уравнение на первое, получим $\sqrt{2}=m/n$. Последнее равенство невозможно, так как $\sqrt{2}$ – иррациональное число. □

6.3. Монотонные функции

В этом разделе мы докажем несколько утверждений о монотонных функциях.

Сначала сформулируем необходимое и достаточное условие монотонности функции на промежутке. Рассмотрим графики двух функций, одна из которых возрастает (рис. $3, a$), а другая убывает (рис. $3, b$) на данном промежутке.

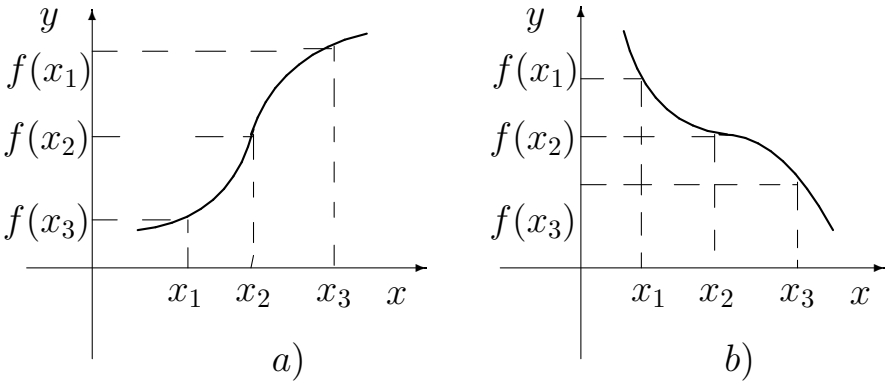

Рис. 3

Легко видеть, что каждая из этих функций обладает следующим свойством: каковы бы ни были x_1, x_2, x_3 из промежутка монотонности из того, что x_2 лежит между x_1, x_3 следует, что $f(x_2)$ лежит между $f(x_1), f(x_3)$. Оказывается, это условие является необходимым и достаточным для монотоности функции на промежутке.

Теорема 6.1. *Функция $y = f(x), x \in X$ монотонна на промежутке $E \subseteq X$ тогда и только тогда, когда для любых $x_1, x_2, x_3 \in \in E$ из неравенства*

$$(x_2 - x_1)(x_3 - x_2) > 0 \tag{2}$$

следует неравенство

$$(f(x_2) - f(x_1))(f(x_3) - f(x_2)) > 0. \tag{3}$$

Доказательство. Проверим, что сформулированное условие влечет монотонность. Пусть $t_1, t_2 \in E$, причем $t_1 < t_2$. Предположим, что $f(t_1) < f(t_2)$, и докажем, что в этом случае данная

функция возрастает на E. Пусть x – произвольное число из E, отличное от t_1, t_2. Допустим, что $x < t_1$. Тогда $(t_1 - x)(t_2 - t_1) > 0$, поэтому $(f(t_1) - f(x))(f(t_2) - f(t_1)) > 0$. Поскольку $f(t_2) - f(t_1) > 0$, получаем $f(t_1) - f(x) > 0$, т. е. $f(t_1) > f(x)$. Итак, имеем

$$x < t_1 \Longrightarrow f(x) < f(t_1). \tag{4}$$

Аналогично проверяется, что

$$t_1 < x < t_2 \Longrightarrow f(t_1) < f(x) < f(t_2) \tag{5}$$

Пусть $x_1, x_2 \in E$ и $x_1 < x_2$. Если x_1, x_2 лежат по разные стороны от t_1, то $x_1 < t_1 < x_2$, откуда при помощи соотношений (4) и (5) сразу вытекает, что $f(x_1) < f(t_1) < f(x_2)$, т. е. $f(x_1) < f(x_2)$. Предположим, что x_1, x_2 находятся по одну сторону от t_1. Из двух возможностей рассмотрим только одну: $x_1 < x_2 < t_1$. Тогда $f(x_2) < f(t_1)$. Теперь видно, что в соотношении (5) можно t_1, x, t_2 заменить на x_1, x_2, t_1. Отсюда снова $f(x_1) < f(x_2)$. Итак, доказано, что из предположения $f(t_1) < f(t_2)$ следует возрастание функции на промежутке E. Аналогично можно проверить, что неравенство $f(t_1) > f(t_2)$ влечет убывание функции на данном промежутке.

Проверка обратного утверждения очень проста и потому оставляется читателю.

Предложение 6.1. *Пусть функции $y = f(x)$, $y = g(x)$ возрастают (убывают) на промежутке E. Тогда их сумма $y = f(x) + g(x)$ также возрастает (убывает) на E.*

Доказательство. Пусть $x_1, x_2 \in E$ и $x_1 < x_2$. Тогда

$$(f(x_1) + g(x_1)) - (f(x_2) + g(x_2)) = f(x_1) - g(x_1) + f(x_2) - g(x_2).$$

Разности $f(x_1) - g(x_1)$, $f(x_2) - g(x_2)$ имеют одинаковые знаки; тот же знак, очевидно, имеет и разность $(f(x_1) + g(x_1)) - (f(x_2) + g(x_2))$.

Предложение 6.2. *Пусть функции $y = f(x)$, $y = g(x)$ возрастают (убывают) на промежутке E. Если обе функции положительны на E, то их произведение $y = f(x)g(x)$ также возрастает (убывает) на E.*

Доказательство. Для произвольных $x_1, x_2 \in E$, $x_1 < x_2$ имеем

$$f(x_1)g(x_1) - f(x_2)g(x_2) = f(x_1)(g(x_1) - g(x_2)) + g(x_2)(f(x_1 - f(x_2).$$

Разности $f(x_1) - g(x_1)$, $f(x_2) - g(x_2)$ имеют одинаковые знаки, а числа $f(x_1)$, $g(x_2)$ положительны, поэтому тот же знак имеет разность $f(x_1)g(x_1) - f(x_2)g(x_2)$.

Предложение 6.3. *Пусть функции $y = f(u)$, $u = g(x)$ монотонны в своих областях определения, причем $E(f) \subseteq D(g)$. Если функции f и g имеют одинаковый характер монотонности (т. е. либо обе возрастают, либо обе убывают), то их композиция возрастает на множестве $D(f)$; если же функции имеют различный характер монотонности, то их композиция убывает на том же множестве.*

Доказательство. Рассмотрим один из четырех возможных случаев: функция f убывает, а функция g возрастает. Если $x_1, x_2 \in$ $\in D(f)$ и $x_1 < x_2$, то $f(x_1) > f(x_2)$, и потому $g(f(x_1)) > g(f(x_2))$. Следовательно, композиция $g \circ f$ убывает на $D(f)$. Остальные случаи могут быть рассмотрены совершенно аналогично.

При помощи предложений 6.1 – 6.3 в некоторых случаях легко находить промежутки возрастания и убывания функций. Рассмотрим в качестве примера задачу: найти промежутки возрастания и убывания функции

$$y = \frac{2x^2 - 2x + 1}{x^2}. \tag{6}$$

Перепишем уравнение (6) в виде

$$y = 2 - \frac{2}{x} + \frac{1}{x^2}.$$

Пусть $g(u) = 2 - 2u + u^2$, $f(x) = 1/x$. Тогда исходная функция является композицией функций $y = g(u)$ и $u = f(x)$. Нетрудно проверить, что функция g убывает на луче $(-\infty; 1]$ и возрастает на луче $[1; +\infty)$, а функция f убывает на каждом из лучей $(-\infty; 0)$ и $(0; +\infty)$. Чтобы воспользоваться предложением 6.3, поступим следующим образом. Заметим сначала, что

$$f(x) \in [1; +\infty) \Longleftrightarrow 0 < x \leqslant 1.$$

Рассмотрим пару функций $y = 2 - 2u + u^2, u \geqslant 1$ и $u = 1/x$, $0 < x \leqslant 1$. Первая из этих функций возрастает, вторая убывает, поэтому их композиция убывает. Но эта композиция определена на полуинтервале $(0; 1]$. Стало быть, на исходная функция убывает на полуинтервале $(0; 1]$. Далее,

$$f(x) \in (0; 1] \Longleftrightarrow x \geqslant 1.$$

Аналогично предыдущему, введем в рассмотрение две функции $y = 2 - 2u + u^2, 0 < u \leqslant 1$ и $u = 1/x, x \geqslant 1$. Теперь обе функции убывающие, поэтому их композиция возрастает в своей области определения. Отсюда вытекает, что исходная функция возрастает на луче $[1; +\infty)$. Наконец, рассматривая функции $y = 2 - 2u + u^2, u < 0$ и $u = 1/x, x < 0$, можно убедиться, что исходная функция возрастает на луче $(-\infty; 0)$.

6.4. Применение свойств функций для решения уравнений

1. Решить уравнение $(x^2 + 1)(x^2 - 2x + 2) = 2x$.

□ Запишем данное уравнение в виде

$$x^2 - 2x + 2 = \frac{2x}{x^2 + 1}. \tag{7}$$

Заметив, что $x^2 - 2x + 2 = (x - 1)^2 + 1$, имеем

$$x^2 - 2x + 2 \geqslant 1.$$

Так как правая часть уравнения (7) при $x \leqslant 0$ неположительна, получаем, что на луче $-(\infty; 0]$ уравнение решений не имеет. Пусть $x > 0$. Тогда $x^2 + 1 \geqslant 2x$, поэтому

$$\frac{2x}{x^2 + 1} \leqslant \frac{2x}{2x} = 1.$$

Следовательно, на луче $(0; +\infty)$ уравнение (7) равносильно системе

$$\begin{cases} x^2 - 2x + 2 = 1, \\ \dfrac{2x}{x^2 + 1} = 1. \end{cases}$$

Единственным решением этой системы является $x = 1$. $\square$

2. Решить уравнение $x^3 + x = \sqrt{x+2}(x+3)$.

$\square$ Заметим, что $\sqrt{x+2}(x+3) = (\sqrt{x+2})^3 + \sqrt{x+2}$. Если x^3+x обозначить через $f(x)$, то данное уравнение можно переписать в виде $f(x) = f(\sqrt{x+2})$. Но функция $= f(x)$ является возрастающей (проверьте это утверждение) и потому каждое свое значение принимает только один раз. Отсюда следует, что

$$f(x) = f(\sqrt{x+2}) \Longleftrightarrow x = \sqrt{x+2}.$$

Уравнение $x = \sqrt{x+2}$ равносильно системе

$$\begin{cases} x^2 = x + 2, \\ x \geqslant 0, \end{cases}$$

откуда $x = 2$. $\square$

3. Решить уравнение $x^5 + x^2 + x = 3$.

$\square$ Заметив, что $x = 0$ не является решением этого уравнения, перепишем его в виде

$$x^4 + x + 1 = \frac{3}{x}.$$

Легко убедиться, что выражение $x^4 + x + 1$ принимает только положительные значения. Это очевидно при положительных x. Пусть x отрицательно. Если $x \leqslant -1$, то $x^4 \geqslant |x|$. Следовательно,

$$x^4 + x + 1 \geqslant |x| + x + 1 \geqslant 1.$$

Если же $-1 \leqslant x < 0$, то $1 + x \geqslant 0$, и потому

$$x^4 + x + 1 > 0.$$

Отсюда вытекает, что на луче $(-\infty; 0)$ данное уравнение решений не имеет, поскольку при $x < 0$ выражение $3/x$ отрицательно.

Осталось решить уравнение на луче $(0; +\infty)$. Легко проверить, что на этом луче функция $y = x^4 + x + 1$ возрастает, а функция $y = 3/x$ убывает. Отсюда немедленно следует, что на луче $(0; +\infty)$ наше уравнение имеет не более одного решения. Поскольку $x = 1$ является решением данного уравнения, получаем, что 1 является единственным его решением. $\square$

Следующее утверждение иногда оказывается полезным при решении уравнений.

Предложение 6.4. *Если функция $y = f(x)$ возрастает в своей области определения и $E(f) \subseteq D(f)$, то уравнения*

$$f(f(x)) = x \quad \text{и} \quad f(x) = x$$

равносильны.

Доказательство. Пусть $f(x_0) = x_0$. Тогда

$$f(f(x_0)) = f(x_0) = x_0,$$

стало быть, уравнение $f(f(x)) = x$ является следствием уравнения $f(x) = x$.

Допустим теперь, что $f(f(x_0)) = x_0$, но $f(x_0) \neq x_0$. Если $f(x_0) < x_0$, то в силу возрастания функции f имеем

$$f(f(x_0)) < f(x_0) < x_0.$$

Поэтому $f(f(x_0)) < x_0$, что противоречит равенству $f(f(x_0)) = x_0$. Если же $f(x_0) > x_0$, то аналогично получается неравенство $f(f(x_0)) > x_0$, противоречащее условию.

4. Для каждого значения параметра $a \leqslant 0$ решить уравнение

$$x^2 - a = \sqrt{x + a}.$$

□ Пусть $t = \sqrt{x + a}$. Тогда $t \geqslant 0$ и $x = t^2 - a$. Таким образом, t удовлетворяет системе

$$\begin{cases} (t^2 - a)^2 - a = t, \\ t \geqslant 0. \end{cases} \tag{8}$$

Пусть $f(t) = t^2 - a, t \geqslant 0$. Понятно, что на луче $[0; +\infty)$ функция $y = f(t)$ возрастает. Кроме того, $D(f) = [0; +\infty)$, $E(f) = [-a; +\infty)$. Ясно, что при отрицательном a включение $E(f) \subseteq D(f)$ выполнено. Используя предложение 6.4, получаем систему

$$\begin{cases} t^2 - a = t, \\ t \geqslant 0. \end{cases}$$

Квадратное уравнение $t^2 - t - a = 0$ имеет решения, если его дискриминант $D = 1 + 4a$ неотрицателен, откуда $a \geqslant -1/4$. Пусть

t_1, t_2 – корни этого уравнения, причем $t_1 \leqslant t_2$. По формулам Виета имеем

$$\begin{cases} t_1 + t_2 = 1, \\ t_1 t_2 = -a. \end{cases}$$

Поскольку $-a \geqslant 0$, мы видим, что сумма корней t_1, t_2 положительна, а их произведение неотрицательно. Отсюда следует, что при $a \in [-1/4; 0]$ корни t_1, t_2 неотрицательны. Следовательно, если $-1/4 \leqslant a \leqslant 0$, то $t = (1 \pm \sqrt{1+4a})/2$. Возвращаясь к x, получаем $x = t^2 - a$, $t = (1 \pm \sqrt{1+4a})/2$.

Заметим, что попытка применить тот же способ для случая $a > 0$ приведет к неверному решению. Это связано с тем, что при $a > 0$ для функции $f(t) = t^2 - a, t \geqslant 0$ включение $E(f) \subseteq$ $\subseteq D(f)$ не выполняется. Покажем, как можно решить систему (8) для $a > 0$. Записывая уравнение этой системы в виде

$$a^2 - (2a+1)t + t^4 - t = 0$$

и решая это уравнение относительно a, получим $a = t^2 - t$ или $a =$ $= t^2 + t + 1$. Следовательно, система (8) равносильна совокупности

$$\begin{cases} t^2 - t - a = 0, \\ t \geqslant 0 \end{cases}, \qquad \begin{cases} t^2 + t + 1 - a = 0, \\ t \geqslant 0. \end{cases}$$

Проводя рассуждения, аналогичные приведенным выше, получим, что первая система имеет решение $t = (1 + \sqrt{1+4a})/2$ при любом положительном a; решением второй системы является число $t = (-1 + \sqrt{4a-3})/2$ при $a \geqslant 1$.

Окончательно имеем: если $a \geqslant 1$, то $x = (1 + \sqrt{1+4a})/2$, $x =$ $= (-1 - \sqrt{4a-3})/2$; если $0 < a < 1$, то $x = (1 + \sqrt{1+4a})/2$. $\square$

6.5. Выпуклость функции на промежутке

В этом разделе мы познакомимся еще с одним свойством, которым могут обладать числовые функции. Обратимся к рис. 4. На нем изображены графики двух функций $y = f_1(x)$, $y = f_2(x)$, имеющих в качестве области определения отрезок $[a; b]$.

Обе функции, как нетрудно видеть, являются возрастающими на $[a; b]$. Тем не менее понятно, что поведение этих функций на отрезке $[a; b]$ различно. Попробуем сформулировать, в чем состоит

эта разница. Пусть A_1 и A_2 – две произвольные точки на графике функции $y = f_1(x)$, x_1, x_2 – абсциссы этих точек. Нетрудно видеть, что на интервале $(x_1; x_2)$ график функции лежит ниже хорды A_1A_2. Если график функции обладает указанным свойством, то говорят, что функция *выпукла вниз* (на данном отрезке). Аналогично, если на каждом интервале $(x_1; x_2)$ график функции лежит выше хорды A_1A_2 функцию называют *выпуклой вверх*.

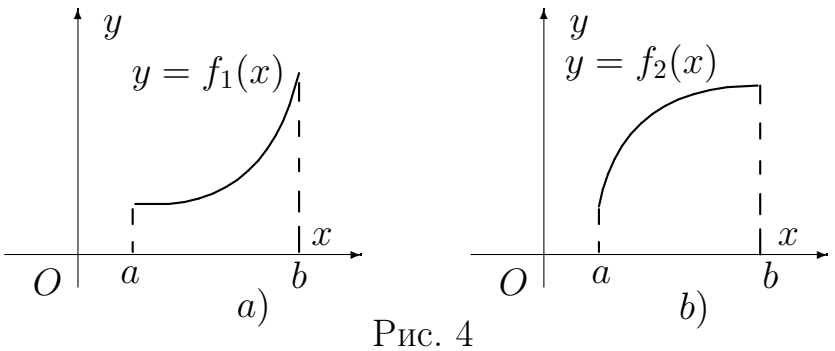

Рис. 4

Дадим теперь алгебраическое определение функции, выпуклой вниз на данном промежутке E. Нам понадобятся два вспомогательных утверждения.

Лемма 1. *Пусть числа x_1, x_2 различны. Число x лежит на интервале с концами x_1, x_2 тогда и только тогда, когда $x = \lambda_1 x_1 + \lambda_2 x_2$, где $\lambda_1, \lambda_2 > 0$ и $\lambda_1 + \lambda_2 = 1$.*

Доказательство. Заметим, что x лежит на указанном интервале тогда и только тогда, когда

$$(x_2 - x)(x - x_1) > 0. \tag{9}$$

Пусть $x = \lambda_1 x_1 + \lambda_2 x_2$, причем $\lambda_1, \lambda_2 > 0$ и $\lambda_1 + \lambda_2 = 1$. Тогда

$$x_2 - x = (1 - \lambda_2)x_2 - \lambda_1 x_1 = \lambda_1(x_2 - x_1),$$

$$x - x_1 = (\lambda_1 - 1)x_1 + \lambda_2 x_2 = \lambda_2(x_2 - x_1).$$

Из этих равенств сразу следует, что

$$(x_2 - x)(x - x_1) = \lambda_1\lambda_2(x_2 - x_1)^2 > 0.$$

Стало быть, выполнено неравенство (9).

Обратно, пусть выполнено неравенство (9). Введем обозначения

$$\lambda_1 = \frac{x_2 - x}{x_2 - x_1}, \qquad \lambda_2 = \frac{x - x_1}{x_2 - x_1}. \tag{10}$$

Легко видеть, что

$$\lambda_1 + \lambda_2 = \frac{x_2 - x}{x_2 - x_1} + \frac{x - x_1}{x_2 - x_1} = 1.$$

Из равенств (10) можно двумя способами выразить x:

$$x = x_1 + \lambda_2(x_2 - x_1), \qquad x = x_2 - \lambda_1(x_2 - x_1). \tag{11}$$

Умножая первое из равенств (11) на λ_1, а второе – на λ_2, и учитывая, что $\lambda_1 + \lambda_2 = 1$, получаем

$$x = \lambda_1 x + \lambda_2 x = \lambda_1 x_1 + \lambda_2 x_1 + \lambda_1\lambda_2(x_2 - x_1) - \lambda_1\lambda_2(x_2 - x_1). \tag{12}$$

Стало быть,

$$x = \lambda_1 x_1 + \lambda_2 x_1.$$

Осталось проверить, что λ_1, λ_2 положительны. С учетом равенства $\lambda_1 + \lambda_2 = 1$ достаточно убедиться, что $\lambda_1\lambda_2 > 0$. Последнее неравенство с очевидностью вытекает из равенств (10) и неравенства (9).

Лемма 2. *Пусть $A_1(x_1, y_1)$, $A_2(x_2, y_2)$ – точки координатной плоскости с различными абсциссами, $x = \lambda_1 x_1 + \lambda_2 x_2$, $y = \lambda_1 y_1 + \lambda_2 y_2$, где $\lambda_1 + \lambda_2 = 1$, $\lambda_1, \lambda_2 > 0$. Тогда точка $A(x, y)$ лежит на отрезке $[A_1A_2]$.*

Доказательство. Достаточно проверить, что для векторов $\overrightarrow{A_1A} = (x - x_1; y - y_1)$ и $\overrightarrow{A_1A_2} = (x_2 - x_1; y_2 - y_1)$ выполнено равенство $\overrightarrow{A_1A} = k\overrightarrow{A_1A_2}$, где $0 < k < 1$. Поскольку

$$x - x_1 = \lambda_2(x_2 - x_1), \qquad y - y_1 = \lambda_2(y_2 - y_1),$$

имеем

$$\overrightarrow{A_1A} = (x - x_1; y - y_1) = \lambda_2(x_2 - x_1; y_2 - y_1) = \lambda_2\overrightarrow{A_1A_2}.$$

По условию $0 < \lambda_2 < 1$. Положив $k = \lambda_2$, получим требуемое равенство.

Теперь дадим определение функции, выпуклой вниз на промежутке.

Определение. Функция $y = f(x), x \in X$ называется выпуклой вниз на промежутке $E \subseteq X$, если для любых различных $x_1, x_2 \in E$ и любых чисел $\lambda_1, \lambda_2 > 0$ таких, что $\lambda_1 + \lambda_2 = 1$, выполнено неравенство

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) > f(\lambda_1 x_1 + \lambda_2 x_2). \tag{13}$$

Функция, выпуклая вверх на промежутке E, определяется аналогично, только неравенство (13) должно быть заменено противоположным.

При исследовании функций на выпуклость, как правило, применяются средства математичекого анализа. Однако в некоторых случаях такое исследование может быть проведено и элементарными средствами.

В качестве примера рассмотрим степенную функцию $y = x^r$, где r – произвольное рациональное число.

Теорема 6.2. *Если $r > 1$ или $r < 0$, то степенная функция выпукла вниз на луче $(0; +\infty)$; если $0 < r < 1$, то на том же луче степенная функция выпукла вверх.*

Доказательство. Пусть $r > 1$. Нужно убедиться в справедливости неравенства

$$\lambda_1 x_1^r + \lambda_2 x_2^r > (\lambda_1 x_1 + \lambda_2 x_2)^r, \tag{14}$$

где x_1, x_2 положительны и различны, а λ_1, λ_2 также положительны и $\lambda_1 + \lambda_2 = 1$. Пусть

$$t_1 = \frac{x_1}{\lambda_1 x_1 + \lambda_2 x_2}, \quad t_2 = \frac{x_2}{\lambda_1 x_1 + \lambda_2 x_2}.$$

Легко видеть, что

$$\lambda_1 t_1 + \lambda_2 t_2 = 1. \tag{15}$$

Поскольку выражение $(\lambda_1 x_1 + \lambda_2 x_2)^r$ определено и положительно, вместо неравенства (14) достаточно проверить неравенство

$$\lambda_1 t_1^r + \lambda_2 t_2^r > 1. \tag{16}$$

Для доказательства неравенства (14) воспользуемся неравенством Бернулли. Так как $t_1 > 0$ и $r > 1$, имеем

$$t_1^r = (1 + (t_1 - 1))^r \geqslant 1 + r(t_1 - 1) = 1 - r + rt_1.$$

Стало быть,

$$t_1^r \geqslant 1 - r + rt_1. \tag{17}$$

Аналогично

$$t_2^r \geqslant 1 - r + rt_2. \tag{18}$$

Теперь заметим, что $t_1 \neq t_2$. Поэтому одно из чисел t_1, t_2 отлично от 1; значит, одно из неравенств (17), (18) является строгим. Умножая неравенства (17), (18) на положительные числа λ_1, λ_2 соответственно, получим

$$\lambda_1 t_1^r + \lambda_2 t_2^r > \lambda_1(1 - r) + \lambda_2(1 - r) + \lambda_1 rt_1 + \lambda_2 rt_2 = 1 - r + r = 1,$$

что и требовалось доказать.

Случаи, когда $r < 0$ или $0 < r < 1$ могут быть рассмотрены совершенно аналогично.

Заметим, что при положительном r функция $y = x^r$ определена на замкнутом луче $[0; +\infty)$. Легко проверить, что на этом луче она выпукла вниз (выпукла вверх), если $r > 1$ (соответственно $0 < r < 1$).

В заключение этого раздела отметим одно полезное свойство функций, выпуклых вниз на данном промежутке. Разумеется, выпуклые вверх функции обладают аналогичным свойством.

Теорема 6.3. *Пусть функция $y = f(x)$ выпукла вниз на промежутке X. Если $\lambda_1, \lambda_2, \ldots, \lambda_n$ – такие положительные числа, что*

$$\lambda_1 + \lambda_2 + \ldots + \lambda_n = 1,$$

а $x_1, x_2, \ldots, x_n$ – числа из промежутка X, среди которых хотя бы два различны, то выполнено неравенство

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) + \ldots + \lambda_n f(x_n) > f(\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n). \tag{19}$$

Доказательство. Применим метод математической индукции.

Если $n = 2$, то требуемое неравенство совпадает с неравенством (13) из определения выпуклой вниз функции.

Пусть при $n = k \geqslant 2$ теорема выполняется. Проверим, что она верна и при $n = k+1$. Пусть $\lambda_1, \lambda_2, \ldots, \lambda_k, \lambda_{k+1}$ и $x_1, x_2, \ldots, x_k, x_{k+1}$ удовлетворяют условиям, сформулированным в теореме. В частности, среди чисел $x_1, x_2, \ldots, x_k, x_{k+1}$ имеется хотя бы два различных. Без ограничения общности можно считать, что x_1 – наименьшее из чисел $x_1, x_2, \ldots, x_k, x_{k+1}$. Положим

$$\mu = \lambda_2 + \ldots + \lambda_{k+1}, \quad y = \frac{\lambda_2}{\mu} x_2 + \ldots + \frac{\lambda_{k+1}}{\mu} x_{k+1}.$$

Легко убедиться в том, что $x_1 \neq y$. В самом деле,

$$\mu(x_1 - y) = \lambda_2(x_1 - x_2) + \ldots + \lambda_{k+1}(x_1 - x_{k+1}) < 0.$$

Последнее неравенство следует из того, что λ_i $(2 \leqslant i \leqslant k+1)$ положительны, а разности $x_1 - x_i$ $(2 \leqslant i \leqslant k+1)$ неположительны, причем хотя бы одна из этих разностей отрицательна. Кроме того,

$$\frac{\lambda_2}{\mu} + \ldots + \frac{\lambda_{k+1}}{\mu} = 1.$$

Отсюда следует, в частности, что y принадлежит промежутку X. Стало быть,

$$f(\lambda_1 x_1 + \mu y) > \lambda_1 f(x_1) + \mu f(y).$$

Используя предположение индукции, имеем

$$\mu f(y) = \mu f\left(\frac{\lambda_2}{\mu} x_2 + \ldots + \frac{\lambda_{k+1}}{\mu} x_{k+1}\right) > \lambda_2 f(x_2) + \ldots + \lambda_{k+1} f(x_{k+1}).$$

Из последних двух неравенств легко получается неравенство (19) при $n = k + 1$.

Неравенство (19) часто называют неравенством Иенсена[1].

Выведем из неравенства Иенсена известное нам неравенство между средним степенным порядка $\alpha > 1$ и средним арифметическим. Пусть $x_1, \ldots, x_n$ – произвольные положительные числа,

[1] И.Л.Иенсен (1859–1925) – датский математик.

$\lambda_1 = \ldots = \lambda_n = 1/n$. Поскольку при $\alpha > 1$ степенная функция $y = x^\alpha$ выпукла вниз на луче $[0; +\infty)$, в силу неравенства Иенсена имеем

$$\frac{x_1^\alpha + \ldots + x_n^\alpha}{n} > \left(\frac{x_1 + \ldots + x_n}{n}\right)^\alpha.$$

Возводя обе части последнего неравенства в положительную степень $1/\alpha$, получим требуемое неравенство.

6.6. Функция, обратная к данной

При изучении отображений произвольных множеств мы убедились, что для каждого биективного отображения существует обратное отображение. В случае, когда рассматриваются числовые функции, будет определена функция, являющаяся обратной к произвольной инъективной функции.

Пусть $y = f(x), x \in X$ – инъективная функция, Y – ее множество значений. Из предложения 5.4 следует, что существует такая функция $x = g(y), y \in Y$, что

$$x = g(y) \Longleftrightarrow y = f(x).$$

Функцию g мы и будем называть обратной к данной числовой функции f.

Таким образом, применительно к числовым функциям мы расширили класс функций, имеющих обратные. В дальнейшем инъективную числовую функцию мы будем называть обратимой.

Если функция $x = g(y)$ является обратной к функции $y = f(x)$, $x \in X$, то выполнены следующие свойства:

1. Область определения функции g совпадает с множеством значений Y функции f;

2. Множество значений функции g совпадает с областью определения функции f;

3. $g(f(x)) = x$ для любого $x \in X$;

4. $f(g(y)) = y$ для любого $y \in Y$.

Для того чтобы доказать, что данная числовая функция $y = f(x)$, $x \in X$ является обратимой, достаточно убедиться в том, что для каждого y из множества значений Y функции f уравнение $f(x) = y$ имеет единственное решение на множестве X. Если при

этом удается выразить x через y, то тем самым получается правило, определяющее обратную функцию. Рассмотрим несколько примеров на нахождение функции, обратной к данной. В каждом из примеров требуется убедиться в том, что данная функция обратима, и найти обратную к ней функцию.

1. $y = 2x - 6, x \in [1; 4]$.

□ Нетрудно понять, что уравнение $2x - 6 = y$ всегда имеет единственное решение

$$x = y/2 + 3. \tag{20}$$

Стало быть, данная функция обратима. Правило, определяющее обратную к данной функцию, задано равенством (20). Найдем область определения обратной функции. Решая двойное неравенство

$$1 \leqslant \frac{y}{2} + 3 \leqslant 4,$$

получим $-4 \leqslant y \leqslant 2$. Значит, функция, обратная к заданной, имеет вид $x = y/2 + 3, y \in [-4; 2]$. □

2. $y = x^2 - 2x + 3, x \in (-\infty; 1]$.

□ Найдем сначала множество значений Y данной функции. Мы знаем, что $y \in Y$ тогда и только тогда, когда уравнение

$$x^2 - 2x + 3 - y = 0 \tag{21}$$

имееет хотя бы одно решение. Для этого достаточно, чтобы его дискриминант $D = 4(y - 2)$ был неотрицателен. Стало быть, $Y = [2; +\infty)$. Покажем теперь, что для каждого $y \geqslant 2$ уравнение (21) имеет единственное решение. Пусть x_1, x_2 – корни этого уравнения, причем $x_1 \leqslant x_2$. Тогда

$$(x_1 - 1)(x_2 - 1) = x_1x_2 - (x_1 + x_2) + 1. \tag{22}$$

Из равенства (22) при помощи формул Виета $x_1 + x_2 = 2$, $x_1x_2 = 3 - y$ получаем

$$(x_1 - 1)(x_2 - 1) = 2 - y. \tag{23}$$

Пусть y принадлежит множеству значений исходной функции, т. е. $y \geqslant 2$. Если $y > 2$, то $2 - y < 0$, а потому $x_1 - 1 < 0$, $x_2 - 1 > 0$. Это означает, что только x_1 лежит на луче $(-\infty; 1]$. Если же $y = 2$,

то уравнение (21) имеет совпадающие корни $x_1 = x_2 = 1$. Таким образом, если $y \geqslant 2$, то на луче $(-\infty; 1]$ лежит только меньший корень уравнения (21). Вычисляя этот корень, окончательно получаем

$$x = 1 - \sqrt{y-2}, y \in [2; +\infty). \qquad \square$$

Предложение 6.5. *Пусть $y = f(x)$, $x \in X$, – функция, Y – ее множество значений. Если f возрастает (убывает) на множестве X, то*

1) f – обратима;

2) обратная к f функция g является возрастающей (убывающей) на множестве Y.

Доказательство. Допустим, что f – возрастающая на X функция.

1. Если $x_1, x_2 \in X$ и $x_1 \neq x_2$, то либо $x_1 < x_2$, либо $x_2 < x_1$. В первом случае $f(x_1) < f(x_2)$, во втором $f(x_2) < f(x_1)$. Таким образом, $f(x_1) \neq f(x_2)$.

2. Пусть $g : Y \to X$ – функция, обратная к f. Предположим, что существуют $y_1, y_2 \in Y$ такие, что $y_1 < y_2$, но $g(y_1) \geqslant g(y_2)$. Тогда $f(g(y_1)) \geqslant f(g(y_2))$, откуда $y_1 \geqslant y_2$.

Очевидно, что случай, когда f убывает на множестве X, рассматривается аналогично.

6.7. График числовой функции

Определение. График числовой функции $y = f(x)$, $x \in \in X$, – это множество всех точек координатной плоскости вида $(x, f(x))$, $x \in X$.

График является очень наглядным способом представления функции. Поэтому важно научиться строить графики функций, изучаемых в школьном курсе математики. В разд. 6.8 мы рассмотрим приемы построения графиков, основанные на их преобразованиях. А пока займемся графиками следующих функций:

(a) линейной функции $y = ax + b$;

(b) функции $y = ax^2$, $a \neq 0$;

(c) функции $y = k/x$, $k \neq 0$.

Если спросить, что представляет собой график функции в каждом из случаев (a) – (c), то каждый ответит, что в случае (a) графиком является прямая, а в случаях (b), (c) – парабола и гипербола соответственно. Казалось бы, эти факты не нуждаются в пояснениях. Однако призадумаемся: откуда все-таки следует, что график линейной функции – прямая. Понятие прямой возникает в курсе геометрии. Причем определение этого понятия не дается; все, что мы знаем о прямой – это некоторые ее свойства, описываемые аксиомами. Линейная функция задается алгебраическим выражением специального вида. Почему же между этими внешне различными понятиями существует связь? В случаях (b) и (c) ситуация еще хуже: мы пока даже не можем ответить на вопрос – а что такое парабола или гипербола? Данный раздел посвящен ответу на поставленные вопросы.

Теорема 6.4. *Графиком линейной функции $y = ax+b$ является прямая, не параллельная оси ординат. Обратно, всякая прямая, не параллельная оси ординат, является графиком некоторой линейной функции.*

Доказательство. Пусть дана линейная функция $y = ax+b$ и пусть G – ее график (рис. 5). По определению

$$G = \{(x; ax + b) | x \in \mathbb{R}\}.$$

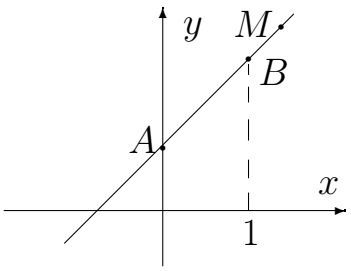

Рис. 5

Рассмотрим точки $A(0; b)$, $B(1, a + b)$. Эти точки, очевидно, принадлежат графику G. Убедимся, что график G и прямая (AB) совпадают. Пусть $M(x; y)$ – произвольная точка. Тогда $\overrightarrow{AM} = (x; y - b)$, $\overrightarrow{AB} = (1; a)$. Понятно, что точка M принадлежит прямой (AB) в том и только том случае, когда векторы $\overrightarrow{AM}$ и $\overrightarrow{AB}$ коллинеарны. Поскольку

$$M \in G \Longleftrightarrow y = ax + b \Longleftrightarrow y - b = ax \Longleftrightarrow \overrightarrow{AM} = x\overrightarrow{AB} \Longleftrightarrow$$
$$\Longleftrightarrow \overrightarrow{AM} \parallel \overrightarrow{AB} \Longleftrightarrow M \in (AB),$$

имеем

$$M \in G \Longleftrightarrow M \in (AB).$$

Отсюда следует совпадение графика G и прямой (AB).

Обратно, пусть l – произвольная прямая, не параллельная оси ординат. Рассмотрим на прямой l точки A, B с абсциссами 0 и 1 соответственно. Обозначим через b и c ординаты этих точек; тогда $A(0;b)$, $B(1;c)$. Пусть $a=c-b$. Ясно, что точки A, B принадлежат графику функции $y=ax+b$. Выше уже было проверено, что в таком случае график линейной функции и прямая $(AB)=l$ совпадают.

Перейдем к изучению графика функции $y=ax^2$, $a\neq 0$. Дадим сначала определение параболы.

О п р е д е л е н и е. Пусть d – произвольная прямая, F – точка, не принадлежащая прямой d. Множество всех таких точек M, что расстояние между точками M и F равно расстоянию от точки M до прямой d называется *параболой*.

Точка F называется фокусом параболы, прямая d – ее директрисой.

Выберем на плоскости систему координат следующим образом. Из точки F опустим перпендикуляр (FD) на прямую d. Совместим начало O системы координат с серединой отрезка $[FD]$. Ось абсцисс проведем параллельно директрисе d; направление на оси Ox можно выбрать произвольно. Ось ординат совместим с прямой (FD), причем будем считать, что положительное направление задается лучом $[DF)$. Длину отрезка $[FD]$ обозначим через $2p$. Тогда $F(0;p)$, а прямая d имеет уравнение $y=-p$.

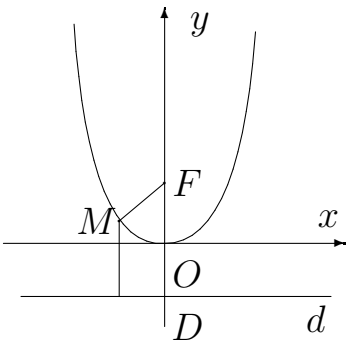

Рис. 6

Пусть $M(x;y)$ – произвольная точка плоскости. Мы знаем, что

$$|MF|=\sqrt{x^2+(y-p)^2}.$$

Кроме того, расстояние от точки M до прямой d равно $|y+p|$. Учитывая определение параболы, мы видим, что точка $M(x;y)$ принадлежит параболе с фокусом F и директрисой d тогда и только

тогда, когда ее координаты удовлетворяют уравнению

$$|y+p| = \sqrt{x^2+(y-p)^2}. \tag{24}$$

Поскольку обе части уравнения (24) неотрицательны, после возведения обеих его частей в квадрат, получим равносильное уравнение

$$y^2+2py+p^2 = x^2+y^2-2py+p^2,$$

или, после очевидных упрощений,

$$y = \frac{x^2}{4p}. \tag{25}$$

Итак, выбрав специальным образом систему координат, мы убедились, что точка $M(x,y)$ принадлежит параболе тогда и только тогда, когда ее координаты удовлетворяют уравнению (25). Иными словами, уравнение (25) является уравнением параболы. Отсюда немедленно вытекает

Теорема 6.5. *Графиком функции* $y = ax^2$ $(a \neq 0)$ *является парабола.*

Доказательство. Пусть $G = \{(x; ax^2) | x \in \mathbb{R}\}$ – график данной функции. Поскольку при отрицательном a график G получается из графика функции $y = |a|x^2$ симметрией относительно оси абсцисс, можно считать, что $a > 0$. Рассмотрим число $p = 1/(4a)$ и введем в рассмотрение точку $F(0;p)$ и прямую d, заданную уравнением $y = -p$. Обозначим через P параболу с фокусом F и директрисой d. Из приведенных выше вычислений следует, что если $M \in P$, то $M \in G$. Таким образом, $P \subseteq G$. Проверим обратное включение. Предположим, что $M(x;y) \in G$. Тогда $y = ax^2$, откуда в силу выбора p имеем $x^2 = 4py$. С учетом последнего равенства имеем

$$\sqrt{x^2+(y-p)^2} = \sqrt{4py+y^2-2py+p^2} = |y+p|.$$

Отсюда следует, что любая точка графика G принадлежит параболе P, т. е. $G \subseteq P$.

Обратимся к изучению графика функции $y = k/x$ $(k \neq 0)$.

Начнем с определения гиперболы.

О п р е д е л е н и е. Пусть F_1, F_2 – различные точки. *Гиперболой* называется множество всех таких точек M, что модуль разности расстояний $|MF_1|$ и $|MF_2|$ есть постоянная величина (рис. 7).

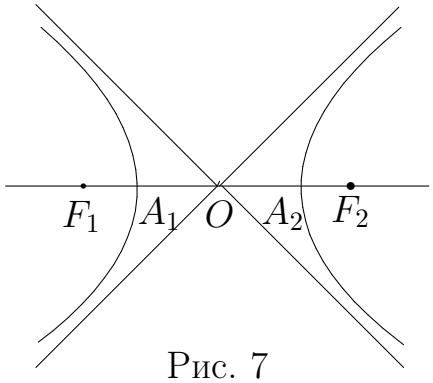

Рис. 7

Точки F_1, F_2 называются *фокусами* гиперболы. Прямую (F_1F_2) называют *осью* гиперболы. Из определения вытекает, что гипербола симметрична относительно оси. Нетрудно понять, что на оси существуют две точки A_1, A_2, принадлежащие гиперболе. Форма гиперболы определяется отношением $|F_1F_2| : |A_1A_2|$, называемым *эксцентриситетом* гиперболы. Для произвольной точки M числа $r_1 = |MF_1|$ и $r_2 = |MF_2|$ называют ее фокальными радиусами.

Пусть $|A_1A_2| = 2a$. Из определения вытекает, что точка M принадлежит данной гиперболе тогда и только тогда, когда ее фокальные радиусы удовлетворяют равенству

$$|r_1 - r_2| = 2a. \tag{26}$$

На координатной плоскости рассмотрим гиперболу, заданную равенством (26) и имеющую фокусы $F_1(-a;-a)$, $F_2(a;a)$ (рис. 8). Пусть $M(x;y)$ – произвольная точка гиперболы. Выражая фокальные радиусы r_1, r_2 этой точки через ее координаты, находим

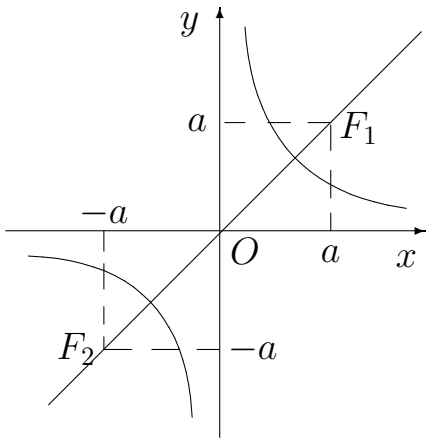

Рис. 8

$$r_1^2 = (x+a)^2 + (y+a)^2, \tag{27}$$

$$r_2^2 = (x-a)^2 + (y-a)^2. \tag{28}$$

Вычитая из равенства (27) равенство (28), получим

$$r_1^2 - r_2^2 = 4a(x+y). \tag{29}$$

Из равенств (26), (29) вытекает, что фокальные радиусы точки $M(x;y)$, лежащей на гиперболе, удовлетворяют системе

$$\begin{cases} |r_1 - r_2| = 2a, \\ r_1^2 - r_2^2 = 4a(x+y). \end{cases} \tag{30}$$

Система (30) равносильна совокупности

$$\begin{cases} r_1 - r_2 = 2a, \\ r_1 + r_2 = 2(x+y), \end{cases} \qquad \begin{cases} r_1 - r_2 = -2a, \\ r_1 + r_2 = -2(x+y). \end{cases} \tag{31}$$

Из первой системы совокупности (31) находим $r_1 = a + x + y$, а из второй системы имеем $r_1 = -(a + x + y)$. Таким образом, $r_1 = |a + x + y|$. С учетом равенства (27) получаем

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

Раскрывая скобки и приводя подобные члены, приходим к уравнению

$$xy = \frac{a^2}{2}. \tag{32}$$

Мы проверили, что координаты точки $M(x;y)$, лежащей на данной гиперболе, удовлетворяют уравнению (32).

Теорема 6.6. *Графиком функции $y = k/x$ $(k \neq 0)$ является гипербола.*

Доказательство. Пусть $G = \{(x; k/x) | x \in \mathbb{R}, x \neq 0\}$ – график данной функции. Предположим сначала, что $k > 0$. Полагая $a = \sqrt{2k}$, рассмотрим точки $F_1(-a;-a)$, $F_2(a;a)$. Обозначим через H гиперболу с фокусами F_1, F_2 и такую, что фокальные радиусы произвольной ее точки удовлетворяют условию (26). Из приведенных выше вычислений следует, что если $M \in H$, то $M \in G$. Таким образом, $H \subseteq G$.

Проверим обратное включение. Предположим, что $M(x;y) \in \in G$. Тогда $y = k/x$, откуда $xy = k$ и, значит, $2xy = a^2$. Поэтому

$$\begin{aligned} r_1^2 &= (x+a)^2 + (y+a)^2 = x^2 + 2ax + a^2 + y^2 + 2ay + a^2 = \\ &= x^2 + 2ax + a^2 + y^2 + 2ay + 2xy = (x + y + a)^2. \end{aligned}$$

Аналогично

$$r_2^2 = (x + y - a)^2.$$

Отсюда

$$r_1 = |x + y + a|, \qquad r_2 = |x + y - a|. \tag{33}$$

Заметим теперь, что в силу равенства $2xy = a^2$ числа x, y либо оба положительны, либо оба отрицательны. Если $x, y > 0$, то $x + {} + y + a > 0$. Кроме того,

$$x + y \geqslant 2\sqrt{xy} = a\sqrt{2} > a,$$

откуда $x + y - a > 0$. Стало быть, $r_1 = x + y + a$, $r_2 = x + y - a$, и потому $r_1 - r_2 = 2a$. Пусть $x, y < 0$. Тогда $-x, -y > 0$, и, значит,

$$(-x) + (-y) \geqslant 2\sqrt{(-x)(-y)} = 2\sqrt{xy} = a\sqrt{2} > a.$$

Отсюда $x + y + a < 0$. Ясно, что $x + y - a < 0$. Поэтому $r_1 = {} = -(x+y+a)$, $r_2 = a-x-y$ и $r_2 - r_1 = 2a$. Итак, в обоих случаях $|r_1 - r_2| = 2a$, и включение $G \subseteq H$ доказано.

Случай, когда $k < 0$ рассматривается аналогично предыдущему, если положить $a = \sqrt{-2k}$, а в качестве фокусов взять точки $F_1(a; -a)$ и $F_2(-a; a)$.

6.8. Преобразования графиков

Иногда построение графиков функций облегчают следующие соображения. Пусть построен график G функции $y = f(x), x \in X$. Тогда графики функций $y = f(-x)$, $y = f(x + a)$, $y = -f(x)$, $y = f(x)+A$ могут быть получены из графика G при помощи движений координатной плоскости – симметрий и сдвигов. А именно, справедливо следующее утверждение.

Предложение 6.6. *Пусть $y = f(x)$, $x \in X$, – произвольная числовая функция, G_f – ее график. Тогда*

1. *График функции $y = f(-x)$, $-x \in X$, получается из G_f симметрией относительно оси Oy;*

2. *График функции $y = f(x+a)$, $x+a \in X$, получается из G_f сдвигом на вектор $(-a, 0)$;*

3. *График функции $y = -f(x)$, $x \in X$, получается из G_f симметрией относительно оси Ox;*

4. *График функции $y = f(x) + A$, $x \in X$, получается из G_f сдвигом на вектор $(0, A)$.*

Доказательство.

1. Пусть $h(x) = f(-x)$, G_h – график функции h. Имеем цепочку равносильных утверждений:

$$(x, y) \in G_h \Leftrightarrow y = h(x) \Leftrightarrow y = f(-x) \Leftrightarrow (-x, y) \in G_f.$$

Таким образом,

$$(x, y) \in G_h \Leftrightarrow (-x, y) \in G_f.$$

Поскольку точки (x, y), $(-x, y)$ симметричны относительно оси Oy, фигуры G_h и G_f также симметричны относительно Oy.

2. Пусть $h(x) = f(x + a)$. Тогда

$$(x, y) \in G_h \Leftrightarrow y = h(x) \Leftrightarrow y = f(x + a) \Leftrightarrow (x + a, y) \in G_f.$$

Следовательно,

$$(x, y) \in G_h \Leftrightarrow (x + a, y) \in G_f.$$

Пусть $x' = x + a$, $x = x' - a$, откуда получаем

$$(x', y) \in G_f \Leftrightarrow (x' - a, y) \in G_h.$$

Так как точка $(x' - a, y)$ получается из точки (x', y) сдвигом на вектор $(-a, 0)$, то же самое справедливо и для множеств точек G_f и G_h.

Проверка пунктов 3, 4 проводится аналогично и предоставляется читателю.

В дополнение к предложению 6.6 сформулируем

Предложение 6.7. *Пусть $y = f(x)$, $x \in X$, – произвольная числовая функция, G – ее график. Тогда*

1. *График функции $y = f(|x|)$, $|x| \in X$, является объединением двух множеств G_1 и G_2, где G_1 – это часть G_1, расположенная справа от оси ординат, а G_2 симметрично G_1 относительно оси Oy;*

2. *График функции $y = |f(x)|$, $x \in X$, является объединением двух множеств G_3 и G_4, где G_3 – это часть G_f, расположенная выше оси абсцисс, а G_4 симметрично относительно Ox множеству точек графика G_f, лежащих ниже оси Ox.*

Доказательство.

1. Снимая модуль в выражении $f(|x|)$, получим

$$y = f(|x|) \Leftrightarrow \begin{cases} x \geqslant 0, \\ y = f(x), \end{cases} \quad \begin{cases} x < 0, \\ y = f(-x). \end{cases}$$

Множество точек координатной плоскости, удовлетворяющих первой системе, есть G_1, второй системе – G_2.

2. Снимем модуль в выражении

$$y = |f(x)|.$$

Тогда

$$y = |f(x)| \Leftrightarrow \begin{cases} f(x) \geqslant 0, \\ y = f(x), \end{cases} \quad \begin{cases} f(x) < 0, \\ y = -f(x). \end{cases}$$

Множество точек координатной плоскости, удовлетворяющих первой системе, есть G_3, второй системе – G_4.

Применим предложения 6.6, 6.7 для построения графика функции $y = |||x| - 1| - 3|$.

□ Рассмотрим последовательность выражений:

$f_1(x) = |x|$, $f_2(x) = |x-3|$, $f_3(x) = ||x|-3|$, $f_4(x) = ||x-1|-3|$, $f_5(x) = |||x| - 1| - 3|$.

Ясно, что $y = f_5(x)$ – исходная функция; график функции $y = f_1(x)$ легко построить и график функции $y = f_{i+1}(x)$ получается из графика функции $y = f_i(x)$ при $i = 2, 4, 6$ по пункту 2 предложения 6.6, а при $i = 3, 5$ по пункту 1 предложения 6.7. Читателю рекомендуется самостоятельно построить графики функций $y = f_i(x)$ при $1 \leqslant i \leqslant 5$. График функции $y = |||x| - 1| - 3|$ показан на рис. 9. □

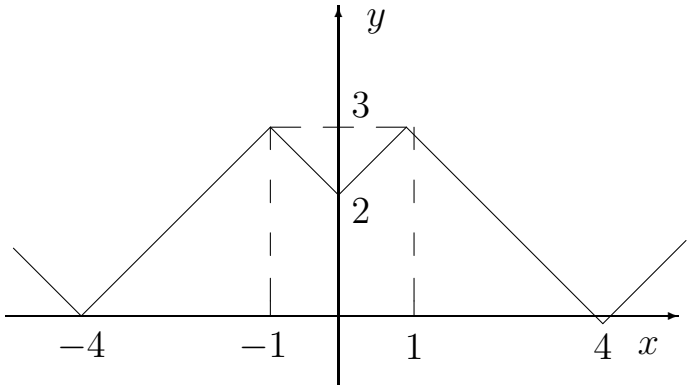

Рис. 9

6.9. Графики дробно-линейной и квадратичной функций

Дробно-линейная функция – это функция $y = \dfrac{ax+b}{cx+d}$, $c \neq$ $\neq 0$, $bc - ad \neq 0$. Функция $y = \dfrac{k}{x}$ (обратно пропорциональная зависимость) является, очевидно, дробно-линейной функцией; график этой функции – гипербола, лежащая в первом и третьем квадрантах при $k > 0$ и во втором и четвертом квадрантах при $k < 0$. Убедимся, что график произвольной дробно-линейной функции может быть получен из графика функции $y = \dfrac{k}{x}$ при помощи сдвигов вдоль осей координат. Для этого преобразуем выражение $y = \dfrac{ax+b}{cx+d}$. Пусть $B = \dfrac{d}{c}$ ($\neq 0$). Тогда $cx + d =$ $= c(x + B)$. Выделяя в числителе выражение $x + B$, получим $ax + b = a(x + B) + b - aB$. Отсюда

$$y = \frac{ax+b}{cx+d} = \frac{a(x+B)+b-aB}{c(x+B)} = \frac{a}{c} + \frac{b-aB}{c(x+B)}.$$

Вводя обозначения $A = \dfrac{a}{c}$, $k = \dfrac{b-aB}{c}$, окончательно получим

$$\frac{ax+b}{cx+d} = A + \frac{k}{x+B}.$$

Таким образом, дробно-линейная функция $y = \dfrac{ax+b}{cx+d}$ может быть записана в виде

$$y = A + \frac{k}{x+B}.$$

Заметим, что из неравенства $bc - ad \neq 0$ следует, что $k \neq 0$.

Из пунктов 2, 4 предложения 4 (см.ниже) вытекает, что график функции $y = \dfrac{ax+b}{cx+d}$ получается из графика функции $y = \dfrac{k}{x}$ сдвигом на вектор $(-B; 0)$, а затем – на вектор $(0; A)$.

Квадратичная функция – это функция $y = ax^2 + bx + c$, $a \neq 0$. График такой функции может быть получен из графика функции

$y = ax^2$ при помощи сдвигов вдоль осей координат. В самом деле, выделяя полный квадрат в выражении $ax^2 + bx + c$, получим

$$ax^2+bx+c = a\left(x^2+\frac{b}{a}x\right)+c = a\left(x^2+2\frac{b}{2a}x+\frac{b^2}{4a^2}\right)-\frac{b^2}{4a^2}+c =$$

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

Поскольку $D = b^2 - 4ac$ – дискриминант квадратного трехчлена, имеем

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

Таким образом, квадратичная функция $y = ax^2 + bx + c$ может быть записана в виде

$$y = a\left(x+\frac{b}{2a}\right)^2-\frac{D}{4a}.$$

Из такого представления видно, что график функции $y = ax^2 + bx + c$ получается из графика функции $y = ax^2$ при помощи сдвигов на векторы $\left(-\frac{b}{2a}; 0\right)$ и $\left(0; -\frac{D}{4a}\right)$.

Для примера построим графики функций $y = \frac{3x-2}{2x-4}$, $y = -x^2 + 4x - 3$.

Преобразуя выражения, определяющие данные функции, указанными выше способами, получим

$$\frac{3x-2}{2x-4} = \frac{3(x-2)+6-2}{2(x-2)} = \frac{3}{2}+\frac{2}{x-2}.$$

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

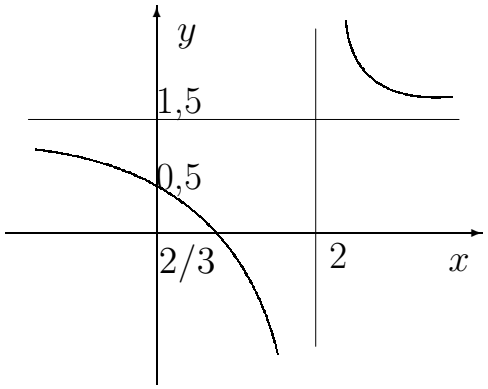

Рис. 10

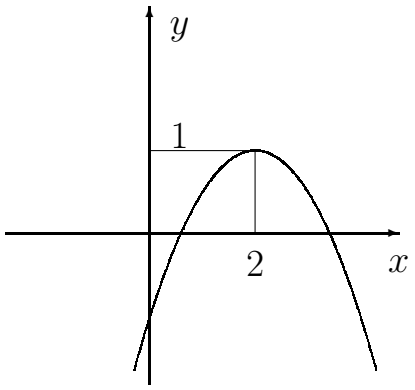

Рис. 11

Отсюда видно, что график функции $y = \dfrac{3x-2}{2x-4}$ получается из графика функции $y = \dfrac{2}{x}$ при помощи сдвигов на векторы $(2;0)$ и $(0;3/2)$ (рис. 10), а график функции $y = -x^2+4x-3$ может быть получен из графика функции $y = -x^2$ сдвигами на векторы $(2;0)$ и $(0;1)$ (рис. 11).

Рассмотрим несколько задач на построение графиков функций.

1. $y = \dfrac{x^3-3x^2-x+3}{|x-1|}$.

□ Естественная область определения этой функции – множество $(-\infty;1) \cup (1;+\infty)$. Учитывая, что $x^3-3x^2-x+3 = (x-1)(x^2-2x-3)$, и снимая модуль, получим

$$y = \begin{cases} -x^2+2x+3, & \text{если } x < 1, \\ x^2-2x-3, & \text{если } x \geqslant 1. \end{cases}$$

График этой функции представлен на рис. 12. □

2. $y = \dfrac{|x^2-3|x|+2|}{x^2-4}$.

□ Естественная область определения этой функции – множество $\mathbb{R} \setminus \{-2,2\}$. Нетрудно видеть, что данная функция является четной, поэтому достаточно построить ее график на луче $[0;+\infty)$, а затем сделать симметрию относительно оси ординат. Снимая мо-

дули на луче $[0;+\infty)$, получим

$$y=\begin{cases}\dfrac{x-1}{x+2}, & \text{если } x\in[0;1]\cup(2;+\infty),\\ -\dfrac{x-1}{x+2}, & \text{если } x\in(1;2).\end{cases}$$

Поскольку

$$\frac{x-1}{x+2}=1+\frac{-3}{x+2},$$

график функции $y=\dfrac{x-1}{x+2}$ может быть получен из графика функции $y=\dfrac{-3}{x}$ сдвигом на вектор $(-2;1)$. Аналогично, график функции $y=-\dfrac{x-1}{x+2}$ получается из графика функции $y=\dfrac{3}{x}$ сдвигом на вектор $(-2;-1)$.

График исходной функции показан на рис. 13.□

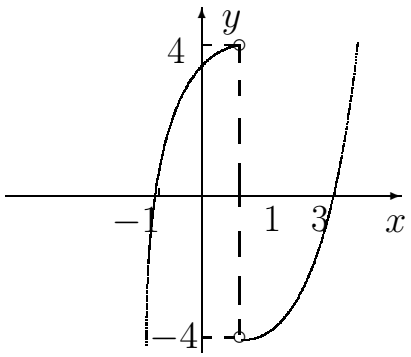

Рис. 12

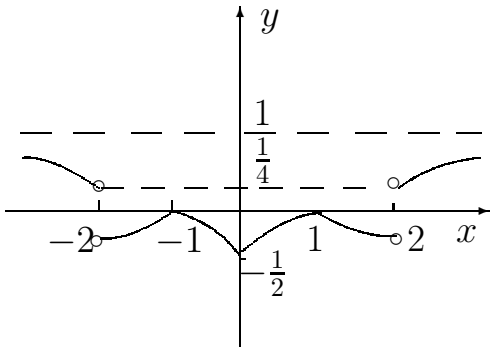

Рис. 13

6.10. Графики линейных уравнений и неравенств с двумя переменными

Пусть $F(x,y)$ – произвольное алгебраическое выражение, зависящее от переменных x, y. Графиком уравнения $F(x,y)=0$ называется множество

$$\{(x;y)|F(x,y)=0\}.$$

Аналогично определяются графики неравенств с двумя переменными.

В этом пункте рассматриваются графики линейных уравнений и неравенств с двумя переменными.

Теорема 6.7. *Графиком линейного уравнения* $ax + by + c = 0$ $(a^2 + b^2 \neq 0)$ *является прямая. Обратно, всякая прямая на координатной плоскости является графиком некоторого линейного уравнения с двумя переменными.*

Доказательство. Пусть G – график уравнения $ax + by + c = 0$ при условии $a^2 + b^2 \neq 0$. Если $b = 0$, то $a \neq 0$, и данное уравнение преобразуется к виду

$$x = -\frac{c}{a}.$$

Ясно, что множество G в этом случае является прямой, параллельной оси ординат. Пусть $b \neq 0$. Тогда G совпадает с графиком линейной функции

$$y = -\frac{a}{b}x - \frac{c}{b}$$

и потому является прямой.

Доказательство обратного утверждения мы оставляем читателю.

Пусть прямая l служит графиком линейного уравнения $ax + by + c = 0$ $(a^2 + b^2 \neq 0)$. С прямой l можно связать два вектора: нормальный вектор $\overrightarrow{n} = (a; b)$ и направляющий вектор $\overrightarrow{s} = (-b; a)$. Легко убедиться в том, что вектор $\overrightarrow{n}$ перпендикулярен прямой l. В самом деле, если $M_1(x_1; y_1)$, $M_2(x_2; y_2)$ – различные точки прямой l, то $ax_1 + by_1 + c = 0$ и $ax_2 + by_2 + c = 0$. Вычитая одно равенство из другого, получим

$$a(x_2 - x_1) + b(y_2 - y_1) = 0.$$

Отсюда видно, что скалярное произведение векторов $\overrightarrow{n}$ и $\overrightarrow{M_1M_2}$ равно нулю, т. е. эти векторы перпендикулярны.

Нетрудно видеть, что скалярное произведение векторов $\overrightarrow{n}$ и $\overrightarrow{s}$ также равно нулю. Стало быть, вектор $\overrightarrow{s}$ перпендикулярен вектору $\overrightarrow{n}$, и потому он параллелен прямой l.

Построение графиков линейных неравенств с двумя переменными основывается на следующем утверждении.

Теорема 6.8. *Прямая l, заданная уравнением $ax + by + c = 0$ $(a^2 + b^2 \neq 0)$, делит координатную плоскость на две полуплоскости так, что во всех точках одной полуплоскости выражение $ax+by+c$ принимает только положительные значения, а во всех точках другой полуплоскости – только отрицательные.*

Доказательство. Для произвольной точки $M(x; y)$, не лежащей на прямой l, обозначим через $M_0(x_0; y_0)$ основание перпендикуляра, опущенного из M на прямую l (рис. 13). Тогда вектор $\overrightarrow{M_0M}$ и нормальный вектор $\overrightarrow{n}$ коллинеарны, и потому $\overrightarrow{M_0M} = k\overrightarrow{n}$ для некоторого числа k. Поскольку $\overrightarrow{M_0M} = (x - x_0; y - y_0)$, имеем $x - x_0 = ka, y - y_0 = kb$. Стало быть, $x = x_0 + ka, y = y_0 + kb$. Отсюда

$$ax + by + c = ax_0 + ka^2 + by_0 + kb^2 + c = ax_0 + by_0 + c + k(a^2 + b^2).$$

Поскольку точка M_0 принадлежит прямой l, выполнено равенство $ax_0 + by_0 + c = 0$. Окончательно получаем

$$ax + by + c = k(a^2 + b^2). \qquad (34)$$

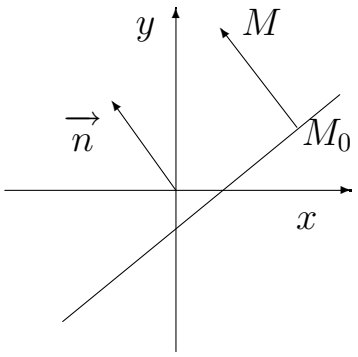

Рис. 14

Отсюда видно, что в каждой точке той полуплоскости, куда «смотрит» вектор $\overrightarrow{n}$, выполнено неравенство $ax + by + c > 0$, а в каждой точке дополнительной полуплоскоскости выполнено противоположное неравенство.

Список литературы

[1] *Коровкин П.П.* Неравенства. (Попул. лекции по математике). М., Наука, 1983.

[2] *Курант Р., Роббинс Г.* Что такое математика: Элементарный очерк идей и методов. М., Просвещение, 1967.

[3] *Оре О.* Приглашение в теорию чисел. (Б-чка "Квант"), М., Наука, 1980.

[4] *Расин В.В.* Действительные числа. Екатеринбург: УрГУ, 1998.

[5] *Серпинский В.* Что мы знаем и чего не знаем о простых числах. М., Физматгиз, 1963.

[6] *Серпинский В.* 250 задач по элементарной теории чисел. М., Просвещение, 1968.

[7] *Соминский И.С.* Метод математической индукции. (Попул. лекции по математике). М., Наука, 1974.

[8] Школа в "Кванте": Арифметика и алгебра / Под ред. А.А.Егорова. М.: Бюро квантум, 1994.

Вениамин Вольфович Расин

ЛЕКЦИИ ПО АЛГЕБРЕ
Элементы теории множеств. Натуральные и целые числа. Неравенства. Отображения множеств. Числовые функции

Учебное пособие

Оригинал-макет подготовлен **В.В.Расиным**
с использованием системы TEX

Подписано в печать 02.09.2004. Формат 60×84 1/16.
Бумага для множительных аппаратов. Печать офсетная.
Уч. изд. л. 7,06. Усл. печ. л. 8,46. Тираж 200 экз. Заказ .
Уральский государственный университет им. А.М.Горького
Екатеринбург, пр. Ленина, 51

Отпечатано на ризографе в СУНЦ УрГУ.
Екатеринбург, ул. Д.Зверева, 30.