

А.А. ЛОКШИН

ЦЕЛЫЕ ЧИСЛА И ДРОБИ

Операторные интерпретации



Москва
«Вузовская книга»
2005

ОГЛАВЛЕНИЕ

Предисловие	3
ГЛАВА 1. Количественный подход к построению системы целых неотрицательных чисел (ц.н.ч)	5
§ 1. Конечные множества	5
§ 2. Определение множества N_0	9
§ 3. Сложение ц.н.ч.	10
§ 4. Коммутативность и ассоциативность сложения	12
§ 5. Отношение «меньше» и его связь со сложением	13
§ 6. Вычитание ц.н.ч.	16
§ 7. Попытка явного описания множества N_0	18
§ 8. Умножение ц.н.ч.	20
§ 9. Деление ц.н.ч.	23
ГЛАВА 2. Множество N_0 как система Пеано	25
§ 1. Аксиомы Пеано	25
§ 2. Метод математической индукции в системах Пеано	26
§ 3. Отношение «меньше» на множестве P	28
§ 4. Установление взаимно-однозначного соответствия между множествами P и N_0	29
§ 5. Некоторые варианты метода математической индукции. Доказательство теоремы о конечности декартова произведения двух конечных множеств	34
§ 6. Простые числа. Основная теорема арифметики	36
ГЛАВА 3. Три подхода к построению множества целых чисел	40
§ 1. Расширение множества N_0 до Z . Алгебраический подход	40
§ 2. Расширение множества N_0 до Z . Геометрический подход	48
§ 3. Вспомогательные сведения из теории операторов	51
§ 4. Натуральное число как аддитивный оператор	53
§ 5. Оператор «минус». Целые отрицательные числа как произведения операторов	55
§ 6. Множество Z как совокупность операторов	56
ГЛАВА 4. Множество Q_+ положительных рациональных чисел	58
§ 1. Обратимые операторы и их свойства	58
§ 2. Определение положительного рационального числа	61
§ 3. Дроби	63
§ 4. Сложение на множестве Q_+	64
§ 5. Отношение «меньше» и его связь со сложением	65
§ 6. Вычитание на множестве Q_+	67
§ 7. Умножение на множестве Q_+	68
§ 8. Деление на множестве Q_+	69
§ 9. Соизмеримость и мера с операторной точки зрения	71
Литература	76
Предметный указатель	77

ББК 22.130
Л 73

В оформлении обложки использована
гравюра «Пифагор и Боэций»
из книги Грегора Рейша «Marguerita philosophica», 1504 г.

Локшин А.А.
Л 73 Целые числа и дроби. Операторные интерпретации /
А.А. Локшин. — М.: Вузовская книга, 2005. — 80 с.: ил.
ISBN 5-9502-0145-0

Учебное пособие посвящено построению систем целых рациональных чисел. Ряд вопросов изложен нетрадиционно, с применением понятия оператора. Все необходимые сведения из теории операторов элементарны и приведены в тексте.

Пособие адресовано в первую очередь студентам младших курсов пединститутов и может быть также полезно старшеклассникам, интересующимся математикой.

ББК 22.130

© Локшин А.А., 2005
ISBN 5-9502-0145-0 © ЗАО «Издательское предприятие «Вузовская книга», 2005

ПРЕДИСЛОВИЕ

Эта книга посвящена построению систем целых неотрицательных, целых и положительных рациональных чисел. Автор попытался изложить основы теории так, чтобы по возможности проявить ее физические корни.

В гл. 1 вниманию читателя предлагается количественный, или теоретико-множественный, подход к построению системы N_0 целых неотрицательных чисел (ц.н.ч.). Этот подход привлекателен в первую очередь своей наглядностью. К сожалению, его последовательное проведение наталкивается на серьезные трудности, которые, насколько это известно автору, могут быть преодолены только с помощью порядкового, или аксиоматического, подхода, излагаемого в гл. 2. Поэтому в большинстве современных руководств предпочтение отдается именно порядковому подходу, в рамках которого теорию ц.н.ч. удастся изложить в логически безупречном виде (см., например, [1], [2]).

Однако, на взгляд автора, наглядность количественного подхода отражает его непосредственную связь с физикой и делает именно этот подход базовым, невзирая на технические трудности. (Сходная точка зрения отражена в [3], [4].)

В гл. 2, посвященной в основном порядковому подходу, показано, что множество N_0 , построенное в гл. 1 в рамках количественного подхода, удастся отождествить с числовой системой P , элементы которой удовлетворяют аксиомам Пеано. В качестве следствия такого отождествления мы получаем, что все аксиомы Пеано оказываются теоремами количественной теории N_0 . В частности, такой теоремой оказывается аксиома индукции, что позволяет в итоге считать метод математической индукции утверждением, независимым от этой аксиомы и доказываемым средствами «наивной» теории множеств.

Далее в гл. 3 строятся различные интерпретации множества Z всех целых чисел. Основной упор в изложении делается на то, чтобы понять, откуда берутся арифметические законы и правила,

действующие на множестве \mathbb{Z} . В частности, показано, что, интерпретируя целые числа как операторы, действующие на одномерные вектора, удастся дать наиболее естественное объяснение правилу умножения целых чисел.

Наконец, в гл. 4 предложена операторная интерпретация множества \mathbb{Q}_+ положительных рациональных чисел. А именно, каждое число из \mathbb{Q}_+ рассматривается как произведение оператора растяжения и оператора сжатия (в целое число раз), действующих, как и в гл. 3, на одномерные вектора. Существенно, что при таком подходе изложение данной темы значительно упрощается, а школьная терминология и школьные обозначения оказываются в полном согласии с принятыми в высшей математике.

Автор
Москва, 2005 г.

ГЛАВА 1

КОЛИЧЕСТВЕННЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ЦЕЛЫХ НЕОТРИЦАТЕЛЬНЫХ ЧИСЕЛ

В этой главе на основе предложенного Р. Дедекиндом понятия конечного множества строится система целых неотрицательных чисел (ц.н.ч.); такой подход, как уже упоминалось в предисловии, называется количественным. Изложение в этой главе почти замкнутое, однако решение важного вопроса о конечности декартова произведения двух конечных множеств отложено до гл. 2.

§ 1. Конечные множества

Прежде чем мы сможем непосредственно перейти к построению системы количественных ц.н.ч., нам придется познакомиться с так называемыми конечными множествами.

Напомним вначале, что два множества A и B называются *равномощными*, если между ними можно установить взаимно-однозначное соответствие. Равномощность множеств A и B обозначается так:

$$A \sim B.$$

ОПРЕДЕЛЕНИЕ (Р. Дедекинд). Непустое множество A называется *конечным*, если оно не равномощно никакому своему подмножеству B , не совпадающему с A .

Замечание. Пустое множество \emptyset считается конечным.

Установим теперь несколько результатов, относящихся к конечным множествам.

Теорема 1.1. Пусть множество A конечно, и пусть $A \sim B$. Тогда множество B также конечно.

Доказательство. Предположим противное, а именно, что

$$B \sim B^1, \quad B^1 \subset B$$

(знак \subset обозначает строгое включение). Далее, пусть

$$A \xrightarrow{f} B, \quad B \xrightarrow{g} B^1$$

— взаимно-однозначные отображения, существующие в силу сделанных предположений. Обозначим через f^{-1} отображение,

обратное f . Очевидно, что при отображении f^{-1} множество B^1 перейдет в некоторое множество A^1 , $A^1 \subset A$. С другой стороны, так как все три отображения f , g и f^{-1} взаимно-однозначны, то результат их последовательного применения

$$A \xrightarrow{f} B \xrightarrow{g} B^1 \xrightarrow{f^{-1}} A^1$$

будет снова представлять собой взаимно-однозначное отображение множества A на $A^1 \subset A$ (см. рис. 1).

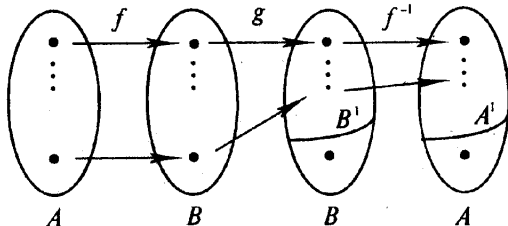


Рис. 1

Однако это противоречит нашему предположению о том, что множество A конечно. ■

Теорема 1.2. Пусть множество A конечно, и пусть $B \subset A$. Тогда B также конечно.

Доказательство. Предположим противное, а именно, что $B \sim B^1$, где $B^1 \subset B$; пусть q — взаимно-однозначное отображение множества B на B^1 . Очевидно, что множество

$$A^1 = (A \setminus B) \cup B^1$$

является подмножеством множества A и не совпадает с ним. Построим теперь отображение

$$A \xrightarrow{f} A^1,$$

положив

$$f(x) = \begin{cases} x & \text{при } x \in A \setminus B \\ q(x) & \text{при } x \in B \end{cases}$$

Нетрудно видеть, что построенное отображение является взаимно-однозначным (см. рис. 2).

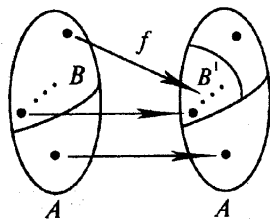


Рис. 2

Тем самым мы получили искомое противоречие. ■

Теорема 1.3. Пусть множества A и B конечны. Тогда их объединение тоже конечно.

Доказательство. Не ограничивая общности, мы можем считать конечные множества A и B непересекающимися. (В противном случае мы всегда можем вместо множества A рассматривать множество $A \setminus B$, которое является конечным в силу предыдущей теоремы.) Для большей наглядности будем представлять себе элементы множества A как белые шары, а элементы множества B — как черные шары. Все шары будем считать имеющими одинаковый радиус (см. рис. 3).

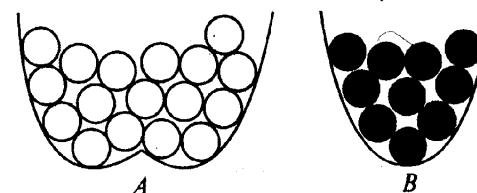


Рис. 3

Будем доказывать теорему от противного. А именно, предположим, что для некоторого $C \subset A \cup B$ можно построить взаимно-однозначное отображение

$$C \xrightarrow{f} A \cup B.$$

Нам будет удобно представлять себе, что действие отображения f осуществляется следующим образом.

Представим себе, что справа от множества $A \cup B$ помещена его фотография и при отображении f каждый шар из множества C перемещается вдоль соответствующей стрелки, идущей от этого шара к некоторому новому месту на фотографии множества $A \cup B$. Тогда, после применения отображения f ко всему множеству C , шары из C займут все места на фотографии множества $A \cup B$; при этом, поскольку к шарам из непустого множества $(A \cup B) \setminus C$ отображение f не применялось, эти шары окажутся «лишними» (см. рис. 4).

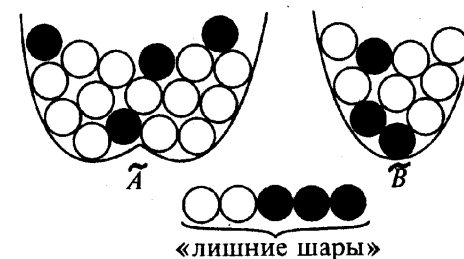


Рис. 4

Далее, обозначим через \bar{A} множество, образовавшееся на месте фотографии множества A , а через \bar{B} — множество, образовавшееся на месте фотографии множества B .

Рассмотрим теперь множество \bar{C} , состоящее из черных шаров, содержащихся в \bar{A} , и множество \bar{B} , состоящее из белых шаров, содержащихся в \bar{B} . Однако чтобы двигаться дальше, нам потребуется следующее теоретико-множественное утверждение, которое мы приведем без доказательства.

УТВЕРЖДЕНИЕ 1.1 (см., например, [6]). *Каковы бы ни были два множества, по крайней мере одно из них равномощно некоторому подмножеству другого.*

Вернемся к доказательству нашей теоремы. Будем для определенности считать, что множество \bar{C} равномощно некоторому подмножеству множества \bar{B} .

В этом случае мы можем обменять все черные шары из \bar{A} на некоторые белые шары из \bar{B} . Множества, образовавшиеся после указанной процедуры на месте \bar{A} и \bar{B} , обозначим через A^* и B^* соответственно. Геометрически очевидно, что

$$A^* \sim A, \quad (1.1)$$

а также, что

$$B^* \sim B. \quad (1.1')$$

Разберем теперь три случая:

а) Среди «лишних» шаров имеются белые. В этом случае, очевидно, имеет место строгое включение

$$A^* \subset A. \quad (1.2)$$

Из (1.1) и (1.2) получаем искомое противоречие с предположением о том, что A — конечное множество;

б) Все «лишние» шары — черные, но белые шары остаются в множестве B^* , получившемся из \bar{B} в результате обмена черными и белыми шарами между \bar{A} и \bar{B} . Очевидно, что тогда (1.2) по-прежнему имеет место, и (1.1), (1.2) снова приводят нас к противоречию;

в) Все «лишние» шары черные и B^* состоит только из черных шаров. В этом случае, очевидно, имеем

$$B^* \subset B. \quad (1.3)$$

Однако соотношения (1.1') и (1.3) противоречат предположению о том, что множество B конечно. Теорема доказана. ■

З а м е ч а н и е. Пусть множество B одноэлементно, т.е. $B = \{x\}$. В этом случае доказательство теоремы 1.3, очевидно, не требует ссылки на утверждение 1.1. Как мы увидим в следующей главе, случай одноэлементного множества B оказывается для нас единственно важным.

В заключение этого параграфа приведем еще один результат, относящийся к теории конечных множеств. Но вначале напомним следующее

ОПРЕДЕЛЕНИЕ. *Декартовым произведением $A \times B$ множеств A и B называется множество, состоящее из всевозможных упорядоченных пар вида (a, b) , где $a \in A$, $b \in B$.*

Теорема 1.4. *Пусть множества A и B конечны. Тогда их декартово произведение $A \times B$ также конечно.*

Доказательство этой теоремы мы отложим до следующей главы.

Задачи

1. Привести пример бесконечного (т.е. не являющегося конечным) множества.

2. Пусть A — бесконечное, а B — конечное множество. Доказать, что

а) множество $A \cup B$ бесконечно;

б) множество $A \setminus B$ бесконечно;

в) множество $B \setminus A$ конечно.

§ 2. Определение множества N_0

Рассмотрим класс K всех таких непустых конечных множеств, что каждое из них может быть взаимно-однозначно отображено на любое другое множество из этого класса.

ОПРЕДЕЛЕНИЕ. Свойство множеств из K , обеспечивающее их принадлежность классу K , называется *натуральным числом*.

Это же свойство, отнесенное к конкретному множеству $A \in K$, называется *численностью* множества A и обозначается $n(A)$. Таким образом, *численность множества A — это число, характеризующее класс, содержащий множество A .*

Классу, состоящему из пустого множества \emptyset , сопоставляется число 0 (ноль).

Множество всех натуральных чисел обозначается через N .
Множество

$$N_0 = N \cup \{0\} \quad (2.1)$$

называется множеством целых неотрицательных чисел (ц.н.ч.).

Два ц.н.ч. a и b считаются равными ($a = b$), если они характеризуют один и тот же класс конечных множеств. Таким образом, равенство ц.н.ч. — это их совпадение.

§ 3. Сложение ц.н.ч.

Пусть теперь A и B — два конечных множества таких, что

$$A \cap B = \emptyset \quad (3.1)$$

и

$$n(A) = a, \quad n(B) = b. \quad (3.2)$$

Обозначим через K класс, которому принадлежит $A \cup B$.

ОПРЕДЕЛЕНИЕ. Свойство, обеспечивающее принадлежность конечного множества $A \cup B$ классу K , называется суммой чисел a и b и обозначается $a + b$.

Замечание. Таким образом, равенство $a + b = c$,

где $a, b, c \in N_0$, означает в точности, что найдутся два конечных множества A и B , удовлетворяющие условиям (3.1) и (3.2) и такие, что численность множества $C = A \cup B$ равна c .

ОПРЕДЕЛЕНИЕ. Операция, сопоставляющая упорядоченной паре ц.н.ч. (a, b) их сумму, называется сложением.

Почему эта операция всегда осуществима? В [3] дается на этот вопрос следующий ответ: ввиду богатства и разнообразия материального мира, где всегда можно найти два непересекающихся конечных множества нужных численностей.

Предложенный ответ, несомненно, интересен с точки зрения связи математики с физикой. Возможен, однако, и такой вариант ответа: если множества A и B с нужными численностями каким-то образом построены, то всегда можно мысленно представить себе множество B' равномошное B и не пересекающееся с A (см. по этому поводу [7, с. 233]).

Теорема 3.1. Определение суммы двух ц.н.ч. a и b не зависит от выбора конечных множеств A и B , если соблюдены условия (3.1) и (3.2).

Доказательство. Действительно, пусть конечные множества A и B удовлетворяют условиям (3.1) и (3.2), и пусть два других конечных множества A' и B' удовлетворяют таким же условиям:

$$A \cap B = \emptyset, \\ n(A') = a, \quad n(B') = b.$$

Рассмотрим вначале случай, когда все четыре множества A, B, A', B' попарно не пересекаются (см. рис. 5).

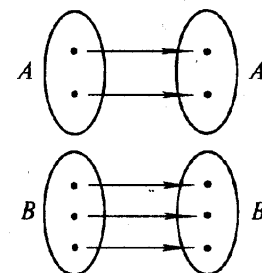


Рис. 5

Из сделанных выше предположений, очевидно, следует, что существует взаимно-однозначное соответствие между множествами A и A' ($A \sim A'$), а также между множествами B и B' ($B \sim B'$). Теперь из рис. 5 геометрически очевидно, что

$$A \cup B \sim A' \cup B',$$

и, следовательно,

$$n(A \cup B) = n(A' \cup B'), \quad (3.4)$$

т.е. независимость суммы $a + b$ от замены множеств A и B на A' и B' установлена.

Возможна, однако, ситуация, когда не пересекающиеся друг с другом множества A' и B' пересекаются с множествами A и B (см. рис. 6).

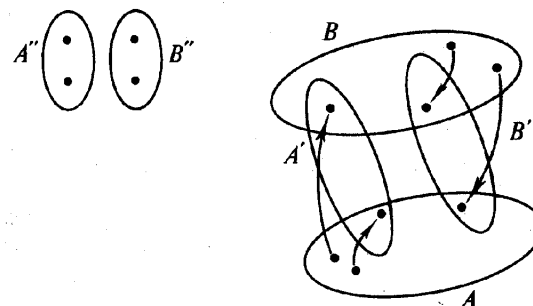


Рис. 6

В этом случае справедливость соотношения (3.3) непосредственно не очевидна. Однако утраченную геометрическую очевидность доказываемой формулы нетрудно восстановить. Для этого рассмотрим пару вспомогательных множеств A'' и B'' таких, что

$$A'' \cap B'' = \emptyset, \\ n(A'') = a, \quad n(B'') = b,$$

и удовлетворяющих тому дополнительному условию, что ни одно из них не пересекается с объединением $A \cup B \cup A' \cup B'$ (см. рис. 6). (Такие множества A'' и B'' также всегда можно найти ввиду многообразия мира.) Геометрически очевидно, что тогда

$$A'' \cup B'' \sim A \cup B$$

и

$$A'' \cup B'' \sim A' \cup B',$$

откуда следует (3.3), а тем самым и искомое соотношение (3.4). ■

Следствие. Сумма двух ц.н.ч. определена однозначно.

Выясним теперь, каковы основные свойства сложения ц.н.ч.

§ 4. Коммутативность и ассоциативность сложения

Коммутативность и ассоциативность операции объединения множеств, т.е. равенства

$$A \cup B = B \cup A \quad (4.1)$$

и

$$(A \cup B) \cup C = A \cup (B \cup C), \quad (4.2)$$

связывающие произвольные множества A, B, C , обеспечивают аналогичные свойства операции сложения ц.н.ч. А именно, справедлива следующая

Теорема 4.1. Пусть a, b, c — произвольные ц.н.ч. Тогда имеют место равенства:

$$a + b = b + a \quad (4.3)$$

(коммутативность сложения);

$$(a + b) + c = a + (b + c) \quad (4.4)$$

(ассоциативность сложения).

Доказательство. Докажем, например, равенство (4.3). Пусть A и B — два непересекающихся конечных множества с численностями a и b соответственно; имеем тогда с учетом (4.1):

$$a + b = n(A) + n(B) = n(A \cup B) = n(B \cup A) = n(B) + n(A) = b + a,$$

что и требовалось установить.

Равенство (4.4) доказывается аналогично. ■

Итак, коммутативность и ассоциативность сложения ц.н.ч. — прямое следствие коммутативности и ассоциативности операции объединения множеств. Заметим, что справедливость равенств (4.1) и (4.2) в свою очередь следует из коммутативности и ассоциативности логического союза «или».

Действительно, утверждать

$$«x \in A \text{ или } x \in B» \quad (4.5)$$

— это то же самое, что утверждать

$$«x \in B \text{ или } x \in A». \quad (4.6)$$

Ясно, что совпадение смыслов предложений (4.5) и (4.6) и означает совпадение множеств $A \cup B$ и $B \cup A$.

Аналогично, утверждать

$$«(x \in A \text{ или } x \in B) \text{ или } x \in C» \quad (4.7)$$

— это то же самое, что утверждать

$$«x \in A \text{ или } (x \in B \text{ или } x \in C)», \quad (4.8)$$

однако совпадение смыслов предложений (4.7) и (4.8) и означает совпадение множеств $(A \cup B) \cup C$ и $A \cup (B \cup C)$.

Таким образом, коммутативность и ассоциативность сложения ц.н.ч. оказывается прямым следствием законов логического мышления.

В заключение этого параграфа отметим, что для любого множества A , очевидно, имеем

$$A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A.$$

Поэтому из определения суммы ц.н.ч. сразу же следует, что для любого $a \in N_0$

$$a + 0 = a. \quad (4.9)$$

§ 5. Отношение «меньше» и его связь со сложением

После того как операция сложения на N_0 была введена, можно определить на этом множестве отношение «меньше» между числами, положив

$$a < b \Leftrightarrow b = a + c, \text{ где } c \in N. \quad (5.1)$$

Замечание 1. Пусть A и B — конечные множества такие, что

$$A \subset B, \quad n(A) = a, \quad n(B) = b. \quad (5.2)$$

Тогда

$$a < b. \quad (5.3)$$

Действительно, представим множество B в виде

$$B = A \cup (B \setminus A).$$

Теперь, поскольку $B \setminus A$ непусто, (5.3) сразу следует из определения суммы ц.н.ч. и определения отношения «меньше». Обратно, если (5.3) выполнено, то, очевидно, найдутся конечные множества A и B , удовлетворяющие условиям (5.2).

Замечание 2. Из данного выше определения сразу следует, что

$$0 < a, \quad (5.4)$$

каково бы ни было $a \in N$. Действительно, имеем $0 + a = a$, откуда в силу (5.1) и следует (5.4).

Нетрудно проверить также, что введенное нами отношение «меньше» обладает следующими свойствами:

а) для любого $a \in N_0$ неверно, что $a < a$

(антирефлексивность);

б) для любых $a, b \in N_0$ таких, что $a \neq b$, имеет место по крайней мере одно из соотношений

$$a < b \text{ или } b < a$$

(связность);

в) для любых $a, b \in N_0$ таких, что $a \neq b$, не могут одновременно выполняться соотношения

$$a < b \text{ и } b < a$$

(асимметричность);

г) для любых $a, b, c \in N_0$

$$a < b, b < c \Rightarrow a < c$$

(транзитивность).

Докажем, например, справедливость утверждения б). Пусть A и B — конечные множества такие, что $n(A) = a$, $n(B) = b$. В силу утверждения 1.1 по крайней мере одно из этих множеств равномощно некоторому подмножеству другого. Пусть, например,

$$A \sim B', \text{ где } B' \subseteq B. \quad (5.5)$$

Однако $B' \neq B$, ибо в противном случае множества A и B принадлежали бы одному классу и мы имели бы $a = b$, что противоречит предположению.

Итак, $B' \subset B$. Следовательно, $B \setminus B'$ непусто; кроме того, множества B и $B \setminus B'$ очевидно, не пересекаются. Из определения сложения поэтому имеем

$$n(B) = n(B') + n(B \setminus B'),$$

где $n(B') = a$ в силу (5.5), $n(B \setminus B') \in N$.

Итак, мы пришли в рассматриваемом случае к равенству вида

$$b = a + c, \quad c \in N,$$

откуда в силу определения отношения «меньше» получаем, что $a < b$.

Случай, когда вместо (5.5) справедливо соотношение

$$B \sim A', \text{ где } A' \subseteq A,$$

рассматривается аналогично.

Тем самым утверждение б) доказано.

Замечание 3. Вместо того, чтобы говорить по отдельности о каждом из свойств а)–г), говорят, что отношение «меньше» на N_0 является отношением *строгого линейного порядка*.

Замечание 4. После того как отношение «меньше» введено, отношения «меньше или равно», «больше», «больше или равно» могут быть введены на N_0 очевидным образом:

$$\begin{aligned} a \leq b &\Leftrightarrow a < b \text{ или } a = b; \\ a > b &\Leftrightarrow b < a; \\ a \geq b &\Leftrightarrow a > b \text{ или } a = b. \end{aligned} \quad (5.6)$$

Дальнейшую связь между отношением «меньше» и операцией сложения на N_0 устанавливает следующая

Теорема 5.1 (монотонность сложения).

Пусть $a, b, c \in N_0$. Тогда

$$a < b \Rightarrow a + c < b + c. \quad (5.7)$$

Доказательство. Пусть $a < b$, тогда в силу (5.1) найдется такое $d \in N$, что $b = a + d$. Следовательно,

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

откуда, пользуясь ассоциативностью и коммутативностью сложения, получаем

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

т.е. $a + c < b + c$, что и требовалось установить. ■

Задача. Пусть $a, b, c, d \in N_0$ и пусть $a < b$, $c < d$. Доказать, что $a + c < b + d$.

В заключение этого параграфа установим с помощью теоремы 5.1 еще одно важное свойство операции сложения.

Теорема 5.2 (сократимость сложения).

Пусть $a, b, c, d \in \mathbb{N}_0$. Тогда

$$a + c = b + c \Rightarrow a = b. \quad (5.8)$$

Доказательство. Будем рассуждать от противного. Пусть $a + c = b + c$, но неверно, что $a = b$. Тогда либо $b < a$, либо $a < b$ (в силу установленных ранее свойств отношения «меньше»). В первом случае, пользуясь теоремой 5.1, получаем, что

$$b + c < a + c,$$

что противоречит условию.

Во втором случае, очевидно, получим

$$a + c < b + c,$$

что также противоречит условию. ■

§ 6. Вычитание ц.н.ч.

ОПРЕДЕЛЕНИЕ. Пусть $a, b \in \mathbb{N}_0$. Разностью $a - b$ называется такое число $c \in \mathbb{N}_0$, что $a = c + b$. Число a называется при этом *уменьшаемым*, а число b — *вычитаемым*. Операция, сопоставляющая упорядоченной паре ц.н.ч. (a, b) их разность, называется *вычитанием*.

Итак, по определению для любых $a, b, c \in \mathbb{N}_0$

$$a - b = c \Leftrightarrow a = c + b. \quad (6.1)$$

Иными словами, вычитание на множестве \mathbb{N}_0 — это операция, обратная сложению.

Очевидно, что разность $a - b$ существует в \mathbb{N}_0 в том и только том случае, когда $b \leq a$ (см. определения отношений «меньше» и «меньше или равно»).

Нетрудно видеть также, что если разность двух ц.н.ч. существует, то она определена однозначно. Действительно, будем рассуждать от противного. Пусть $b \leq a$, и пусть существуют такие два ц.н.ч. c и c^* , $c \neq c^*$, что $a = c + b$ и $a = c^* + b$. Тогда, приравняв правые части двух последних равенств, имеем

$$c + b = c^* + b,$$

откуда в силу сократимости сложения получаем

$$c = c^*,$$

т.е. мы пришли к противоречию.

Установим теперь несколько простых, но важных результатов, характеризующих вычитание в \mathbb{N}_0 .

Теорема 6.1. Пусть $a, b \in \mathbb{N}_0$. Тогда

$$(a + b) - b = a; \quad (6.2)$$

кроме того, если $b \leq a$, то

$$(a - b) + b = a. \quad (6.3)$$

Доказательство. Докажем вначале равенство (6.2). Имеем в силу определения разности:

$$(a + b) - b = a \Leftrightarrow a + b = a + b,$$

т.е. утверждение о справедливости (6.2) оказалось эквивалентным утверждению о справедливости заведомо верного равенства $a + b = a + b$. Тем самым (6.2) установлено.

Аналогично, в силу определения разности:

$$(a - b) + b = a \Leftrightarrow a - b = a - b,$$

откуда и следует (6.3). ■

Теорема 6.2 (монотонность вычитания).

Пусть $a, b, c \in \mathbb{N}_0$ и пусть, кроме того, $c \leq a$. Тогда, если

$$a < b, \quad (6.4)$$

то

$$a - c < b - c. \quad (6.5)$$

Доказательство. Будем рассуждать от противного. Предположим, что условия теоремы выполнены, но (6.5) неверно. Это значит, что найдутся ц.н.ч. a_0, b_0, c_0 , удовлетворяющие неравенствам

$$c_0 \leq a_0, \quad a_0 < b_0$$

и такие, что

$$a_0 - c_0 = b_0 - c_0 \quad \text{или} \quad a_0 - c_0 > b_0 - c_0.$$

Прибавляя теперь c_0 к обеим частям каждого из двух последних соотношений, получаем в силу теоремы 6.1, что должно быть

$$a_0 = b_0 \quad \text{или} \quad a_0 > b_0,$$

т.е. мы пришли к противоречию с условием $a_0 < b_0$. ■

Задача. Пусть $a, b, c, d \in \mathbb{N}_0$ и пусть $a < b$, $c > d$.

Доказать, что тогда имеет место неравенство

$$a - c < b - d$$

(предполагается, что все рассматриваемые разности существуют).

Теорема 6.3. Пусть $a, b, c \in \mathbb{N}_0$. Тогда справедливы следующие три соотношения:

$$(a + b) - c = a + (b - c) \quad (6.6)$$

(предполагается, что $b \geq c$);

$$a - (b + c) = (a - b) - c \quad (6.7)$$

(предполагается, что $a \geq b + c$);

$$a - (b - c) = (a + c) - b \quad (6.8)$$

(предполагается, что $a + c \geq b \geq c$).

З а м е ч а н и е. Свойства (6.6)–(6.8) наиболее естественным образом доказываются не в теории N_0 , а в теории целых чисел, при этом необходимость в дополнительных ограничениях типа неравенств отпадает. Для нас, однако, представляет интерес доказательство этих свойств, не выводящее за рамки теории N_0 .

Доказательство теоремы 6.3. Мы ограничимся доказательством соотношения (6.8), наиболее трудного из трех. Прежде всего, заметим, что в силу определения разности справедливость (6.8) эквивалентна справедливости равенства

$$[a - (b - c)] + b = a + c.$$

Далее, в силу (6.6) справедливость предыдущего равенства эквивалентна тому, что

$$(a + b) - (b - c) = a + c.$$

Однако в силу определения разности справедливость этого равенства эквивалентна справедливости равенства

$$a + b = (a + c) + (b - c).$$

Но справедливость последнего равенства в силу (6.6) эквивалентна справедливости равенства

$$a + b = [(a + c) + b] - c,$$

которое, очевидно, эквивалентно тому, что

$$a + b = [(a + b) + c] - c,$$

т.е.

$$a + b = a + b.$$

Тем самым справедливость проверяемого соотношения (6.8) установлена. ■

§ 7. Попытка явного описания множества N_0

Обозначение для одного ц.н.ч. мы уже ввели раньше, положив

$$0 = n(\emptyset). \quad (7.1)$$

Введем теперь еще одно обозначение:

$$1 = n(\{0\}). \quad (7.2)$$

Этих двух числовых символов нам достаточно, чтобы с помощью операции сложения образовать множество

$$M = \{0; 1; 1+1; 1+1+1; \dots\}. \quad (7.3)$$

Определение множества M с помощью равенства (7.3) следует понимать как сокращенную запись следующих требований, которым должно удовлетворять это множество:

а) $0 \in M$;

б) если $a \in M$, то $a+1 \in M$;

в) M является наименьшим из множеств, удовлетворяющих требованиям а) и б).

Опираясь на свойства сложения, нетрудно показать, что, каково бы ни было $a \in N_0$, не существует такого $b \in N_0$, которое одновременно удовлетворяло бы неравенствам

$$a < b < a+1. \quad (7.4)$$

Действительно, предположим противное, а именно, что для некоторого $a \in N_0$ найдется такое $b \in N_0$, что имеет место (7.4). Тогда в силу монотонности вычитания, очевидно, будем иметь

$$0 < c < 1, \quad (7.5)$$

где обозначено $c = b - a$. Далее, тот факт, что $c \neq 0$, означает, что $c = n(A)$, где A — некоторое непустое конечное множество. Но тогда найдется элемент $x \in A$, и мы можем представить A в виде

$$A = \{x\} \cup (A \setminus \{x\}). \quad (7.6)$$

Оба множества, входящие в правую часть (7.6), очевидно, конечны и не пересекаются. Поэтому, вспоминая определение сложения, получаем из (7.6), что

$$c = 1 + n(A \setminus \{x\}). \quad (7.7)$$

Рассмотрим теперь два случая:

1) $A \setminus \{x\} = \emptyset$ и 2) $A \setminus \{x\} \neq \emptyset$.

В первом случае из (7.7) следует, что $c = 1$, и мы получаем противоречие с правым неравенством из (7.5). Во втором случае имеем $n(A \setminus \{x\}) \in N$, поэтому из (7.7) и определения отношения «меньше» следует, что $1 < c$. Однако и это неравенство противоречит правому неравенству из (7.5).

Итак, мы доказали, что не существует числа $b \in N_0$, удовлетворяющего (7.4). В частности, это означает, что между двумя любыми соседними числами из M невозможно вставить ни одного ц.н.ч. так, чтобы не нарушилась цепочка строгих неравенств.

Однако остается невыясненным вопрос, содержит ли множество M все ц.н.ч., т.е. верно ли, что

$$M = N_0. \quad (7.8)$$

Ответить на этот вопрос мы пока не в состоянии. Впрочем, это не мешает нам начать пользоваться общепринятыми обозначениями:

$$1 + 1 = 2, (1 + 1) + 1 = 3 \text{ и т.д.}$$

§ 8. Умножение ц.н.ч.

ОПРЕДЕЛЕНИЕ. Пусть a, b — два ц.н.ч. Их произведением $a \cdot b$ называется численность множества $A \times B$, где A и B — конечные множества, численности которых равны соответственно a и b . Таким образом,

$$a \cdot b = n(A \times B). \quad (8.1)$$

Операция, сопоставляющая упорядоченной паре ц.н.ч. (a, b) их произведение, называется *умножением*.

Нетрудно видеть, что если

$$A \sim A_1, B \sim B_1,$$

то

$$A \times B \sim A_1 \times B_1.$$

Поэтому определение произведения двух ц.н.ч. a и b не зависит от выбора конкретных конечных множеств A и B , удовлетворяющих условиям $n(A) = a, n(B) = b$. (Тем самым произведение двух ц.н.ч. определено однозначно.)

Замечание 1. Каково бы ни было конечное множество A , имеем $A \times \emptyset = \emptyset$, поэтому для любого $a \in N_0$

$$a \cdot 0 = 0. \quad (8.2)$$

Замечание 2. Ниже для сокращения записи мы будем, как правило, опускать точку, обозначая произведение двух чисел.

Установим теперь несколько важнейших свойств, характеризующих умножение.

Теорема 8.1. Пусть $a, b \in N_0$. Тогда справедливы равенства:

$$ab = ba \quad (8.3)$$

(коммутативность умножения);

$$(ab)c = a(bc) \quad (8.4)$$

(ассоциативность умножения).

Доказательство. Докажем, например, соотношение (8.3). Пусть $n(A) = a, n(B) = b$ и пусть $x \in A, y \in B$. Тогда по определению декартова произведения двух множеств упорядоченная пара (x, y) принадлежит множеству $A \times B$, а упорядоченная пара (y, x) — множеству $B \times A$. Заставим теперь элементы x и y пробегать множества A и B соответственно.

Очевидно, что соответствие

$$(x, y) \rightarrow (y, x)$$

является взаимно однозначным, откуда и следует, что $n(A \times B) = n(B \times A)$, т.е. равенство (8.3).

Соотношение (8.4) доказывается аналогично. ■

Теорема 8.2 (дистрибутивность умножения относительно сложения). Пусть $a, b, c \in N_0$. Тогда справедливы равенства

$$\begin{aligned} a(b + c) &= ab + ac, \\ (b + c)a &= ba + ca. \end{aligned} \quad (8.5)$$

Доказательство. Установим вначале первое из равенств (8.5). Пусть A, B и C — конечные множества, численности которых равны a, b и c соответственно, и пусть $B \cap C = \emptyset$. Нетрудно видеть, что

$$A \times (B \cup C) = (A \times B) \cup (A \times C); \quad (8.6)$$

ясно также, что

$$(A \times B) \cap (A \times C) = \emptyset.$$

Переходя в (8.6) к численностям соответствующих множеств, получаем требуемый результат.

Второе равенство (8.5) следует из первого и коммутативности умножения. ■

Лемма 8.1. Пусть $a, b \in N$. Тогда $ab \in N$.

Доказательство очевидно. ■

Задача

а) Доказать, что $a \cdot 1 = a$ при любом $a \in N_0$.

б) Доказать, что при любых $a \in N_0, b \in N$

$$ab = \underbrace{a + \dots + a}_{b \text{ раз}}.$$

Теорема 8.3 (монотонность умножения).

Пусть $a, b \in N_0, a < b$. Тогда для любого натурального c имеем

$$ac < bc. \quad (8.7)$$

Доказательство. Поскольку $a < b$, существует натуральное d такое, что $a + d = b$.

Следовательно,

$$(a + d)c = bc, \quad (8.8)$$

откуда в силу теоремы 8.2

$$ac + dc = bc.$$

Однако, как следует из леммы 8.1, dc — натуральное число. Теперь (8.7) вытекает из (8.8) и определения отношения «меньше». ■

СЛЕДСТВИЕ (сократимость умножения).

а) Пусть $a, b, c \in \mathbb{N}_0$, $c \neq 0$. Тогда

$$ac = bc \Rightarrow a = b. \quad (8.9)$$

б) Пусть $a, b, c \in \mathbb{N}_0$. Тогда

$$ac < bc \Rightarrow a < b. \quad (8.10)$$

Задача. Пусть $a, b, c, d \in \mathbb{N}_0$, причем $a < b$, $c < d$. Доказать, что $ac < bd$.

Теорема 8.4 (дистрибутивность умножения относительно вычитания).

Пусть $a, b, c \in \mathbb{N}_0$, причем $c \leq b$. Тогда справедливы соотношения:

$$a(b - c) = ab - ac \quad (8.11)$$

и

$$(b - c)a = ba - ca. \quad (8.12)$$

Доказательство. Прежде всего заметим, что вследствие предыдущей теоремы обе части (8.11), а также обе части (8.12), определены. Докажем соотношение (8.11). В силу определения разности справедливость (8.11) эквивалентна тому, что

$$a(b - c) + ac = ab. \quad (8.13)$$

Подчеркнем, что «раскрыть скобки» в левой части (8.13) мы сейчас не имеем права — именно эту возможность мы и обосновываем. Однако мы можем воспользоваться дистрибутивностью умножения относительно сложения, написав (8.13) в эквивалентном виде

$$a[(b - c) + c] = ab,$$

что в силу обратности вычитания к сложению эквивалентно

$$ab = ab.$$

Тем самым справедливость (8.11) доказана.

Равенство (8.12) следует из (8.11) и коммутативности умножения. ■

§ 9. Деление ц.н.ч.

ОПРЕДЕЛЕНИЕ. Пусть $a, b \in \mathbb{N}_0$, причем $b \neq 0$. Частным от деления a на b называется такое число $c \in \mathbb{N}_0$, что $a = cb$. (Частное от деления a на b обозначается $a : b$.) Число a называется при этом *делимым*, а число b — *делителем*.

Таким образом, при $b \neq 0$

$$a : b = c \Leftrightarrow a = cb. \quad (9.1)$$

Операция, сопоставляющая упорядоченной паре чисел (a, b) их частное, называется *делением*. (Как следует из (9.1), деление является операцией, обратной по отношению к умножению.)

Деление (подобно вычитанию) выполнимо в \mathbb{N}_0 не всегда. Покажем, например, что число 1 не делится на 2. Будем рассуждать от противного. Предположим, что существует такое $c \in \mathbb{N}_0$, что $1 : 2 = c$. Тогда в силу определения частного получим

$$1 = 2c.$$

Очевидно, что $c \neq 0$. Следовательно, как мы знаем,

$$0 < c. \quad (9.2)$$

Далее, так как $c \neq 0$, то, очевидно,

$$1 = c \text{ или } 1 < c. \quad (9.3)$$

Теперь, складывая (9.2) с каждым из соотношений (9.3), получаем в обоих случаях $1 < 2c$, что противоречит исходному предположению.

В приводимых ниже теоремах мы установим основные свойства деления.

Теорема 9.1 (единственность деления).

Пусть $a, b, c, c_1 \in \mathbb{N}_0$, $b \neq 0$. Тогда, если

$$a : b = c \text{ и } a : b = c_1, \quad (9.4)$$

то

$$c = c_1.$$

Доказательство. Предположим противное, т.е. что условия теоремы выполнены, но $c \neq c_1$. Однако из (9.4) и определения частного следует, что

$$a = cb, \quad a = c_1b,$$

откуда

$$cb = c_1b.$$

Пользуясь теперь сократимостью умножения, заключаем, что $c = c_1$. Итак, мы пришли к противоречию с предположением. ■

Следующая теорема вполне аналогична теореме 6.1, и мы опускаем ее доказательство.

Теорема 9.2. Пусть $a, b \in \mathbb{N}_0$, $b \neq 0$.

Тогда

$$(ab) : b = a, \quad (9.5)$$

кроме того, если частное $a : b$ существует в \mathbb{N}_0 , то

$$(a : b)b = a. \quad (9.6)$$

В приводимой ниже теореме мы устанавливаем те свойства деления в \mathbb{N}_0 , аналоги которых встретятся нам в гл. 4 при изучении правил действия над дробями.

Теорема 9.3. Пусть $a, b, c \in \mathbb{N}_0$. Тогда, в предположении, что все участвующие ниже разности и частные существуют в \mathbb{N}_0 , справедливы равенства

$$(a : c) \pm (b : c) = (a \pm b) : c; \quad (9.7)$$

$$(a : c) \cdot (b : d) = (ab) : (cd); \quad (9.8)$$

$$(a : b) : (c : d) = (ad) : (bc). \quad (9.9)$$

Доказательство. Справедливость (9.7) и (9.8) доказывается совсем просто; проведение соответствующих выкладок представляется читателю. Докажем (9.9). В силу определения частного вместо (9.9) достаточно установить равенство

$$a : b = [(ad) : (bc)] : (c : d).$$

Однако в силу (9.8) правая часть предыдущей формулы может быть представлена в виде $[(ad)c] : [(bc)d]$, или, что то же самое, в виде $[a(cd)] : [b(cd)]$. Таким образом, достаточно проверить, что

$$a : b = [a(cd)] : [b(cd)].$$

Но справедливость последнего равенства легко следует из (9.8). ■

Задача. Пусть $a, b, c, d \in \mathbb{N}_0$. Доказать, что тогда

$$(a : b) \pm (c : d) = (ad \pm bc) : bd. \quad (9.10)$$

(Все действия предполагаются осуществимыми в \mathbb{N}_0).

ГЛАВА 2

МНОЖЕСТВО \mathbb{N}_0 КАК СИСТЕМА ПЕАНО

Данная глава посвящена изложению основ теории так называемых систем Пеано. Показано, что на множестве \mathbb{N}_0 операция прибавления единицы порождает отношение «непосредственного следования», удовлетворяющее аксиомам Пеано. Это обстоятельство позволяет обосновать некоторые утверждения из гл. 1, оставшиеся недоказанными (в частности, теорему о конечности декартова произведения двух конечных множеств), дать независимое доказательство теоремы о конечности объединения двух конечных множеств и, кроме того, привести более явное описание множества \mathbb{N}_0 .

§ 1. Аксиомы Пеано

Системой Пеано мы будем называть всякое множество P , на котором задано отношение *непосредственного следования*, обозначаемое штрихом и удовлетворяющее приводимым ниже аксиомам, которые мы, следуя традициям, будем называть *аксиомами Пеано* (см. [2]). (На самом деле эти аксиомы были впервые предложены Дедекиндом.)

Аксиома 1. Для каждого элемента $a \in P$ существует единственный непосредственно следующий за ним элемент a' .

Аксиома 2. Существует начальный элемент $\Omega \in P$, который непосредственно не следует ни за каким элементом из P .

Аксиома 3. Каковы бы ни были $a, b \in P$, равенство $a' = b'$ влечет $a = b$.

Аксиома 4 (аксиома индукции). Пусть M есть подмножество множества P , содержащее Ω и такое, что если $a \in M$, то и $a' \in M$. Тогда $M = P$.

Заметим, что аксиомы Пеано сами по себе не обеспечивают единственность множества P и заданного на нем отношения следования. Однако это обстоятельство нам нисколько не мешает.

§ 2. Метод математической индукции в системах Пеано

В этом параграфе мы сформулируем и докажем теорему о методе математической индукции применительно к произвольной взятой системе Пеано. Для того чтобы этот метод превратился в мощное математическое орудие, позволяющее решать, казалось бы, нерешаемые задачи, нам еще предстоит доказать, что множество N_0 можно превратить в систему Пеано, положив

$$\begin{aligned} 0 &= \Omega, \\ a+1 &= a', \quad a \in N_0. \end{aligned}$$

(Этому будут посвящены следующие параграфы данной главы.)

Итак, вернемся к произвольной системе Пеано P . Справедлива следующая

Теорема 2.1 (о методе математической индукции для произвольной системы Пеано). Пусть $A(k)$ — некоторое утверждение, зависящее от $k \in P$. Пусть, далее, известно, что

- а) $A(\Omega)$ — истинное утверждение;
- б) каково бы ни было $m \in P$, из истинности $A(m)$ следует истинность $A(m')$.

Тогда $A(k)$ истинно при всех $k \in P$.

Доказательство. Рассмотрим множество, состоящее из всех таких $k \in P$, что $A(k)$ — истинное утверждение. Из условий теоремы и четвертой аксиомы Пеано следует тогда, что рассматриваемое множество совпадает со всем P . Но именно это и требовалось установить. ■

На практике метод математической индукции применяют так:

1. Доказывают утверждение $A(\Omega)$.
2. Делают предположение о том, что $A(m)$ верно при некотором произвольном, но фиксированном $m \in P$.
3. Доказывают, что тогда $A(m')$ также верно, каково бы ни было $m \in P$.

Существуют и иные разновидности метода математической индукции (см., например, [2], [5]); наиболее распространен вариант, в котором множество P заменяется на $P \setminus \{\Omega\}$, а роль Ω играет Ω' .

Часто используется также тот вариант метода математической индукции, в котором множество P заменяется на $P \setminus \{\Omega, \Omega'\}$, а роль Ω играет Ω'' .

(Для того чтобы обосновать справедливость первого из двух только что упомянутых вариантов метода математической индук-

ции, достаточно доопределить $A(k)$ при $k = \Omega$, взяв в качестве $A(\Omega)$ какое-нибудь истинное утверждение. Для второго из двух упомянутых вариантов метода ситуация полностью аналогична: нужно доопределить $A(k)$ при $k = \Omega$ и при $k = \Omega'$, взяв в качестве $A(\Omega)$ и $A(\Omega')$ какие-нибудь истинные утверждения.)

Установим теперь с помощью метода математической индукции следующие два полезных результата.

Лемма 2.1. Каково бы ни было $k \in P$,
 $k' \neq k$. (2.1)

Доказательство. Будем рассуждать по индукции. Пусть вначале $k = \Omega$. В этом случае утверждение леммы, очевидно, верно, т.е.

$$\Omega' \neq \Omega$$

(см. вторую аксиому Пеано).

Предположим теперь, что утверждение леммы справедливо при $k = m$, т.е. что

$$m' \neq m, \quad (2.2)$$

и докажем, что тогда оно справедливо и для $k = m'$, каково бы ни было $m \in P$. А именно, покажем, что

$$(m')' \neq m'. \quad (2.3)$$

Предположим противное, т.е. допустим, что $(m')' = m'$. Тогда в силу третьей аксиомы Пеано должно быть $m' = m$, однако это противоречит предположению (2.2). Тем самым (2.3) установлено, и лемма доказана. ■

Введем теперь одно полезное

ОПРЕДЕЛЕНИЕ. Пусть $s, t \in P$ и пусть

$$s' = t,$$

т.е. элемент t непосредственно следует за элементом s . Мы будем в этом случае говорить, что элемент s непосредственно предшествует элементу t и записывать это в виде

$$t = 's. \quad (2.4)$$

Лемма 2.2. Пусть $k \in P$, $k \neq \Omega$. Тогда существует единственный элемент $'k \in P$.

Доказательство. Снова воспользуемся методом индукции. При $k = \Omega'$ утверждение леммы, очевидно, верно. (Тот факт, что Ω является единственным элементом, непосредственно предшествующим Ω' , следует из третьей аксиомы Пеано.)

Предположим теперь, что утверждение леммы верно при $k = m$, и докажем, что оно оказывается тогда верным и при $k = m'$. Однако m' непосредственно следует за m ; следовательно, m непосредственно предшествует m' . Других элементов, непосредственно предшествующих m' , не существует в силу третьей аксиомы Пеано. ■

З а м е ч а н и е. Нетрудно проверить, что справедливы формулы

$$('k)' = k, \quad k \in P \setminus \{\Omega\}; \quad (2.5)$$

$$'(k') = k, \quad k \in P. \quad (2.6)$$

§ 3. Отношение «меньше» на множестве P

В этом параграфе мы увидим, что отношение непосредственного следования, введенное при помощи аксиом Пеано, позволяет определить на множестве P отношение «меньше», обладающее теми же свойствами, что и отношение «меньше» на множестве N_0 .

Прежде всего, определим по индукции множества T_k , $k \in P$, положив

$$\begin{aligned} T_\Omega &= \{\Omega\}, \\ T_{k'} &= T_k \cup \{k'\}. \end{aligned} \quad (3.1)$$

З а м е ч а н и е. Множества T_k мы будем называть *начальными отрезками* множества P .

Действуя по индукции, можно показать, что справедливы следующие утверждения.

Лемма 3.1. Для каждого $k \in P$ начальный отрезок T_k является подмножеством множества P и определен единственным образом.

Лемма 3.2. Для любого $k \in P$

$$T_k \cap \{k'\} = \emptyset. \quad (3.2)$$

Теорема 3.1. Пусть $k, m \in P$. Тогда

$$T_k \subset T_m \text{ либо } T_m \subset T_k, \text{ либо } k = m. \quad (3.3)$$

Определим теперь отношение «меньше» на множестве P , положив для любых $a, b \in P$

$$a < b \Leftrightarrow T_a \subset T_b. \quad (3.4)$$

Из теоремы 3.1, очевидно, следует, что введенное на P отношение «меньше» оказывается отношением строгого линейного порядка (как и отношение «меньше», введенное в § 5 гл. 1 на множестве N_0).

Справедлива следующая

Теорема 3.2 (см., например, [2]). Пусть $T \subseteq P$, $T \neq \emptyset$. Тогда в T найдется наименьший элемент.

§ 4. Установление взаимно-однозначного соответствия между множествами P и N_0

В этом параграфе мы установим такое взаимно-однозначное соответствие между элементами множеств P и N_0 , которое сохраняет отношение «меньше», элемент $\Omega \in P$ переводит в ноль, а операцию «штрих» переводит в операцию прибавления единицы. В силу взаимной однозначности этого соответствия мы сможем заключить, что все аксиомы Пеано справедливы (уже в качестве теорем) и для множества N_0 , если «непосредственное следование» понимать как «возрастание на единицу», а ноль выбрать в качестве начального элемента. Тем самым у нас появится возможность пользоваться методом математической индукции в арифметических задачах, сформулированных на языке количественной теории N_0 .

Установим теперь несколько вспомогательных результатов.

Лемма 4.1. Для любого $k \in P$ множество T_k конечно.

Доказательство. Воспользуемся индукцией по k . Прежде всего, очевидно, что множество $T_\Omega = \{\Omega\}$ конечно. Далее, предположим, что утверждение леммы справедливо при некотором $k = m$ и докажем его при $k = m'$. Однако в силу своего определения множество $T_{m'}$ представляет собой объединение $T_m \cup \{m'\}$ и, следовательно, конечно, в силу замечания к теореме 1.3 из гл. 1. ■

Лемма 4.2. Множество P бесконечно (т.е. не является конечным).

Доказательство. Рассмотрим отображение

$$f: P \rightarrow P \setminus \{\Omega\},$$

задаваемое формулой

$$f(k) = k'$$

(здесь k пробегает все P). В силу леммы 2.2 у любого элемента $m \in P \setminus \{\Omega\}$ существует непосредственно предшествующий ему элемент $'m \in P$. Поэтому имеем

$$f('m) = ('m)' = m,$$

т.е. f отображает P на все $P \setminus \{\Omega\}$. Взаимная однозначность этого отображения следует из теоремы 3.1. Теперь бесконечность множества P вытекает из определения конечного множества. ■

Пусть теперь A — некоторое непустое множество; обозначим через S_A совокупность всех подмножеств множества A , равномошных каким-нибудь T_k .

Лемма 4.3. *Непустое множество A содержит подмножество, равномошное P , тогда и только тогда, когда для любого $A_\alpha \in S_A$*

$$A \setminus A_\alpha \neq \emptyset. \quad (4.1)$$

Доказательство.

Необходимость. Будем рассуждать от противного. Пусть A содержит подмножество B , равномошное P (и тем самым бесконечное в силу леммы 4.2), но найдется такое $A_\alpha \in S_A$, что

$$A \setminus A_\alpha = \emptyset. \quad (4.2)$$

Поскольку в силу леммы 4.1 A_α конечно, из (4.2) следует, что и A конечно. Однако множество A не может быть конечным, так как у него имеется бесконечное подмножество B . Итак, мы пришли к противоречию.

Достаточность. Пусть выполнено условие (4.1) для каждого $A_\alpha \in S_A$. Покажем, что тогда каждому $k \in P$ можно сопоставить элемент $x_k \in A$, причем так, что

$$x_{k_1} \neq x_{k_2} \text{ если } k_1 < k_2. \quad (4.3)$$

Действительно, поскольку множество A непусто, всегда можно выбрать в нем какой-нибудь элемент; обозначим этот элемент через x_Ω и образуем множество $A_\Omega = \{x_\Omega\}$. Очевидно, что $A_\Omega \sim T_\Omega$.

Следующие элементы определим индуктивным образом.

Пусть нами уже построены элемент x_k и множество $A_k \subseteq A$ такое, что $A_k \sim T_k$. В силу (4.1) множество $A \setminus A_k$ непусто; выберем в нем какой-нибудь элемент, который обозначим через $x_{k'}$, после чего образуем множество

$$A_{k'} = A_k \cup \{x_{k'}\}.$$

Ясно, что $A_{k'} \sim T_{k'}$.

Нетрудно видеть, что в силу своего построения элементы x_k удовлетворяют условию (4.3). Однако из (4.3) сразу же вытекает и формально более сильное условие:

$$x_{k_1} \neq x_{k_2} \text{ если } k_1 \neq k_2. \quad (4.3')$$

Это и означает, что в A существует подмножество

$$\{x_k \mid k \in P\},$$

равномошное P . ■

З а м е ч а н и е. Осуществляя выбор элемента в каждом из множеств $A \setminus A_k$, мы фактически использовали так называемую *аксиому выбора* (см., например, [14]).

Лемма 4.4. *Пусть A — непустое множество, не содержащее подмножества, равномошного P . Тогда A равномошно некоторому T_k , $k \in P$.*

Доказательство. В силу леммы 4.3 должно найтись такое A_α , что

$$A \setminus A_\alpha = \emptyset \text{ и, тем самым, } A = A_\alpha.$$

(Здесь, как и в предыдущей лемме, A_α — подмножество множества A , равномошное некоторому T_k .) Отсюда и следует требуемое утверждение. ■

Приведем теперь основной результат этого параграфа.

Теорема 4.1. *Непустое множество A конечно тогда и только тогда, когда оно равномошно некоторому начальному отрезку T_k множества P .*

Доказательство. Достаточность уже была установлена в лемме 4.1.

Необходимость. Пусть непустое множество A конечно. Тогда оно не может содержать подмножества B , равномошного P . Действительно, в силу леммы 4.2 такое подмножество B , очевидно, было бы бесконечным, что противоречит свойствам конечных множеств. Теперь требуемое утверждение следует из леммы 4.4. ■

Наша следующая задача — установить взаимно-однозначное соответствие между P и N_0 ; это позволит нам затем перенести на N_0 свойства систем Пеано.

Определим отображение

$$P \xrightarrow{\varphi} N_0 \quad (4.4)$$

индуктивными соотношениями:

$$\begin{aligned} \varphi(\Omega) &= 0, \\ \varphi(k') &= \varphi(k) + 1 \end{aligned} \quad (4.5)$$

(здесь $k \in P$ произвольно) и докажем вначале два вспомогательных утверждения.

Лемма 4.5. Пусть $k \in P$. Тогда

$$\varphi(k) = n(T_k) - 1. \quad (4.6)$$

(Здесь через $n(T_k)$ обозначена численность множества T_k .)

Доказательство. Как обычно, действуем по индукции. При $k = \Omega$ утверждение леммы очевидно. Допустим, что (4.6) верно при $k = m$, т.е. что

$$\varphi(m) = n(T_m) - 1, \quad (4.7)$$

и докажем, что тогда (4.6) верно и при $k = m'$, т.е.

$$\varphi(m') = n(T_{m'}) - 1. \quad (4.8)$$

Однако из (4.5) следует, что

$$\varphi(m') = \varphi(m) + 1; \quad (4.9)$$

кроме того, из определения множества $T_{m'}$ и леммы 3.2 имеем

$$T_{m'} = T_m \cup \{m'\}, \quad T_m \cap \{m'\} = \emptyset,$$

откуда вытекает, что

$$n(T_{m'}) = n(T_m) + 1. \quad (4.10)$$

Теперь (4.8) следует из (4.7), (4.9) и (4.10). ■

Лемма 4.6. Соответствие между множествами P и $\varphi(P)$, определяемое формулами (4.5), взаимно-однозначно.

Доказательство. Пусть $k, s \in P, k \neq s$. Покажем, что тогда $\varphi(k) \neq \varphi(s)$. Действительно, в силу теоремы 3.1 имеем $T_s \subset T_k$ или $T_k \subset T_s$. Пусть, например, $T_s \subset T_k$. Но тогда, очевидно,

$$\varphi(s) < \varphi(k),$$

так что $\varphi(s) \neq \varphi(k)$. (Обратим внимание на то, что связностью отношения «меньше» на N_0 мы здесь не пользовались.)

В то же время каждое $k \in P$ имеет единственный образ $\varphi(k)$ в силу того, что множество T_k определено однозначно. Тем самым утверждение леммы доказано. ■

Теперь с помощью теоремы 4.1 удастся установить следующий важный результат.

Теорема 4.2. Отображение φ , задаваемое формулами (4.5), устанавливает взаимно-однозначное соответствие между P и N_0 .

Доказательство. Учитывая результат леммы 4.6, нам остается доказать только, что φ отображает P на все N_0 , т.е. что

$$\varphi(P) = N_0.$$

Действительно, пусть $A \rightarrow$ конечное множество такое, что $n(A) = a$. В силу предыдущей теоремы существует $k \in P$ такое, что $n(A) = n(T_k)$, откуда

$$a = \varphi(k'),$$

что и доказывает утверждение теоремы. ■

Замечание 1. Нетрудно видеть, что отображение (4.5) сохраняет отношение «меньше». Иными словами,

$$k < m \Leftrightarrow \varphi(k) < \varphi(m) \quad (4.11)$$

(здесь $k, m \in P$).

Докажем вначале, что из левого неравенства (4.11) следует правое. Действительно, неравенство $k < m$ означает по определению, что $T_k \subset T_m$, откуда имеем $n(T_k) < n(T_m)$ (см. § 5 гл. 1) и, следовательно, $\varphi(k) < \varphi(m)$.

Обратно, пусть выполнено правое неравенство (4.11); покажем, что тогда левое неравенство (4.11) также справедливо. Действительно, в силу леммы 4.5

$$\varphi(k) = n(T_k) - 1, \quad \varphi(m) = n(T_m) - 1,$$

поэтому из правого неравенства (4.11) следует, что

$$n(T_k) < n(T_m).$$

Учитывая результат теоремы 3.1, сразу получаем отсюда, что

$$T_k \subset T_m,$$

и, следовательно,

$$k < m,$$

что и требовалось установить. ■

Замечание 2. Из теорем 3.2, 4.2 и соотношения (4.11), очевидно, следует, что в каждом непустом подмножестве множества N_0 имеется наименьшее число.

Замечание 3. Кроме того, из теоремы 4.2, соотношения (4.11) и связности отношения «меньше» на множестве P следует независимое доказательство связности отношения «меньше» на N_0 .

Замечание 4. Очевидно, что при взаимно-однозначном отображении

$$P \xrightarrow{\varphi} N_0$$

операции «штрих», заданной на P , соответствует операция прибавления единицы, заданная на N_0 . Таким образом, само множество N_0 можно рассматривать как систему Пеано, в которой элементом, «непосредственно следующим» за данным, является

элемент, больший на единицу, а нуль играет роль начального элемента Ω . Очевидно также, что все аксиомы Пеано оказываются тем самым теоремами количественной теории N_0 . При этом новым, неизвестным нам ранее, оказывается следующее утверждение, соответствующее аксиоме индукции.

Теорема 4.3. Пусть M — подмножество множества N_0 , удовлетворяющее условиям:

- а) $0 \in M$;
- б) если $s \in M$, то $s+1 \in M$.

Тогда $M = N_0$.

Итак, мы получили, наконец, ответ на вопрос, поставленный в § 6 гл. 1 относительно справедливости равенства (6.8) из этой главы.

§ 5. Некоторые варианты метода математической индукции.

Доказательство теоремы о конечности декартова произведения двух конечных множеств

Прежде всего, сформулируем еще один вариант теоремы о методе математической индукции, опирающийся на этот раз на теорему 4.3.

Теорема 5.1. Пусть $A(k)$ — некоторое утверждение, зависящее от номера $k \in N_0$, $k \geq k_0$. Пусть, далее, известно, что:

- а) $A(k_0)$ — истинное утверждение;
- б) каково бы ни было $m \in N_0$, $m \geq k_0$, из истинности $A(m)$ следует истинность $A(m+1)$.

Тогда $A(k)$ истинно при всех $k \in N_0$, $k \geq k_0$.

Доказательство. Определим серию утверждений $B(s)$, $s \in N_0$ равенствами

$$B(s) = A(k_0 + s)$$

и положим

$$M = \{s \in N_0 \mid B(s) \text{ истинно}\}.$$

Нетрудно видеть, что множество M удовлетворяет обоим условиям, сформулированным в теореме 4.3. Следовательно, $M = N_0$, что и доказывает теорему. ■

Замечание 1. Подчеркнем, что все результаты этой главы (и теорему 5.1, в частности) мы получили, не опираясь на теоретико-множественное утверждение 1.1 из гл. 1, приведенное там без доказательства.

Замечание 2. Теперь с помощью теоремы 5.1 мы можем доказать, что объединение двух конечных множеств конечно, не используя утверждения 1.1 из гл. 1.

Действительно, пусть C и D — конечные множества; не ограничивая общности, считаем, что C и D не пересекаются. Обозначим

$$n(D) = d$$

и воспользуемся индукцией по d . При $d = 1$ сделанное утверждение, очевидно, верно, поскольку объединение конечного множества C с одним новым элементом по-прежнему конечно. (Для доказательства этого факта не требуется привлекать утверждение 1.1 гл. 1; см. замечание к теореме 1.3 из гл. 1.)

Допустим теперь, что наше утверждение верно при $d = m$ и докажем его при $d = m+1$. Однако добавление одного нового элемента по-прежнему оставляет конечное множество конечным, что и завершает доказательство.

Замечание 3. Точно так же, опираясь на теорему 5.1, теперь мы сумеем доказать теорему 1.4 из гл. 1 (о конечности декартова произведения двух конечных множеств).

Доказательство теоремы 1.4, гл. 1. Пусть C и D — два произвольных конечных множества; обозначим $n(D) = d$. Докажем, что декартово произведение $C \times D$ конечно, пользуясь индукцией по d .

Нам будет удобно обозначать численность множества D с помощью индекса. А именно, $n(D_1) = 1$, $n(D_2) = 2$, ...

Пусть вначале $d = 1$; в этом случае, очевидно, имеем

$$C \times D_1 = C,$$

что и доказывает конечность множества $C \times D_1$.

Предположим теперь, что утверждение теоремы верно при $d = m$, т.е. что множество $C \times D_m$ конечно, и докажем, что тогда утверждение теоремы остается справедливым и при $d = m+1$.

Нетрудно видеть, однако, что

$$C \times D_{m+1} = (C \times D_m) \cup (C \times D_1).$$

Теперь конечность множества $C \times D_{m+1}$ следует из предположения индукции в силу теоремы о конечности объединения двух конечных множеств. ■

Задачи

1. Доказать, что $n(\{1, 2, \dots, k\}) = k$.2. Пусть $A(k)$ — утверждение, зависящее от номера $k \in N_0$.

Пусть, далее, известно что:

а) $A(0)$ — истинное утверждение;б) каково бы ни было $m \in N_0$, из истинности $A(0), \dots, A(m)$ следует истинность $A(m+1)$.Доказать, что тогда $A(k)$ истинно при всех $k \in N_0$.3. Пусть снова $A(k)$ — утверждение, зависящее от номера $k \in N_0$. Пусть, кроме того, известно, что:а) утверждения $A(0)$ и $A(1)$ истинны;б) каково бы ни было $m \in N_0$, из истинности $A(m)$ следует истинность $A(m+2)$.Доказать, что тогда $A(k)$ истинно при всех $k \in N_0$.

§ 6. Простые числа. Основная теорема арифметики

Материал этого параграфа будет в дальнейшем использован в гл. 4 один-единственный раз при определении несократимых дробей.

Прежде всего нам потребуется следующее

ОПРЕДЕЛЕНИЕ 1. Пусть $k, m \in N$. Число m называется *множителем* числа k , если

$$k = mq \quad (6.1)$$

для некоторого $q \in N$.

Из (6.1), очевидно, вытекает, что

$$k : m = q, \quad (6.1')$$

поэтому число m иногда называют также *делителем* числа k .

Замечание. Очевидно, что у каждого натурального k , большего единицы, имеются по крайней мере два множителя: это 1 и само число k .

Следующее определение является основным в данном параграфе.

ОПРЕДЕЛЕНИЕ 2. Натуральное число p , большее единицы, называется *простым*, если у него нет других множителей, кроме 1 и p . В противном случае число p называется *составным*.

Замечание. Число 1 по определению не относят ни к простым, ни к составным.

Приведем еще одно важное

ОПРЕДЕЛЕНИЕ 3. Натуральные числа k и m называются *взаимно простыми*, если у них нет общих множителей, отличных от 1.

Замечание. Взаимно простые числа сами не обязательно являются простыми. Например, составные числа 8 и 9 взаимно просты.

Условимся также о том, что всякое произведение вида $k_1 \dots k_n$, где числа $k_i \in N$ не обязательно все попарно различны, мы будем называть *конечным*.

Сформулируем теперь и докажем утверждение, которое принято называть «основной теоремой арифметики». (Наше доказательство будет в общих чертах следовать [11].)

Теорема 6.1. Каждое натуральное число k , большее единицы, единственным образом (с точностью до перестановки сомножителей) представимо в виде конечного произведения простых чисел.

Замечание. В случае простого k мы будем по определению считать, что $k = k$ и есть искомое представление числа k .

Доказательство теоремы.

Существование. Будем рассуждать от противного. А именно, предположим, что существуют натуральные числа, большие единицы и не представимые в виде конечного произведения простых множителей. Множество всех таких чисел обозначим через M . Из замечания 2 к теореме 4.1 следует тогда, что в M (ибо M , по предположению, непусто) должно найтись наименьшее число. Обозначим это число через k_0 ; очевидно, что $k_0 > 1$.

Если допустить, что k_0 — простое, то мы сразу приходим к противоречию с тем, что $k_0 \in M$.

Поэтому мы вправе считать, что число k_0 — составное. Однако в этом случае из определения составного числа следует, что

$$k_0 = k_1 k_2, \quad (6.2)$$

где k_1 и k_2 — натуральные числа, из которых по крайней мере одно отлично от 1 и от k_0 . Пусть, например,

$$k_1 \neq 1, k_0. \quad (6.3)$$

Однако из (6.2), (6.3) ясно, что и для другого множителя справедливо аналогичное утверждение:

$$k_2 \neq 1, k_0. \quad (6.4)$$

Далее, из (6.2)–(6.4) легко следует, что должны выполняться неравенства

$$1 < k_1, k_2 < k_0,$$

из которых, в свою очередь, вытекает, что числа k_1 и k_2 не могут принадлежать множеству M . Следовательно, для k_1 и k_2 существуют представления в виде конечных произведений

$$k_1 = p_1 p_2 \dots p_n, \quad k_2 = q_1 q_2 \dots q_m, \quad (6.5)$$

где все p_i и q_j — простые числа.

Из (6.2) и (6.5) имеем теперь

$$k_0 = p_1 p_2 \dots p_n q_1 q_2 \dots q_m, \quad (6.6)$$

однако обнаруженная возможность представить k_0 в виде произведения (6.6) противоречит тому, что $k_0 \in M$.

Единственность. Будем, как и при доказательстве существования, рассуждать от противного. А именно, предположим, что существуют натуральные числа, большие единицы и представимые в виде конечного произведения простых чисел по крайней мере двумя способами. Пусть m_0 — наименьшее среди таких чисел; очевидно, что $m_0 > 1$.

Далее, пусть

$$m_0 = c_1 c_2 \dots c_t \quad (6.7)$$

и

$$m_0 = d_1 d_2 \dots d_s \quad (6.8)$$

— два различных (т.е. отличающихся не только порядком сомножителей) представления числа m_0 в виде конечного произведения простых чисел. Нетрудно видеть, что ни одно из c_i не может совпадать ни с одним из d_j . Действительно, если бы, например, было

$$c_1 = d_1,$$

то число $m_0 : c_1$, очевидно, разлагалось бы в произведение простых множителей двумя различными способами, будучи при этом меньше, чем m_0 .

Итак, мы установили, что каждое c_i должно отличаться от каждого d_j . Пусть, например,

$$d_1 < c_1. \quad (6.9)$$

Рассмотрим произведение

$$m = (c_1 - d_1) c_2 \dots c_t. \quad (6.10)$$

Заметим теперь, что множитель $c_1 - d_1$ может быть составным числом, однако $c_1 - d_1$ не может иметь d_1 в качестве простого множителя.

Действительно, если бы было:

$$c_1 - d_1 = d_1 b, \quad b \in N,$$

то мы бы имели

$$c_1 = d_1 (1 + b),$$

что противоречит простоте числа c_1 . Поэтому, разлагая $c_1 - d_1$ на простые множители и подставляя это разложение в (6.10), мы, очевидно, получим представление числа m в виде произведения простых множителей, среди которых не содержится d_1 .

С другой стороны, раскрывая в (6.10) скобки и пользуясь тем, что в силу (6.7), (6.8)

$$c_1 c_2 \dots c_t = d_1 d_2 \dots d_s,$$

получим:

$$\begin{aligned} m &= c_1 c_2 \dots c_t - d_1 c_2 \dots c_t = d_1 d_2 \dots d_s - d_1 c_2 \dots c_t = \\ &= d_1 (d_2 \dots d_s - c_2 \dots c_t). \end{aligned} \quad (6.11)$$

Из (6.11), очевидно, следует, что m представимо в виде такого произведения простых множителей, в которое входит простое число d_1 . Кроме того, из (6.9)–(6.11) ясно, что $m > 1$.

Итак, число m удалось разложить на простые множители двумя различными способами (отличающимися не только порядком сомножителей).

Нетрудно видеть, однако, что

$$m < m_0,$$

и мы приходим к противоречию с предположением о том, что m_0 — наименьшее натуральное число, большее единицы, которое раскладывается на простые множители более чем одним способом. ■

С дальнейшими сведениями, касающимися простых чисел, можно познакомиться, например, по учебнику [1].

ГЛАВА 3

ТРИ ПОДХОДА К ПОСТРОЕНИЮ МНОЖЕСТВА ЦЕЛЫХ ЧИСЕЛ

В этой главе излагаются три различных подхода к пополнению множества N_0 целыми отрицательными числами и, тем самым, к построению множества Z всех целых чисел.

Первый подход является чисто алгебраическим; он основан на естественном для математика желании сделать операцию вычитания всегда выполнимой и одновременно сохранить «хорошие свойства» операций, заданных на N_0 . Однако при таком подходе природа целого числа ускользает от понимания и остается неясным, отражают ли введенные нами числа какую-нибудь реальность.

При втором подходе — геометрическом — целые числа уподобляются направленным отрезкам с кратными длинами, расположенным на прямой и исходящим из фиксированной точки, выбранной в качестве начала координат. Как мы увидим ниже, такая интерпретация целых чисел позволяет дать превосходное объяснение арифметическим законам, действующим на множестве Z .

Однако геометрический подход недостаточно гибок, и с его помощью неудобно обосновывать арифметические законы, действующие на множестве всех рациональных чисел.

Поэтому мы рассмотрим также третий подход, при котором числа из Z интерпретируются как произведения операторов отражения и кратного растяжения, действующих на направленные отрезки. В следующей главе аналогичная интерпретация будет дана положительным рациональным числам.

§ 1. Расширение множества N_0 до Z . Алгебраический подход.

В этом параграфе мы займемся расширением множества N_0 до Z исходя из соображений, лежащих внутри самой математики. А именно, мы постараемся присоединить к N_0 новые элементы так, чтобы

- 1) операция вычитания стала всегда выполнимой;
- 2) наиболее общие законы арифметики, действовавшие на N_0 , сохранили свою силу и при сделанном расширении.

Еще одно требование (также чисто математическое), которому мы хотим удовлетворить, таково:

- 3) построенное расширение множества N_0 не должно содержать «лишних» элементов, без которых можно обойтись, удовлетворив требованиям 1) и 2). (Последнее требование называют *условием минимальности*.)

Итак, пусть a и b — два произвольных п.н.ч., и пусть

$$b - a = c$$

— их разность, уже не обязательно принадлежащая N_0 . По-прежнему считая вычитание операцией, обратной к сложению, перепишем предыдущее равенство в эквивалентном виде:

$$b = c + a.$$

Положим здесь $b = 0$ и переобозначим c через $-a$; в результате получим, что, каково бы ни было $a \in N_0$, в расширении множества N_0 должен найтись элемент $-a$ такой, что

$$0 = -a + a. \quad (1.1)$$

Итак, желая сделать операцию вычитания всегда выполнимой, мы пришли к необходимости пополнить множество N_0 элементами вида $-a$, удовлетворяющими соотношению (1.1). Как мы увидим далее, указанного пополнения достаточно, чтобы удовлетворить требованиям 1) и 2), сформулированным выше. Очевидно, что тем самым условие минимальности для нашего расширения также оказывается соблюденным.

Приступим теперь непосредственно к построению системы целых чисел Z .

В соответствии со сказанным выше, сопоставим каждому числу $a \in N_0$ *противоположное* число $-a$, которое будем считать элементом некоторого абстрактного множества N_0^- . Таким образом,

$$N_0^- = \{-a \mid a \in N_0\}.$$

Затем по определению положим

$$Z = N_0 \cup N_0^- \quad (1.2)$$

и станем называть Z *множеством целых чисел*. Конечно, это определение не будет содержательным, пока мы не ввели на Z арифметические операции.

Прежде всего, определим на \mathbb{Z} операцию сложения с помощью следующих условий:

а) сложение на множестве \mathbb{Z} является всюду однозначно определенной, коммутативной и ассоциативной операцией, которая на подмножестве $N_0 \subset \mathbb{Z}$ совпадает со сложением, введенным в теории N_0 ранее;

б) для любого $a \in \mathbb{Z}$

$$0 + a = a; \quad (1.3)$$

в) для любого $a \in N_0$ справедливо равенство (1.1).

Докажем теперь серию простых утверждений, которые дадут нам дополнительную информацию о том, как устроено множество \mathbb{Z} .

УТВЕРЖДЕНИЕ 1.1. Пусть $a, b \in N_0$. Тогда, если $a \neq b$, то $-a \neq -b$.

Доказательство. Будем рассуждать от противного. Пусть $a \neq b$, но

$$-a = -b.$$

Прибавим к обеим частям этого равенства выражение $a + b$. Пользуясь коммутативностью и ассоциативностью сложения на множестве \mathbb{Z} , легко получим, что

$$a = b,$$

т.е. мы пришли к противоречию. ■

УТВЕРЖДЕНИЕ 1.2. Пусть $a, b \in N_0$, $b \neq 0$. Тогда $-a \neq b$.

Доказательство. От противного. Пусть выполнены все сформулированные условия, но

$$-a = b.$$

Прибавим к обеим частям этого равенства число $a \in N_0$; получим

$$0 = a + b,$$

откуда следует, что

$$0 \geq b > 0,$$

т.е. мы пришли к противоречию. ■

УТВЕРЖДЕНИЕ 1.3.

$$-0 = 0. \quad (1.4)$$

Доказательство. Имеем из (1.1), (1.3) с учетом коммутативности сложения на множестве \mathbb{Z} :

$$-0 = 0 + (-0) = 0,$$

что и требовалось установить. ■

Таким образом, в соответствии с нашей терминологией, нуль противоположен сам себе.

Из доказанных утверждений, очевидно, следует, что

$$N_0 \cap N_0^- = \{0\}.$$

Обозначим

$$N^- = N_0^- \setminus \{0\}; \quad (1.5)$$

множество N^- мы будем в дальнейшем называть *множеством целых отрицательных чисел*. Ясно, что

$$N_0 \cap N^- = \emptyset. \quad (1.6)$$

Теперь, очевидно, можно переписать (1.2) следующим образом:

$$\mathbb{Z} = N \cup \{0\} \cup N^-. \quad (1.7)$$

Замечание. По аналогии с N^- множество N иногда называют *множеством целых положительных чисел*.

УТВЕРЖДЕНИЕ 1.4. Пусть $a, b \in \mathbb{Z}$, и пусть

$$a + b = 0. \quad (1.8)$$

Тогда либо $a \in N$, $b = -a$, либо $b \in N$, $a = -b$, либо $a = b = 0$.

Доказательство. Достаточно рассмотреть случай, когда $a \neq 0$. Пусть, например, $a \in N^-$. Тогда $a = -c$, где $c \in N$ (причем в силу утверждения 1.1 такое представление единственно). Прибавляя к обеим частям равенства $(-c) + b = 0$, получим $b = c$. Следовательно, $a = -b$.

Случай $a \in N$ рассматривается аналогично. ■

Замечание. Таким образом, каково бы ни было $a \in \mathbb{Z}$, существует единственное $b \in \mathbb{Z}$ такое, что выполняется (1.8). Условимся в этом случае писать:

$$b = -a.$$

При $a \in N_0$ введенные обозначения, очевидно, совпадают с прежними (см. (1.1)). Если же $a = -c$, $c \in N$, то (1.8) приобретает вид

$$(-c) + b = 0, \quad (1.8')$$

и в новых обозначениях имеем

$$b = -(-c).$$

В то же время из утверждения 1.4 следует, что при заданном $c \in N$ единственным решением уравнения (1.8') является

$$b = c.$$

Из двух последних равенств, очевидно, получаем, что

$$-(-c) = c.$$

(При выводе (1.9) мы считали, что $c \in N$, однако это равенство, как нетрудно видеть, остается справедливым при любом $c \in Z$.)

УТВЕРЖДЕНИЕ 1.5. Пусть $a, b \in N_0, a \geq b$. Тогда

$$a + (-b) = a - b, \quad (1.10)$$

где $a - b$ — разность чисел a и b , вычисленная в N_0 .

Доказательство. Имеем

$$a = (a - b) + b;$$

прибавляя $(-b)$ к обеим частям этого равенства, получаем требуемый результат. ■

Определим теперь модуль числа $a \in Z$, положив

$$|a| = \begin{cases} a, & a \in N_0, \\ -a, & a \in N^-. \end{cases} \quad (1.11)$$

Таким образом, в силу (1.9)

$$|-c| = c \text{ для всякого } c \in N_0.$$

Справедлива следующая

Теорема 1.1. Пусть $a, b \in Z$. Тогда

а) если $a, b \in N_0$, то

$$a + b \in N_0 \text{ и } |a + b| = |a| + |b|;$$

б) если $a \in N_0, b \in N^-$ и $|a| \geq |b|$, то

$$a + b \in N_0 \text{ и } |a + b| = |a| - |b|;$$

в) если $a \in N_0, b \in N^-$ и $|b| > |a|$, то

$$a + b \in N^- \text{ и } |a + b| = |b| - |a|;$$

г) если $a, b \in N^-$, то

$$a + b \in N^- \text{ и } |a + b| = |a| + |b|.$$

Доказательство. Проверим, например, утверждение в). Пусть $a \in N_0, b = -c$, где $c \in N$. Имеем тогда

$$[a + (-c)] + [c + (-a)] = 0$$

(мы воспользовались ассоциативностью сложения на множестве Z и соотношениями (1.1), (1.3)). Учитывая утверждение 1.5, можно переписать последнее равенство в виде

$$[a + (-c)] + [c - a] = 0, \quad \text{откуда}$$

откуда в силу утверждения 1.4

$$a + (-c) = -(c - a) \in N^-.$$

Из последнего соотношения и определения модуля имеем также

$$|a + (-c)| = c - a = |c| - |a|,$$

что и завершает доказательство утверждения в). Остальные утверждения теоремы доказываются аналогично. ■

Определим теперь вычитание на множестве Z как операцию, обратную сложению.

Иными словами, положим для любых $a, b, c \in Z$

$$a - b = c \Leftrightarrow a = c + b. \quad (1.12)$$

Прибавляя $(-b)$ к обеим частям правого равенства из (1.12), получим

$$a = c + b \Leftrightarrow a + (-b) = c. \quad (1.12')$$

Теперь из (1.12), (1.12'), очевидно, имеем

$$a - b = a + (-b), \quad (1.13)$$

т.е. для целых чисел вычитание сводится к сложению с числом, противоположным вычитаемому. Из (1.13) следует также, что вычитание на множестве Z является всюду однозначно определенной операцией.

З а м е ч а н и е. Из однозначности операции вычитания целых чисел и того факта, что вычитание на множестве N_0 было также определено как операция, обратная к сложению, очевидно, вытекает, что для любых $a, b \in N_0$, таких, что $a \geq b$, имеем

$$a - b = a - b.$$

Введем теперь отношение «меньше» на множестве Z . А именно, положим для любых $a, b \in Z$

$$a < b \Leftrightarrow b - a \in N. \quad (1.14)$$

На множестве N_0 введенное отношение «меньше», очевидно, совпадает с отношением «меньше», введенным ранее в теории N_0 .

Можно показать, что отношение «меньше» на Z является отношением строгого линейного порядка. Нетрудно видеть также, что если $a \in N$, то из определения (1.14) следует, что

$$\begin{aligned} 0 &< a, \\ -a &< 0. \end{aligned}$$

Что касается отношений «меньше или равно», «больше», «больше или равно», то они вводятся на \mathbb{Z} с помощью отношения «меньше» точно так же, как это было сделано в теории N_0 (см. гл. 1, § 5).

Определим теперь операцию умножения на множестве \mathbb{Z} с помощью следующих условий:

а) умножение целых чисел является всюду однозначно определенной, коммутативной и ассоциативной операцией;

б) умножение целых чисел дистрибутивно относительно сложения;

в) на подмножестве $N_0 \subset \mathbb{Z}$ эта операция совпадает с умножением, введенным ранее в теории N_0 ;

г) для всех $a \in \mathbb{Z}$

$$1 \cdot a = a; \quad (1.15)$$

д) для всех $a \in \mathbb{Z}$

$$0 \cdot a = a. \quad (1.16)$$

УТВЕРЖДЕНИЕ 1.6. Пусть $a \in \mathbb{Z}$. Тогда

$$-1 \cdot a = -a. \quad (1.17)$$

Доказательство.

Имеем $1 + (-1) = 0$, откуда в силу (1.16) $[1 + (-1)]a = 0$. Пользуясь дистрибутивностью умножения относительно сложения, получаем из последнего равенства с учетом (1.15):

$$a + (-1)a = 0,$$

откуда и следует (1.17) (см. замечание к утверждению 1.4). ■

Приведем теперь основной результат, характеризующий умножение на множестве \mathbb{Z} .

Теорема 1.2 («правило знаков»). Пусть $a, b \in \mathbb{N}$. Тогда

$$(-a)b = a \cdot (-b) = -(ab) \quad (1.18)$$

и

$$(-a) \cdot (-b) = ab. \quad (1.19)$$

Доказательство. Докажем, например, соотношение (1.19). Имеем, учитывая утверждение 1.6:

$$\begin{aligned} (-a) \cdot (-b) &= [(-1)a] \cdot [(-1)b] = (-1) \cdot (-1)ab = \\ &= (-1) \cdot (-ab) = -(-ab) = ab, \end{aligned} \quad (1.20)$$

что и требовалось установить. ■

Замечание 1. В (1.20) мы использовали запись $(-1) \cdot (-1)ab$, в которой обошлись без лишних скобок, учитывая ассоциативность умножения целых чисел.

Замечание 2. Из теоремы 1.2 ясно, что умножение в \mathbb{Z} (в отличие от умножения в N_0) не монотонно. Действительно, $2 < 5$ и $-2 < -1$, но $2 \cdot (-2) > 5 \cdot (-1)$.

Следствие из теоремы 1.2. Пусть $a, b \in N_0$. Тогда

$$|ab| = |a| \cdot |b|. \quad (1.21)$$

Теперь мы можем, наконец, определить деление на множестве \mathbb{Z} как операцию, обратную умножению. А именно, положим для любых $a, b, c \in \mathbb{Z}$, $b \neq 0$:

$$a : b = c \Leftrightarrow a = cb. \quad (1.22)$$

Нетрудно видеть, что на подмножестве $N_0 \subset \mathbb{Z}$ только что введенная операция совпадает с делением, введенным в теории N_0 ранее.

Заметим также, что из равенства $a = cb$ следует, что $|a| = |c| \cdot |b|$, и, значит,

$$|c| = |a| : |b|,$$

т.е. модуль частного равен частному от деления модулей.

Что касается знака частного, то он, очевидно, определяется по правилу, вытекающему из «правила знаков» для умножения:

$$\begin{aligned} a : b &> 0, \text{ если } a \text{ и } b \text{ одного знака,} \\ a : b &< 0, \text{ если } a \text{ и } b \text{ разных знаков} \end{aligned}$$

(здесь предполагается, что не только b , но и a отлично от нуля); ясно также, что

$$0 : b = 0.$$

Из сказанного выше ясно, что если частное от деления двух чисел из \mathbb{Z} существует, то оно определено единственным образом.

Итак, мы в общих чертах описали действие арифметических операций на множестве целых чисел.

Однако у нас остались без ответа некоторые важные вопросы. Например, такие:

Почему следовало распространять с множества N_0 на все \mathbb{Z} действие каждого из выбранных нами законов арифметики? Почему монотонностью умножения было целесообразно пожертвовать? Те ли числа мы построили, которые нужны «на самом деле»?

В следующих параграфах мы попытаемся получить ответы на эти вопросы.

§ 2. Расширение множества N_0 до Z . Геометрический подход

Попробуем теперь подойти к вопросу о расширении множества ц.ч. несколько иначе. Будем исходить из модели, в которой целые положительные и отрицательные числа обозначают изменение некоторой дискретной величины с указанием на одно из двух возможных направлений этого изменения.

Общепринятая (и самая удобная) модель такова. Нарисуем прямую l и выберем на ней в качестве начала отсчета (начала координат) произвольную точку O (см. рис. 7).

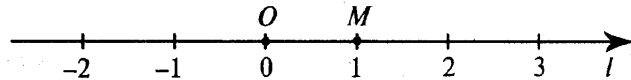


Рис. 7

Правее точки O выберем на нашей прямой некоторую точку M ; отрезок OM будем считать *единичным*. Теперь, последовательно откладывая отрезок OM вправо от точки O неограниченное число раз, будем отмечать и нумеровать концы получающихся отрезков числами 1, 2, Аналогично, откладывая отрезок OM влево от точки O , будем отмечать и последовательно нумеровать концы образующихся отрезков с помощью символов -1, -2, Наконец, рядом с точкой O напомним символ 0 (ноль).

Теперь если мы скажем, например, что координата точки A на прямой l равна -3, то это будет означать, что точка A находится левее точки O на расстоянии, равном утроенной длине отрезка OM .

Итак, точки, отмеченные нами на прямой l , изображают множество Z , однако этого нам явно недостаточно. Прежде всего, следует указать, по какому правилу складываются изображенные нами числа из Z .

Пусть A — некоторая точка из числа отмеченных нами на прямой l . Заметим, что этой точке соответствует не только ее координата (т.е. стоящая рядом числовая отметка), но и направленный отрезок OA (с началом в точке O и концом в точке A).

Сформулируем теперь известное *правило сложения направленных отрезков*.

Пусть OA и OB — направленные отрезки, расположенные на прямой l . Суммой $OA + OB$ назовем отрезок OC , где C — точка на прямой l , в которую перейдет конец отрезка OB , если его начало совместить с точкой A при помощи параллельного переноса.

Такое определение сложения хорошо согласуется с его интуитивным пониманием: сумма $OA + OB$ представляет собой направленное изменение величины OA на величину OB .

Теперь заметим, что мы фактически дали определение операции сложения целых чисел: если $k, m \in Z$ и если k есть координата точки A , а m — координата точки B на нашей прямой, то, чтобы сложить числа k и m , нужно найти сумму $OC = OA + OB$ и посмотреть на координату точки C . (Для чисел из N_0 это определение, очевидно, совпадает с определением сложения, известным нам из количественной теории.)

Покажем теперь, что определенное нами сложение чисел из Z коммутативно. Действительно, пусть $a, b \in N$ и пусть, например, $a < b$. Нам следует проверить, что

$$a + (-b) = (-b) + a.$$

Однако справедливость этого равенства геометрически очевидна из рис. 8.

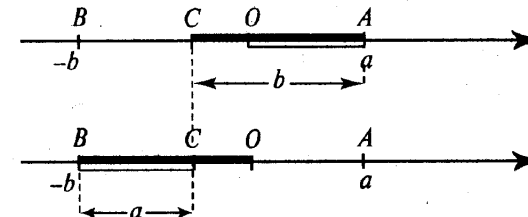


Рис. 8

Остальные случаи рассматриваются аналогично.

Точно так же доказывается ассоциативность сложения; без труда вводится и вычитание как операция, обратная к сложению.

Итак, операция сложения чисел из Z удачно моделируется с помощью сложения направленных отрезков (длины которых кратны длине некоторого «единичного» отрезка). Но как определить произведение двух чисел из Z с помощью этой модели? Здесь приходит на помощь следующее рассуждение (см. по этому поводу, например, [10]).

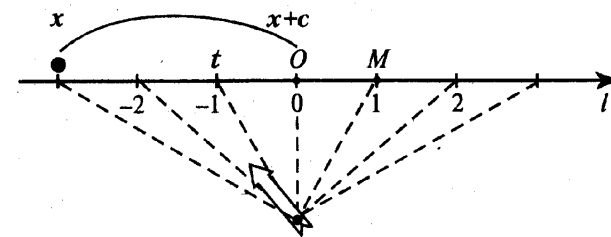


Рис. 9

Рассмотрим часы, в которых прямая l играет роль циферблата (см. рис. 9) и предположим, что всякий раз, когда часовая стрелка перемещается на одно деление, материальная частица, расположенная на прямой, скачком перемещается из точки с целочисленной координатой x в точку с целочисленной координатой $x + c$ ($c \in \mathbb{Z}$). В качестве нормирующего условия примем, что в момент времени $t = 0$ частица приобретает координату $x = 0$.

Пусть вначале $c \in \mathbb{N}$. Тогда в момент времени $t \in \mathbb{N}$, очевидно, будем иметь

$$x = ct. \quad (2.1)$$

Таким образом, для натуральных c и t отображение, переводящее упорядоченную пару (c, t) в соответствующую координату x частицы сводится к перемножению чисел c и t .

Естественно поэтому и для любых $c, t \in \mathbb{Z}$ назвать отображение

$$(c, t) \rightarrow x \quad (2.1')$$

умножением числа c на число t и записывать (2.1') по-прежнему в виде (2.1).

Проверим, приведет ли это определение умножения чисел из \mathbb{Z} к тому же «правилу знаков», что и в § 1. Пусть, например,

$$c = -c_1, \quad t = -t_1, \quad (2.2)$$

где c_1 и t_1 — натуральные числа. Элементарный подсчет показывает, что в этом случае координата частицы оказывается равной

$$x = c_1 t_1,$$

так что с учетом (2.1) и (2.2) получаем:

$$(-c_1)(-t_1) = c_1 t_1.$$

Действуя аналогичным образом, нетрудно придти к выводу, что при нашем определении умножения

$$(-c_1)t_1 = -(c_1 t_1),$$

$$c_1(-t_1) = -(c_1 t_1)$$

(здесь, как и выше, $c_1, t_1 \in \mathbb{N}$).

Итак, «правило знаков» при вышеприведенном определении умножения сохраняется.

Рассмотренная модель представляется достаточно убедительной и, по сути, завершает обоснование сформулированных в § 1 арифметических законов для чисел из \mathbb{Z} .

И все же проблема обоснования упомянутых арифметических законов настолько важна, что мы разберем еще одно ее решение.

Для этого нам придется взглянуть на числа из \mathbb{Z} с совершенно иной — операторной — точки зрения.

§ 3. Вспомогательные сведения из теории операторов

В следующих параграфах мы рассмотрим операторную модель числовой системы \mathbb{Z} . Однако для этого нам придется сделать сейчас небольшое отступление от основной темы данной главы и изложить первоначальные сведения из теории операторов.

Пусть X — множество, на котором задана коммутативная и ассоциативная операция сложения, и пусть

$$L: X \rightarrow X \quad (3.1)$$

— отображение множества X в себя, т.е. закон, согласно которому каждый элемент $x \in X$ переходит в некоторый другой элемент того же множества X . Отображение (3.1) мы будем называть *оператором*, заданным на X , а результат применения оператора L к элементу $x \in X$ будем обозначать через Lx .

Пусть L_1 и L_2 — два оператора, заданные на X ; мы будем называть эти операторы *равными* и писать

$$L_1 = L_2,$$

если $L_1 x = L_2 x$ для всех $x \in X$.

Далее, пусть L — оператор, заданный на X . Назовем оператор L *аддитивным*, если для любых $x_1, x_2 \in X$

$$L(x_1 + x_2) = Lx_1 + Lx_2. \quad (3.2)$$

Множество всех заданных на X аддитивных операторов мы будем обозначать через $\Lambda(X, X)$.

Суммой операторов $L_1, L_2 \in \Lambda(X, X)$ мы будем называть оператор L , определяемый равенством

$$Lx = L_1 x + L_2 x, \quad (3.3)$$

а произведением операторов L_1 и L_2 — оператор M , определяемый равенством

$$Mx = L_1(L_2 x). \quad (3.4)$$

(В (3.3) и (3.4) x пробегает все множество X .)

Коротко соотношения (3.3) и (3.4) записываются в виде

$$L = L_1 + L_2 \quad (3.3')$$

и

$$M = L_1 L_2 \quad (3.4')$$

соответственно.

Замечание 1. Пусть $L_i, i = 1, 2, 3, 4$ — операторы, заданные на X . Тогда, если

$$L_1 = L_2, \quad L_3 = L_4,$$

то

$$L_1 + L_3 = L_2 + L_4$$

и

$$L_1 L_3 = L_2 L_4.$$

Справедливость сказанного сразу следует из определения равенства операторов.

Сделанное замечание представляется вполне очевидным, однако оно нам очень пригодится в гл. 4.

Замечание 2. Из приведенных выше определений, очевидно, следует, что сумма и произведение аддитивных операторов, заданных на X , также являются аддитивными операторами, заданными на X .

Итак, мы определили сложение и умножение на множестве $\Lambda(X, X)$. Справедлива следующая

Теорема 3.1. Пусть $L_1, L_2, L_3 \in \Lambda(X, X)$. Тогда

$$L_1 + L_2 = L_2 + L_1 \quad (3.5)$$

(коммутативность сложения операторов);

$$(L_1 + L_2) + L_3 = L_1 + (L_2 + L_3) \quad (3.6)$$

(ассоциативность сложения операторов);

$$(L_1 L_2) L_3 = L_1 (L_2 L_3) \quad (3.7)$$

(ассоциативность умножения операторов);

$$\begin{aligned} L_1 (L_2 + L_3) &= L_1 L_2 + L_1 L_3, \\ (L_2 + L_3) L_1 &= L_2 L_1 + L_3 L_1 \end{aligned} \quad (3.8)$$

(дистрибутивность умножения аддитивных операторов относительно сложения).

Доказательство. Равенство (3.5) следует из определения суммы операторов и коммутативности сложения на X . Аналогично, равенство (3.6) следует из определения суммы операторов и ассоциативности сложения на X . Далее, равенство (3.7) следует непосредственно из определения произведения операторов. Наконец, равенства (3.8) следуют из аддитивности рассматриваемых операторов, а также из определения суммы и произведения операторов. ■

Замечание 1. Подчеркнем, что при доказательстве соотношений (3.5)–(3.7) аддитивность участвующих в них операторов не играла никакой роли. Особо отметим, что для доказательства ассоциативности умножения операторов нам не потребовалась также ни коммутативность, ни ассоциативность сложения на X .

Замечание 2. Обратим внимание читателя также на то, что в общем случае $L_1 L_2 \neq L_2 L_1$, т.е., вообще говоря, умножение операторов из $\Lambda(X, X)$ не коммутативно.

Отметим, наконец, что оператор $I \in \Lambda(X, X)$ такой, что

$$Ix = x \text{ для всех } x \in X \quad (3.9)$$

называется *единичным*. Нетрудно видеть, что

$$IL = LI = L \quad (3.10)$$

для каждого оператора $L \in \Lambda(X, X)$.

§ 4. Натуральное число как аддитивный оператор

Расширим систему направленных отрезков, введенную в § 2, рассмотрев совокупность E всех направленных отрезков на прямой l , начало которых совпадает с выделенной точкой O . При этом нам будет удобно считать, что в систему E входит и «нулевой» отрезок \overline{OO} , которому можно приписать любое из двух имеющихся на прямой l направлений.

Мы будем по-прежнему предполагать, что направленные отрезки из системы E складываются в соответствии с правилом, сформулированным в § 2.

Сопоставим теперь каждому натуральному числу k оператор

$$\hat{k} : E \rightarrow E,$$

который удлиняет отрезки из рассматриваемой системы в k раз, сохраняя при этом их направления. Множество всех операторов вида \hat{k} , где $k \in \mathbb{N}$, мы будем обозначать через $\hat{\mathbb{N}}(E, E)$.

Пример. Рассмотрим точки A, B, C и D на прямой l (см. рис. 10). В соответствии с данным выше определением мы, очевидно, можем написать:

$$\hat{3}\overline{OA} = \overline{OB}, \quad \hat{5}\overline{OC} = \overline{OD}.$$

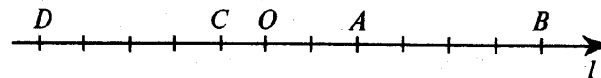


Рис. 10

З а м е ч а н и е. Очевидно, что для «нулевого» отрезка \overline{OO} будем иметь

$$\hat{k}\overline{OO} = \overline{OO} \quad (4.1)$$

при каждом $\hat{k} \in \hat{N}(E, E)$.

Итак, натуральному числу оказалось возможным сопоставить оператор. Подчеркнем, что эта возможность появилась у нас потому, что мы рассмотрели систему E однородных объектов (направленных отрезков), обладающих следующим свойством: каков бы ни был отрезок $\overline{OA} \in E$ и каково бы ни было $k \in N$, найдется отрезок $\overline{OB} \in E$ такой, что его направление совпадает с направлением отрезка \overline{OA} , а длина в k раз превышает длину \overline{OA} .

(В принципе, мы могли бы вместо направленных отрезков рассматривать и другую систему объектов — например, набор гирь, которые можно ставить на одну из двух чаш весов. Тогда оператор \hat{k} увеличивал бы вес гири в k раз.)

Приведем теперь два простых утверждения, характеризующих введенные нами операторы.

УТВЕРЖДЕНИЕ 4.1. Пусть $\hat{k} \in \hat{N}(E, E)$. Тогда для любых двух направленных отрезков $\overline{OA}, \overline{OB} \in E$ справедливо равенство

$$\hat{k}(\overline{OA} + \overline{OB}) = \hat{k}\overline{OA} + \hat{k}\overline{OB}, \quad (4.2)$$

т.е. оператор \hat{k} аддитивен.

Доказательство этого утверждения геометрически очевидно.

УТВЕРЖДЕНИЕ 4.2. Пусть $\hat{k}_1, \hat{k}_2 \in \hat{N}(E, E)$. Тогда

$$\hat{k}_1 + \hat{k}_2 = \widehat{k_1 + k_2} \quad (4.3)$$

и

$$\hat{k}_1 \hat{k}_2 = \widehat{k_1 k_2}. \quad (4.4)$$

Доказательство. Пусть \overline{OA} — произвольный направленный отрезок из системы E . Геометрически очевидно, что тогда

$$\hat{k}_1 \overline{OA} + \hat{k}_2 \overline{OA} = \widehat{(k_1 + k_2)} \overline{OA},$$

а также что

$$\hat{k}_1 (\hat{k}_2 \overline{OA}) = \widehat{(k_1 k_2)} \overline{OA},$$

откуда и вытекают соотношения (4.3), (4.4). ■

З а м е ч а н и е. Из (4.3), (4.4) следует, в частности, что на множестве $\hat{N}(E, E)$:

- а) сложение коммутативно;
- б) сложение ассоциативно;

- в) умножение коммутативно;
- г) умножение ассоциативно;
- д) умножение дистрибутивно относительно сложения.

Впрочем, все эти свойства операций на множестве $\hat{N}(E, E)$ (за исключением коммутативности умножения) были нам уже известны из общей теоремы 3.1.

Наконец, заметим, что соответствие

$$k \rightarrow \hat{k}$$

между элементами множеств N и $\hat{N}(E, E)$ является взаимно-однозначным, причем оператор $\hat{1}$ оказывается единичным, так что

$$\hat{1}\hat{k} = \hat{k} \quad (4.5)$$

для любого $\hat{k} \in \hat{N}(E, E)$.

Фактически мы приходим к тому, что введенное нами множество операторов $\hat{N}(E, E)$ устроено точно так же как множество натуральных чисел. Поэтому естественно отождествить операторы из $\hat{N}(E, E)$ с соответствующими натуральными числами, а само множество $\hat{N}(E, E)$ — с множеством N . Начиная с этого момента мы будем считать такое отождествление произведенным и вместо \hat{k} будем всюду писать просто k .

§ 5. Оператор «минус». Целые отрицательные числа как произведения операторов

Введем теперь в рассмотрение оператор «минус», действие которого заключается в том, что он меняет направление любого отрезка из E на противоположное.

Пусть \overline{OA} — произвольный направленный отрезок из совокупности E . Тогда в соответствии с данным выше определением $-\overline{OA}$ будет обозначать отрезок, равный \overline{OA} по длине и направленный из точки O в противоположную сторону. Ясно, что двукратное применение оператора «минус» возвращает отрезок \overline{OA} на место:

$$-(-\overline{OA}) = \overline{OA}. \quad (5.1)$$

Очевидно также, что для любых двух отрезков $\overline{OA}, \overline{OB} \in E$ имеем

$$-(\overline{OA} + \overline{OB}) = (-\overline{OA}) + (-\overline{OB}), \quad (5.2)$$

т.е. оператор «минус» аддитивен.

Заметим теперь, что для любого $k \in N$ мы можем рассмотреть оператор $-k$, определив его как произведение (суперпозицию) оператора «минус» и оператора k , так что

$$(-k)\overline{OA} = -(k\overline{OA}), \quad \overline{OA} \in E. \quad (5.3)$$

Далее, нетрудно видеть, что операторы из N и оператор «минус» перестановочны между собой, откуда, учитывая ассоциативность умножения операторов, получаем операторное равенство

$$k(-p) = -(kp); \quad (5.4)$$

кроме того, в силу ассоциативности умножения операторов, очевидно, имеем

$$(-k)p = -(kp). \quad (5.5)$$

Наконец, ассоциативность умножения операторов, перестановочность оператора «минус» с операторами из N и соотношение (5.1) дают

$$(-k)(-p) = kp. \quad (5.6)$$

(Здесь $k, p \in N$.)

Итак, с помощью (5.3) мы фактически ввели в рассмотрение целые отрицательные числа, определив их как операторные произведения вида $-k$, где $k \in N$. Совокупность определенных таким образом целых отрицательных чисел мы будем обозначать через N^- (подобно тому, как мы это делали в § 1). Что касается соотношений (5.4)–(5.6), то они, очевидно, представляют собой уже знакомое нам «правило знаков», которое теперь удалось обосновать с помощью совершенно иных соображений чем в § 2.

§ 6. Множество Z как совокупность операторов

Поскольку наша цель — построение множества Z всех целых чисел, нам не обойтись без нуля. Определим действие оператора $\hat{0}$ на произвольный направленный отрезок $\overline{OA} \in E$ равенством

$$\hat{0}\overline{OA} = \overline{OO}, \quad (6.1)$$

где \overline{OO} — «нулевой» отрезок. Далее, нетрудно видеть, что

$$\hat{0}\overline{OA} = \overline{OO}, \quad (6.2)$$

и из (6.1) и (6.2) вытекает операторное равенство

$$-\hat{0} = \hat{0}.$$

Очевидно также, что $\hat{0}$ — аддитивный оператор.

Заметим далее, что, подобно тому как мы отождествили операторы из $\hat{N}(E, E)$ с натуральными числами, заданный на E оператор $\hat{0}$ можно отождествить с числом $0 \in N_0$. Всюду ниже мы будем считать такое отождествление произведенным и писать вместо $\hat{0}$ просто 0.

Как и в § 1, определим теперь множество целых чисел Z как объединение

$$N \cup \{0\} \cup N^-;$$

сейчас, однако, элементы множества Z понимаются как операторы, заданные на E .

На этом построение системы целых чисел заканчивается, поскольку специально давать определения тому, как взаимодействуют элементы операторных множеств N , $\{0\}$ и N^- при сложении и умножении, очевидно, не нужно.

Из теоремы 3.1 и результатов § 5 непосредственно следует, что все свойства сложения и умножения целых чисел при их операторной интерпретации оказываются точно такими же, как и при построениях, проведенных в §§ 1 и 2.

Возможность показать, что свойства вычитания и деления также совпадают при всех упомянутых подходах, предоставляется читателю.

ГЛАВА 4 МНОЖЕСТВО Q_+ ПОЛОЖИТЕЛЬНЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ

В этой главе предложена операторная интерпретация системы Q_+ положительных рациональных чисел. При таком подходе изложение становится компактным и, что немаловажно, школьные обозначения и школьная терминология (которые принято считать не вполне корректными) приходят в соответствие с обозначениями и терминологией, принятыми в высшей математике.

§ 1. Обратимые операторы и их свойства

Прежде чем приступить к построению множества Q_+ , изложим некоторые элементарные сведения, касающиеся обратимых операторов.

Итак, пусть, как и в § 3 гл. 3, X — множество, на котором задана коммутативная и ассоциативная операция сложения, и пусть теперь

$$L: X \rightarrow X$$

— взаимно-однозначное отображение множества X на себя. В этом случае мы будем также говорить, что на множестве X задан *обратимый оператор* L .

Изобразим графически действие оператора L с помощью стрелок (см. рис. 11).

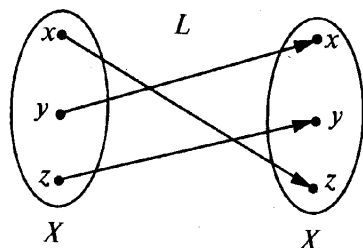


Рис. 11

Обращая направления стрелок на рис. 11, мы, очевидно, получим новое взаимно-однозначное отображение множества X на себя (см. рис. 12).

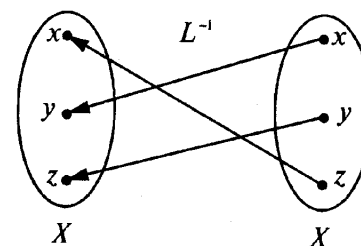


Рис. 12

Построенное таким способом отображение мы назовем *обратным* по отношению к L и обозначим через L^{-1} . В этом случае мы будем говорить также, что на X задан *оператор* L^{-1} , *обратный по отношению к L* . Ясно, что оператор L^{-1} (при заданном L) определяется единственным образом.

Замечание 1. Очевидно, что если L — обратимый оператор, заданный на X , то

$$LL^{-1} = I \quad (1.1)$$

и

$$L^{-1}L = I, \quad (1.1')$$

где I — единичный оператор (т.е. тождественное отображение множества X на себя). Нетрудно видеть также, что каждое из равенств (1.1), (1.1') влечет другое и полностью характеризует оператор L^{-1} .

Покажем, например, как из соотношения (1.1) вывести (1.1'). Имеем из (1.1) для любого $x \in X$:

$$LL^{-1}x = x.$$

Применим к обеим частям этого равенства оператор L^{-1} и обозначим

$$L^{-1}x = y;$$

в результате получим

$$L^{-1}Ly = y.$$

Однако если заставить x пробегать все X , то очевидно, y будет также пробегать все X . Тем самым последнее равенство оказывается эквивалентным (1.1'), т.е. мы вывели (1.1') из (1.1).

Замечание 2. Отметим также очевидное равенство

$$I^{-1} = I. \quad (1.2)$$

Приведем теперь четыре важные для дальнейшего утверждения.

Теорема 1.1. Пусть L — обратимый оператор, заданный на X . Тогда

$$(L^{-1})^{-1} = L. \quad (1.3)$$

Доказательство геометрически очевидно. ■

Теорема 1.2. Пусть L_1 и L_2 — обратимые операторы, заданные на X . Тогда их произведение также обратимо, причем

$$(L_1 L_2)^{-1} = L_2^{-1} L_1^{-1}. \quad (1.4)$$

Доказательство. В силу замечания 1 достаточно показать, что $(L_2^{-1} L_1^{-1})(L_1 L_2) = I$.

Однако последнее равенство сразу следует из (1.1') и ассоциативности умножения операторов. ■

Теорема 1.3. Пусть L_1 и L_2 — обратимые операторы, заданные на X , и пусть известно, что эти операторы коммутируют, т.е.

$$L_1 L_2 = L_2 L_1. \quad (1.5)$$

Тогда все четыре оператора $L_1, L_1^{-1}, L_2, L_2^{-1}$ коммутируют друг с другом.

Доказательство. Докажем, например, что

$$L_1 L_2^{-1} = L_2^{-1} L_1. \quad (1.6)$$

Прежде всего, из (1.5) имеем

$$L_1 L_2 x = L_2 L_1 x$$

(здесь x — произвольный элемент из X).

Применим к предыдущему равенству оператор L_2^{-1} , а затем положим $x = L_2^{-1} y$; в результате получим

$$L_2^{-1} L_1 L_2 L_2^{-1} y = L_2^{-1} L_2 L_1 L_2^{-1} y.$$

Очевидно, что это равенство можно переписать так:

$$L_2^{-1} L_1 (L_2 L_2^{-1}) y = (L_2^{-1} L_2) L_1 L_2^{-1} y,$$

откуда с учетом (1.1), (1.1') имеем

$$L_2^{-1} L_1 y = L_1 L_2^{-1} y.$$

Пусть теперь x пробегает все X , тогда y также пробегает все X ; тем самым из последнего равенства следует (1.6). Остальные утверждения теоремы доказываются аналогично. ■

Теорема 1.4. Пусть L — обратимый аддитивный оператор, заданный на X . Тогда оператор L^{-1} также аддитивен.

Доказательство. Имеем для любых $x, y \in X$:

$$LL^{-1}(x + y) = x + y,$$

$$L(L^{-1}x + L^{-1}y) = LL^{-1}x + LL^{-1}y = x + y.$$

Итак,

$$LL^{-1}(x + y) = L(L^{-1}x + L^{-1}y).$$

Теперь, применяя оператор L^{-1} к обеим частям последнего равенства, окончательно получаем

$$L^{-1}(x + y) = L^{-1}x + L^{-1}y,$$

что и требовалось установить. ■

§ 2. Определение положительного рационального числа

Будем теперь, как и в § 4 гл. 3, рассматривать множество E , состоящее из всех направленных отрезков, расположенных на прямой l и таких, что их начало совпадает с некоторой точкой O на этой прямой. Мы по-прежнему считаем, что отрезки из E складываются по правилу, сформулированному в § 2 гл. 3.

В предыдущей главе уже говорилось о том, что каждое $k \in \mathbb{N}$ можно рассматривать как оператор, увеличивающий длину отрезков из E в k раз и не меняющий их направления. Тем самым, как мы уже отмечали, 1 оказывается единичным оператором. Геометрически очевидно, что оператор k задает взаимно-однозначное отображение множества E на себя и, следовательно, существует оператор k^{-1} , также заданный на E . Нетрудно понять, что оператор k^{-1} сопоставляет каждому отрезку из E другой отрезок, также принадлежащий E , длина которого в k раз меньше, а направление совпадает с направлением исходного отрезка.

Далее, как мы знаем из предыдущей главы,

$$kp = pk, \quad (2.1)$$

каковы бы ни были операторы $k, p \in \mathbb{N}$. Отсюда в силу теоремы 1.3 следует, что

$$kp^{-1} = p^{-1}k \quad (2.2)$$

для любых операторов $k, p \in \mathbb{N}$.

Иными словами, справедлива следующая

Теорема 2.1. Все операторы, принадлежащие семейству

$$\{1; 2; 3; \dots; 2^{-1}; 3^{-1}; \dots\}, \quad (2.3)$$

коммутируют друг с другом.

Приведем теперь основное определение данной главы.

ОПРЕДЕЛЕНИЕ. Оператор, заданный на E и представимый в виде kp^{-1} (где $k, p \in N$), называется *положительным рациональным числом*.

Множество всех положительных рациональных чисел мы будем обозначать через Q_+ .

Подчеркнем, что положительным рациональным числом мы назвали не фиксированное произведение вида kp^{-1} , а оператор, представимый в виде такого произведения. Сейчас мы увидим, что представление операторов из Q_+ в виде kp^{-1} не единственно.

Теорема 2.2. Пусть $k_1, p_1, k_2, p_2 \in N$. Тогда операторное равенство

$$k_1 p_1^{-1} = k_2 p_2^{-1} \quad (2.4)$$

имеет место в том и только том случае, если

$$k_1 p_2 = k_2 p_1. \quad (2.5)$$

Доказательство.

Необходимость. Пусть (2.4) справедливо. Умножим это равенство слева на $p_1 p_2$. Пользуясь коммутативностью умножения операторов из семейства (2.3), а также всегда имеющей место ассоциативностью умножения операторов, получаем (2.5).

Достаточность. Пусть (2.5) справедливо. Умножим это операторное равенство слева на $p_1^{-1} p_2^{-1}$. Пользуясь коммутативностью и ассоциативностью умножения рассматриваемых операторов, приходим к (2.4). ■

Следствие. Пусть в условиях теоремы 2.2 $p_1 = p_2 = p$. Тогда в силу сократимости умножения в N , очевидно, из (2.4), (2.5) имеем

$$k_1 p^{-1} = k_2 p^{-1} \Leftrightarrow k_1 = k_2. \quad (2.6)$$

Замечание. Как мы знаем,

$$1^{-1} = 1.$$

Это обстоятельство дает нам возможность рассматривать натуральные числа как положительные рациональные. Действительно, пусть $k \in N$; имеем тогда

$$k = k \cdot 1^{-1} \in Q_+. \quad (2.7)$$

Представление (2.7) натурального числа из Q_+ , очевидно, не единственное. Более общее представление имеет вид

$$k = (kp) p^{-1}, \quad p \in N \quad (2.8)$$

(см. по этому поводу также следующий параграф).

§ 3. Дроби

Для наших целей будет полезно помимо операторных обозначений, уже применявшихся в § 2, ввести также привычные школьные обозначения, положив для натуральных k и p

$$kp^{-1} \equiv \frac{k}{p}. \quad (3.1)$$

Кроме того, нам потребуется следующее

ОПРЕДЕЛЕНИЕ. Выражение вида $\frac{k}{p}$, где $k, p \in N$, называется *положительной рациональной дробью*; при этом k называется *числителем* дроби, а p — *знаменателем* дроби.

Таким образом, положительная рациональная дробь $\frac{k}{p}$ — это одно из возможных выражений для соответствующего оператора (положительного рационального числа). Теорема 2,2 дает нам необходимое и достаточное условие для того, чтобы две дроби обозначали один и тот же оператор:

$$\frac{k_1}{p_1} = \frac{k_2}{p_2} \Leftrightarrow k_1 p_2 = k_2 p_1. \quad (3.2)$$

Замечание. Пусть $k, p \in N$. Мы будем писать $\frac{k}{p} \in Q_+$ (подобно тому как раньше писали $kp^{-1} \in Q_+$), понимая эту запись следующим образом: оператор, представимый в виде дроби $\frac{k}{p}$, принадлежит множеству Q_+ .

ОПРЕДЕЛЕНИЕ. Положительная рациональная дробь $\frac{k}{p}$ называется *несократимой*, если натуральные числа k и p взаимно просты.

Справедлива следующая важная

Теорема 3.1. Каждое число из Q_+ единственным образом представимо в виде несократимой дроби.

Доказательство этой теоремы сразу следует из существования и единственности разложения натурального числа (большого единицы) на простые множители. ■

Следствие. Пусть $\alpha \in Q_+$, и пусть $\frac{k}{p}$ — представление числа α в виде несократимой дроби. Тогда все остальные представления числа α в виде положительной рациональной дроби таковы:

$$\frac{2k}{2p}, \frac{3k}{3p}, \dots$$

§ 4. Сложение на множестве Q_+

При операторной интерпретации положительных рациональных чисел сложение не нуждается в специальном определении, поскольку сумма двух операторов была уже нами определена в самом общем случае.

Из сказанного, однако, еще не следует, что для любых $\alpha, \beta \in Q_+$ их сумма также представляет собой оператор из Q_+ (а не является каким-то оператором более общего вида, заданным на E).

Заметим, что если

$$\alpha = k_1 p_1^{-1}, \quad \beta = k_2 p_2^{-1} \quad (4.1)$$

(где k_1, k_2, p_1 и p_2 — натуральные числа), то имеют место очевидные операторные равенства

$$\begin{aligned} \alpha + \beta &= k_1 p_1^{-1} + k_2 p_2^{-1} = k_1 p_2 (p_1 p_2)^{-1} + k_2 p_1 (p_1 p_2)^{-1} = \\ &= (k_1 p_2 + k_2 p_1) (p_1 p_2)^{-1} \in Q_+. \end{aligned} \quad (4.2)$$

Итак, мы доказали, что сумма двух любых положительных рациональных чисел также является положительным рациональным числом.

Переходя в (4.2) к традиционным обозначениям (введенным в § 3), получаем известное из школы «правило сложения дробей»:

$$\frac{k_1}{p_1} + \frac{k_2}{p_2} = \frac{k_1 p_2 + k_2 p_1}{p_1 p_2}. \quad (4.2')$$

Замечание 1. При операторной интерпретации положительных рациональных чисел нам, очевидно, не требуется специально доказывать, что положительное рациональное число $\alpha + \beta$ не зависит от выбора представлений α и β в виде (4.1) (см. по этому поводу § 3 гл. 3).

Замечание 2. Очевидно также, что коммутативность и ассоциативность сложения чисел из Q_+ гарантируются нам общей операторной теоремой 3.1. из гл. 3.

§ 5. Отношение «меньше» и его связь со сложением

ОПРЕДЕЛЕНИЕ. Пусть α и β — числа из Q_+ . Скажем, что α меньше, чем β , если существует такое $\gamma \in Q_+$, что

$$\alpha + \gamma = \beta. \quad (5.1)$$

Замечание. Отношение «меньше» определено нами корректно, т.е. не зависит от выбора представлений вида (4.1) для чисел α и β . Действительно, пусть

$$\alpha = \alpha_1, \quad \beta = \beta_1.$$

Тогда из (5.1), очевидно, следует, что

$$\alpha_1 + \gamma = \beta_1$$

(см. по этому поводу также § 3 гл. 3).

Сформулируем теперь основной результат этого параграфа.

Теорема 5.1. Пусть k_1, p_1, k_2 и p_2 — натуральные числа. Тогда

$$\frac{k_1}{p_1} < \frac{k_2}{p_2} \Leftrightarrow k_1 p_2 < k_2 p_1. \quad (5.2)$$

Доказательство.

Необходимость. Пусть выполнено левое неравенство из (5.2), тогда, в силу данного выше определения для отношения «меньше» найдется $\gamma = \frac{r}{s}$ (где $r, s \in N$) такое, что

$$\frac{k_1}{p_1} + \frac{r}{s} = \frac{k_2}{p_2}.$$

Приводя дроби к общему знаменателю, получаем отсюда, что

$$\frac{(k_1 s + r p_1) p_2}{p_1 p_2 s} = \frac{k_2 p_1 s}{p_1 p_2 s},$$

и, значит, в силу следствия из теоремы 2.2

$$(k_1 s + r p_1) p_2 = k_2 p_1 s.$$

Из последнего равенства, пользуясь определением отношения «меньше» на множестве N_0 , имеем

$$k_1 p_2 s < k_2 p_1 s;$$

сокращая обе части этого неравенства на s , получаем требуемый результат.

Достаточность. Пусть выполнено правое неравенство из (5.2). Тогда существует такое натуральное m , что

$$k_1 p_2 + m = k_2 p_1.$$

Умножая это операторное равенство на $(p_1 p_2)^{-1}$, легко получаем, что

$$k_1 p_1^{-1} + m (p_1 p_2)^{-1} = k_2 p_2^{-1},$$

откуда и следует справедливость левого неравенства в (5.2). ■

Следствие. Пусть в условиях предыдущей теоремы $p_1 = p_2 = p$. Тогда из (5.2) и следствия из теоремы о монотонности умножения в N_0 , очевидно, вытекает, что

$$\frac{k_1}{p} < \frac{k_2}{p} \Leftrightarrow k_1 < k_2. \quad (5.3)$$

Замечание. С помощью теоремы 5.1 нетрудно показать, что отношение «меньше» на Q_+ является отношением строгого линейного порядка, т.е. антирефлексивно, транзитивно, асимметрично и связно (см. гл. 1, § 5).

После того как отношение «меньше» на Q_+ определено, можно определить также отношения «меньше или равно», «больше» и «больше или равно», подобно тому как это было сделано в гл. 1 для множества целых неотрицательных чисел.

Из теоремы 5.1 вытекает также следующая важная

Теорема 5.2.

- а) В множестве Q_+ отсутствует наименьший элемент;
- б) в множестве Q_+ отсутствует наибольший элемент;
- в) между любыми двумя элементами $\alpha, \beta \in Q_+$ содержится бесконечно много других элементов из Q_+ .

Доказательство. Утверждения а) и б) теоремы легко доказываются методом от противного; проведение соответствующих рассуждений предоставляется читателю.

Докажем утверждение в). Пусть $\alpha, \beta \in Q_+$ и пусть, для определенности,

$$\alpha < \beta. \quad (5.4)$$

Не ограничивая общности, мы, очевидно, можем считать, что положительные рациональные дроби, представляющие числа α и β , имеют одинаковые знаменатели:

$$\alpha = \frac{k_1}{p}, \quad \beta = \frac{k_2}{p};$$

при этом в силу (5.3), (5.4)

$$k_1 < k_2. \quad (5.5)$$

Теперь, пользуясь монотонностью сложения натуральных чисел, легко получаем из (5.5), что

$$2k_1 < k_1 + k_2 < 2k_2,$$

откуда в силу (5.3)

$$\frac{2k_1}{2p} < \frac{k_1 + k_2}{2p} < \frac{2k_2}{2p}.$$

Итак, мы получили, что положительное рациональное число $\gamma = \frac{k_1 + k_2}{2p}$ заключено между α и β .

Далее, с помощью аналогичной процедуры можно построить положительное рациональное число γ_1 , заключенное между α и γ , а также положительное рациональное число γ_2 , заключенное между γ и β . Продолжая процесс, получаем утверждение в) теоремы. ■

В заключение этого параграфа приведем еще две теоремы, аналогичные теоремам 5.1 и 5.2 из гл. 1.

Теорема 5.3 (монотонность сложения).

Пусть $\alpha, \beta, \gamma \in Q_+$. Тогда

$$\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma. \quad (5.6)$$

Теорема 5.4 (сократимость сложения).

Пусть $\alpha, \beta, \gamma \in Q_+$. Тогда

$$\alpha + \gamma = \beta + \gamma \Rightarrow \alpha = \beta. \quad (5.7)$$

Доказательства этих теорем сходны с доказательствами соответствующих теорем из гл. 1, и мы их опускаем.

§ 6. Вычитание на множестве Q_+

Определим теперь вычитание для чисел из Q_+ как операцию, обратную к сложению. Иными словами, для любых $\alpha, \beta, \gamma \in Q_+$ считаем

$$\alpha - \beta = \gamma \Leftrightarrow \alpha = \gamma + \beta. \quad (6.1)$$

Нетрудно видеть, что разность $\alpha - \beta$ существует в Q_+ в том и только том случае, когда

$$\beta < \alpha. \quad (6.2)$$

Из сократимости сложения следует также, что если разность $\alpha - \beta$ существует в Q_+ , то она определена однозначно.

Покажем, как вычисляется разность $\alpha - \beta$ в случае, когда заданы представления чисел α и β в виде рациональных дробей:

$$\alpha = \frac{k_1}{p_1}, \quad \beta = \frac{k_2}{p_2}, \quad (6.3)$$

где

$$k_2 p_1 < k_1 p_2 \quad (6.4)$$

в силу условия (6.2) и теоремы 5.1.

Пользуясь «правилом сложения дробей» из § 4, нетрудно проверить, что

$$\frac{k_1}{p_1} = \frac{k_1 p_2 - k_2 p_1}{p_1 p_2} + \frac{k_2}{p_2}, \quad (6.5)$$

откуда в силу (6.1) следует, что

$$\frac{k_1}{p_1} - \frac{k_2}{p_2} = \frac{k_1 p_2 - k_2 p_1}{p_1 p_2}, \quad (6.6)$$

т.е. мы пришли к известному из школы «правилу вычитания дробей».

Итак, если α и β представимы в виде (6.3), то их разность представима в виде

$$\alpha - \beta = \frac{k_1 p_2 - k_2 p_1}{p_1 p_2} \in Q_+.$$

(Независимость разности $\alpha - \beta$ от выбора представлений чисел α и β в виде положительных рациональных дробей следует из уже упоминавшейся единственности разности.)

Наконец, нетрудно проверить, что для вычитания в Q_+ справедливы утверждения, аналогичные теоремам 6.1–6.3 из гл. 1; проведение соответствующих выкладок предоставляется читателю.

§ 7. Умножение на множестве Q_+

Пусть α и β — два положительных рациональных числа. При операторной интерпретации множества Q_+ произведение этих чисел специально определять не нужно, ибо мы рассматриваем $\alpha\beta$ как обычное произведение операторов. Ситуация здесь по существу ничем не отличается от рассмотренной в § 4, где мы имели дело со сложением.

Однако для нас, как и в случае суммы $\alpha + \beta$, важно представить произведение $\alpha\beta$ в виде kp^{-1} (где $k, p \in N$), чтобы мы могли утверждать, что произведение двух операторов из Q_+ снова является оператором из Q_+ , а не каким-то оператором более общего

вида. Сделать это удастся в силу коммутативности умножения операторов из семейства

$$\{1; 2; 3; \dots; 2^{-1}; 3^{-1}\},$$

ассоциативности умножения (любых) операторов и теоремы 1.2, согласно которой

$$(pq)^{-1} = q^{-1}p^{-1}$$

для любых $p, q \in N$.

Действительно, пользуясь упомянутыми результатами, легко получаем, что если

$$\alpha = k_1 p_1^{-1}, \quad \beta = k_2 p_2^{-1}, \quad (7.1)$$

то

$$\alpha\beta = (k_1 p_1^{-1})(k_2 p_2^{-1}) = (k_1 k_2)(p_1 p_2)^{-1} \in Q_+. \quad (7.2)$$

Переходя здесь к традиционным обозначениям, приходим к школьному «правилу умножения дробей»:

$$\frac{k_1}{p_1} \cdot \frac{k_2}{p_2} = \frac{k_1 k_2}{p_1 p_2}. \quad (7.2')$$

З а м е ч а н и е 1. При операторной интерпретации положительных рациональных чисел нам, очевидно, не требуется специально доказывать, что произведение $\alpha\beta$ не зависит от выбора представлений для α и β в виде дробей.

З а м е ч а н и е 2. Из теоремы 3.1 гл. 3, а также теорем 1.4 и 2.1 этой главы вытекает, что умножение в Q_+ коммутативно, ассоциативно и дистрибутивно относительно сложения. Дистрибутивность умножения относительно вычитания вытекает из дистрибутивности умножения относительно сложения и определения вычитания. Монотонность умножения в Q_+ сразу следует из определения отношения «меньше» и дистрибутивности умножения относительно сложения. Наконец, сократимость умножения в Q_+ следует из монотонности умножения.

§ 8. Деление на множестве Q_+

Прежде чем давать определение операции деления на множестве положительных рациональных чисел, установим следующий вспомогательный результат.

Лемма 8.1. Пусть $kp^{-1} \in Q_+$. Тогда

$$(kp^{-1})^{-1} = pk^{-1} \in Q_+. \quad (8.1)$$

Доказательство. Заметим, что оператор kp^{-1} обратим, так как представляет собой произведение двух обратимых операторов. Имеем поэтому в силу теорем 1.2 и 1.1

$$(kp^{-1})^{-1} = (p^{-1})^{-1} k^{-1} = kp^{-1},$$

что и требовалось установить. ■

Теперь мы подготовлены к тому, чтобы определить операцию деления на множестве положительных рациональных чисел.

ОПРЕДЕЛЕНИЕ. Делением на множестве Q_+ называется операция, обратная умножению.

Итак, пусть $\alpha, \beta, \gamma \in Q_+$. Тогда в силу данного выше определения

$$\alpha : \beta = \gamma \Leftrightarrow \alpha = \gamma\beta. \quad (8.2)$$

Заметим, однако, что

$$\alpha = \gamma\beta \Leftrightarrow \alpha\beta^{-1} = \gamma.$$

Отсюда и из (8.2), очевидно, следует, что

$$\alpha : \beta = \alpha\beta^{-1}. \quad (8.3)$$

В частности, из (8.3) вытекает, что деление на множестве Q_+ всегда осуществимо и притом единственным образом.

Пусть теперь

$$\alpha = \frac{k_1}{p_1}, \quad \beta = \frac{k_2}{p_2},$$

где k_1, k_2, p_1 и p_2 — натуральные числа. Тогда с учетом (8.1) имеем из (8.3):

$$\frac{k_1}{p_1} : \frac{k_2}{p_2} = \frac{k_1 p_2}{k_2 p_1}, \quad (8.4)$$

т.е. мы пришли к хорошо известному школьному «правилу деления дробей».

Замечание 1. Пусть $p \in N$. Тогда имеем из (8.4):

$$1 : p = \frac{1}{1} : \frac{p}{1} = \frac{1}{p} = p^{-1}. \quad (8.5)$$

Более того, если $k, p \in N$, то (8.4) дает

$$1 : \frac{k}{p} = \frac{1}{1} : \frac{k}{p} = \frac{p}{k} = \left(\frac{k}{p}\right)^{-1} \quad (8.6)$$

(см. лемму 8.1). Тем самым употребление отрицательной степени -1 при обозначении обратного оператора согласуется с общепринятым обозначением:

$$1 : a = a^{-1}.$$

Замечание 2. В заключение этого параграфа отметим, что в рамках операторного подхода расширение множества Q_+ до множества Q всех рациональных чисел может быть проведено точно так же, как это было сделано в предыдущей главе в случае множеств N_0 и Z . Чисто алгебраический подход к построению множества рациональных чисел превосходно изложен в [13].

§ 9. Соизмеримость и мера с операторной точки зрения

Рассмотрим теперь процедуру измерения величин, опираясь на построения предыдущих параграфов.

Нам будет удобно по-прежнему иметь дело с отрезками, так что наши измерения будут измерениями длины. Однако с тем же успехом мы могли бы измерять площади, объемы или веса каких-нибудь иных, подходящих для этого объектов (см. по этому поводу [12, с. 28]).

Измеряя отрезки, мы совершенно не обязаны обращать внимание на их направление и расположение в пространстве. Однако для того, чтобы связать процедуру измерения с операторной интерпретацией чисел из Q_+ , мы ограничимся вначале измерениями отрезков из системы E , а затем укажем, как перейти к общему случаю.

Итак, пусть \overline{OA} — произвольный ненулевой отрезок, принадлежащий системе E . Рассмотрим теперь отрезок $\overline{OB} \in E$ такой, что

$$\overline{OB} = \alpha \overline{OA}, \quad \alpha \in Q_+. \quad (9.1)$$

Равенство (9.1), очевидно, эквивалентно следующему:

$$\overline{OA} = \beta \overline{OB}, \quad \beta \in Q_+, \quad (9.2)$$

где $\beta = \alpha^{-1}$.

ОПРЕДЕЛЕНИЕ 1. Ненулевые отрезки $\overline{OA}, \overline{OB} \in E$ такие, что выполнено (9.1) при некотором $\alpha \in Q_+$, называются *соизмеримыми*.

Замечание 1. Из (9.1), очевидно, следует, что отрезки \overline{OA} и \overline{OB} направлены в одну и ту же сторону.

Замечание 2. Пусть \overline{OA} , \overline{OB} и \overline{OC} — ненулевые отрезки из системы E . Нетрудно видеть, что если \overline{OA} соизмерим с \overline{OB} , а \overline{OB} соизмерим с \overline{OC} , то \overline{OA} соизмерим с \overline{OC} . Иными словами, отношение соизмеримости на множестве E транзитивно.

Справедлива следующая

Лемма 9.1. Пусть \overline{OA} — ненулевой отрезок из системы E . Пусть, далее,

$$\overline{OB_1} = \alpha_1 \overline{OA}, \quad \overline{OB_2} = \alpha_2 \overline{OA}, \quad (9.3)$$

где $\alpha_1, \alpha_2 \in Q_+$. Тогда отрезок $\overline{OB_1}$ короче отрезка $\overline{OB_2}$ в том и только том случае, если $\alpha_1 < \alpha_2$.

Доказательство. Представим числа α_1 и α_2 в виде положительных рациональных дробей:

$$\alpha_1 = \frac{k_1}{p_1}, \quad \alpha_2 = \frac{k_2}{p_2}.$$

Тогда из (9.3) имеем

$$\begin{aligned} \overline{OB_1} &= \frac{k_1}{p_1} \overline{OA} = k_1 p_2 \left(\frac{1}{p_1 p_2} \overline{OA} \right), \\ \overline{OB_2} &= \frac{k_2}{p_2} \overline{OA} = k_2 p_1 \left(\frac{1}{p_1 p_2} \overline{OA} \right). \end{aligned}$$

Из двух последних равенств геометрически очевидно, что $\overline{OB_1}$ короче $\overline{OB_2}$ в том и только том случае, если

$$k_1 p_2 < k_2 p_1.$$

Однако последнее неравенство равносильно тому, что $\alpha_1 < \alpha_2$ (см. теорему 5.1). Лемма доказана. ■

Следствие. Пусть $\alpha_1 \overline{OA} = \alpha_2 \overline{OA}$. Тогда $\alpha_1 = \alpha_2$.

Учитывая результат леммы 9.1, введем теперь следующее

ОПРЕДЕЛЕНИЕ 2. Пусть $\overline{OB} = \alpha \overline{OA}$, где $\alpha \in Q_+$, \overline{OA} — ненулевой отрезок из системы E . Тогда скажем, что α есть значение длины (меры) отрезка \overline{OB} при единичном отрезке \overline{OA} . Записывать это будем так:

$$m_{OA}(\overline{OB}) = \alpha. \quad (9.4)$$

Замечание. В случае, если единичный отрезок \overline{OA} считается раз и навсегда фиксированным, мы будем говорить просто о длине α отрезка \overline{OB} и писать:

$$m(\overline{OB}) = \alpha. \quad (9.4')$$

Введенная нами мера для отрезков из E , соизмеримых с \overline{OA} , обладает следующим важным свойством, которое называют *аддитивностью*. А именно, пусть $\overline{OB_1}$ и $\overline{OB_2}$ — два отрезка, принадлежащие системе E и соизмеримые с \overline{OA} . Тогда имеет место равенство

$$m_{OA}(\overline{OB_1} + \overline{OB_2}) = m_{OA}(\overline{OB_1}) + m_{OA}(\overline{OB_2}). \quad (9.5)$$

Действительно, выражая отрезки $\overline{OB_2}$ и $\overline{OB_1}$ через \overline{OA} в виде (9.3) и пользуясь определением суммы операторов из Q_+ , имеем

$$\overline{OB_1} + \overline{OB_2} = \alpha_1 \overline{OA} + \alpha_2 \overline{OA} = (\alpha_1 + \alpha_2) \overline{OA},$$

откуда и следует (9.5).

Замечание. Подчеркнем, что в (9.5) отрезки $\overline{OB_1}$ и $\overline{OB_2}$ имеют одно и то же направление (см. (9.3)), поэтому их сумму $\overline{OC} = \overline{OB_1} + \overline{OB_2}$ можно рассматривать как объединение двух не налегающих друг на друга отрезков $\overline{OB_1}$ и $\overline{B_1C}$, где отрезок $\overline{B_1C}$ равен отрезку $\overline{OB_2}$. Это обстоятельство позволяет дать очевидную теоретико-множественную интерпретацию равенству (9.5) в важном частном случае, когда отрезки $\overline{OB_1}$ и $\overline{OB_2}$ кратны \overline{OA} (т.е. когда в (9.3) α_1 и α_2 — натуральные числа). Действительно, в этом случае меры всех отрезков, участвующих в (9.5), можно рассматривать как численности множеств, составленных из не налегающих друг на друга отрезков, равных \overline{OA} .

Перейдем теперь к рассмотрению другого важного свойства меры, проявляющегося при переходе от исходной единицы измерения к новой.

Итак, возьмем в качестве новой единицы измерения отрезок $\overline{OA_1} \in E$ такой, что

$$\overline{OA} = \gamma \overline{OA_1}, \quad \gamma \in Q_+. \quad (9.6)$$

Тогда, пользуясь определением произведения операторов из Q_+ , в силу (9.1), (9.6) имеем

$$\overline{OB} = \alpha \gamma \overline{OA_1},$$

откуда

$$m_{OA_1}(\overline{OB}) = m_{OA}(\overline{OB}) \cdot m_{OA_1}(\overline{OA}). \quad (9.7)$$

Это свойство меры отрезков из E называется *мультипликативностью*.

Замечание. В случае, когда меры $m_{OA}(\overline{OB})$ и $m_{OA_1}(\overline{OB})$ — натуральные числа, равенство (9.7) допускает, подобно (9.5), очевидную теоретико-множественную интерпретацию, на которой мы не будем останавливаться.

В заключение этого параграфа покажем, что введенные нами определения соизмеримости и меры легко могут быть обобщены на случай отрезков, произвольным образом ориентированных в пространстве.

А именно, примем

ОПРЕДЕЛЕНИЕ 1'. Два произвольных отрезка $\overline{CC_1}$ и $\overline{DD_1}$ соизмеримы, если они соответственно равны двум соизмеримым отрезкам из системы E .

Нетрудно проверить, что это определение равносильно следующему.

ОПРЕДЕЛЕНИЕ 1''. Два произвольных отрезка $\overline{CC_1}$ и $\overline{DD_1}$ соизмеримы, если существует отрезок, укладывающийся целое число раз в каждом из них.

Что касается меры отрезков, произвольным образом ориентированных в пространстве, то ее проще всего определить следующим образом.

ОПРЕДЕЛЕНИЕ 2'. Пусть $\overline{CC_1}$ — произвольный отрезок, $\overline{OA} \in E$. Положим

$$m_{OA}(\overline{CC_1}) = \alpha, \quad (9.8)$$

если отрезок $\overline{CC_1}$ равен отрезку $\overline{OB} \in E$ такому, что

$$\overline{OB} = \alpha \overline{OA}, \quad \alpha \in Q_+.$$

Очевидно, что при таком определении меры ее мультипликативность сохраняется, т.е.

$$m_{OA_1}(\overline{CC_1}) = m_{OA}(\overline{CC_1}) \cdot m_{OA_1}(\overline{OA}) \quad (9.9)$$

(все меры предполагаются существующими). Действительно, из определения 2' вытекает, что

$$m_{OA}(\overline{CC_1}) = m_{OA}(\overline{OB}),$$

$$m_{OA_1}(\overline{CC_1}) = m_{OA_1}(\overline{OB});$$

отсюда и из (9.7) следует (9.9).

Что касается аддитивности меры, то она, очевидно, тоже сохраняется, но в следующей видоизмененной форме.

Пусть \overline{CD} — произвольный отрезок, C_1 — точка, принадлежащая этому отрезку и не совпадающая ни с одним из его концов. Тогда

$$m(\overline{CD}) = m(\overline{CC_1}) + m(\overline{C_1D}) \quad (9.10)$$

(меры всех отрезков предполагаются существующими).

З а м е ч а н и е 1. Мы специально исключили из рассмотрения тот случай, когда $C_1 = C$ или $C_1 = D$, чтобы не иметь дело с мерой нулевого отрезка. При дальнейшем развитии теории эту меру следовало бы положить равной нулю.

З а м е ч а н и е 2. В заключение отметим, что далеко не все отрезки соизмеримы друг с другом. Например можно показать, что диагональ квадрата несоизмерима с его стороной. С различными геометрическими доказательствами этого факта можно ознакомиться по книгам [7], [12].

ЛИТЕРАТУРА

1. Виленкин Н.Я. и др. Математика, М.: Просвещение, 1977. 351 с.
2. Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел. Ч. I. Числа. М.: Просвещение, 1974. 383 с.
3. Мерзон А.Е., Добротворский А.С., Чекин А.Л. Пособие по математике для студентов факультетов начальных классов. М., 1998. 445 с.
4. Добротворский А.С., Ковригина Л.П. и др. Пособие по математике для студентов факультетов начальных классов. Ч. I. М., 1989. 215 с.
5. Соминский И.С. Метод математической индукции // Популярные лекции по математике. Вып. 3. М.: Наука, 1965. 56 с.
6. Верещагин Н.К., Шень А. Начала теории множеств. М., 1999. 127с.
7. Колмогоров А.Н. Математика — наука и профессия. М.: Наука, 1988. 287 с.
8. Клейн Ф. Элементарная математика с точки зрения высшей. Т. I. Арифметика, алгебра, анализ. М.: Наука, 1987. 431 с.
9. Фройденваль Г. Математика как педагогическая задача. М.: Просвещение, 1982. 208 с.
10. Гарднер М. От мозаик Пенроуза к надежным шифрам. М.: Мир, 1993. 416 с.
11. Нивен А. Числа рациональные и иррациональные. М.: Мир, 1966. 198 с.
12. Дубнов Я.С. Измерение отрезков. М.: Физматиз, 1962. 100 с.
13. Ван дер Варден Б.Л. Алгебра. М.: Наука, 1976. 648 с.
14. Кановой В.Г. Аксиома выбора и аксиома детерминированности. М.: Наука, 1984. 65 с.
15. Нечаев В.И. Числовые системы. М.: Просвещение, 1975. 199 с.
16. Проскуряков И.В. Числа и многочлены. М.: Изд-во Академии педагогических наук РСФСР, 1949. 283 с.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- Декартово произведение множеств 9
- Оператор
- аддитивный 51
 - единичный 53
 - обратимый 58
 - обратный 59
- Отношение на множестве
- антирефлексивное 14
 - асимметричное 14
 - связное 14
 - строгого линейного порядка 15
 - транзитивное 14
- Отображение 5
- Правило знаков
- при умножении 46
 - сложения направленных отрезков 48
- Система
- Пeano P 25
 - направленных отрезков E 53
- Численность множества 9