УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИИ Б. Н. ЕЛЬЦИНА

С.А. Ануфриенко

АЛГЕБРА 10

Учебное пособие

Екатеринбург
2025

УДК
ББК

Подготовлено на кафедре математики СУНЦ УрФУ

Рецензенты: *А. В. Осипов,* зав. сектором топологии Отдела алгебры и топологии ИММ УрО РАН, д.ф.-м.н.,
С. Э. Нохрин, доцент кафедры математического анализа департамента математики, механики и компьютерных наук ИЕНиМ УрФУ, канд.ф.-м.н.

Алгебра 10: учеб. пособие / С. А. Ануфриенко.— : Изд-во , 2025. 214с.

В книгу включены разделы программы по алгебре, которые изучаются в десятых математических классах СУНЦ УрФУ: построение натуральных чисел, теория сравнений, введение в теорию множеств, кольцо многочленов одной и нескольких переменных, элементарное (без производной) исследование свойств числовых функций, тригонометрия, теория решений уравнений, неравенств и систем.

Учебное пособие предназначено для учащихся СУНЦ УрФУ, старшеклассников и учителей математики.

ISBN

Оглавление

Предисловие и система обозначений

Эта книга является первой частью курса алгебры и начал математического анализа для классов с углубленным изучением математики. Материал, собранный в ней, основан на лекциях, прочитанных в десятых специализированных классах СУНЦ УрФУ. Сборник задач для практических занятий по алгебре и началам математического анализа был опубликован ранее.

Учебный материал разбит на несколько глав, каждая глава — на параграфы. Нумерация утверждений двойная: номер параграфа и номер утверждения в нем. В редких случаях возникают ссылки на утверждения других глав, в этом случае явно указывается еще и номер главы.

Кратко о содержании книги. Геометрия в десятых физико-математических классах СУНЦ УрФУ строится аксиоматически на основании системы аксиом Гильберта. В этом же духе, только уже используя аксиомы Пеано, вводятся в первой главе этой книге натуральные числа, определяются операции и порядок на $\mathbb{N}$, доказываются их свойства, с помощью которых в дальнейшем (уже в одиннадцатом классе) развивается теория других числовых множеств: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Завершается глава изучением свойств сравнений по модулю, доказательством теорем Ферма и Эйлера, применением сравнений в решении диофантовых уравнений.

Вторая глава посвящена теории множеств — одной из самых молодых математических дисциплин. Понятие множества оказалось настолько общим и полезным, что многие сложные конструкции алгебры, геометрии и математического анализа получили ясное теоретико-множественное описание. Это сделало теорию множеств универсальным математическим языком. Кроме изучения основных теоретико-множественных операций, в этой главе мы поговорим о соответствиях, выведем основные комбинаторные формулы, докажем несколько теорем Кантора о бесконечных множествах и кардиналах.

В третьей главе изучаются основные свойства числовых функций и их графиков, вводится понятие обратной функция к данной и доказывается обратимость всех строго монотонных функций. Большая часть этой главы посвящена многочленам одной и нескольких переменных. Кроме классических результатов (теорем Безу и Виета, схема Горнера), мы научимся находить все рациональные корни многочленов с целыми коэффициентами и представлять произвольный симметрический многочлен в виде многочлена от элеметарных симметрических. В четвертой главе определяются основные тригонометрические функции и доказываются более полусотни тригонометрических формул.

Пятая глава посвящена различным способам преобразований уравнений и систем уравнений.

Договоримся о некоторых математические обозначениях и сокращениях:

$\forall$ — квантор всеобщности, читается «для всех» или «для любых», появился из английского выражения for **A**ll, выделенную букву в котором отразили относительно горизонтальной оси;

$\exists$ — квантор существования, читается «существует», появился от английского слова **E**xist, выделенную букву в котором отразили относительно вертикальной оси;

$\exists!$ — частный случай квантора существования, читается «существует и единственный»;

$\Rightarrow$ — следует;

$\Leftrightarrow$ — тогда и только тогда;

$\&$ — знак конъюнкции, читается как «и»;

$\vee$ — знак дизъюнкции, читается как «или»;

$:$ или $|$ — в записи утверждения является сокращением для «таких, что»;

$\blacksquare$ — конец доказательства;

О/п или о/п — сокращение для «От противного» или «от противного», в зависимости от места в предложении;

$\lightning$ — противоречие;

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ — соответственно множества всех натуральных, целых, рациональных и вещественных (или действительных) чисел;

$\in$ — знак принадлежности;

$\subseteq$ — знак включения, ставят между множествами в случае, когда множество слева от знака содержится во множестве справа от него, допускаются цепочки, например $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$;

$\{x : P(x)\}$ — множество всех таких элементов x, для которых выполняется свойство $P(x)$;

$\cap$ — пересечение множеств;

$\cup$ — объединение множеств;

$\sum$ — сумма чисел;

$\prod$ — произведение чисел или множеств.

В следующем примере использования кванторов внимательный читатель распознает аксиому Евклида: $\forall B \forall a \exists\, !b : B \in b \;\&\; b \parallel a$.

Критические замечания и конструктивные предложения просьба отправлять по электронной почте `math-lyceum-urfu@mail.ru`.

Глава 1

Введение в теорию чисел

1.1. Аксиомы Пеано

Во многих математических теориях существуют первоначальные, или неопределяемые, понятия и отношения. Причина, по которой невозможно определить абсолютно все понятия, которые мы используем, состоит в следующем. Определяя некоторое понятие через другие, необходимо следить за тем, чтобы это понятие не было определено само через себя. Иначе может возникнуть определение, которое в математике называется «порочным кругом» и считается недопустимым. Вот несколько примеров таких «определений»: «ромб — это ромб», «угол имеет величину 90°, если его стороны перпендикулярны; перпендикулярными прямыми называются прямые, угол между которыми 90°» и т.д. Каждое определение в математике — это замаскированная цепочка определений, каждое звено которой является переходом к определению более простого понятия. Поскольку замыкать цепь нельзя, и иметь дело с бесконечной цепочкой определений крайне неудобно, то каждый нижний уровень цепи является неопределяемым понятием. Так, давая строгое определение ромба, можно через определение замкнутой простой ломаной и ее звена дойти до двух не определяемых в геометрии понятий — точки и прямой. От первоначальных понятий требуется очень многое: при небольшом количестве они должны обеспечить все многообразие понятий данной математической теории. Похожая иерархия возникает среди отношений, которые устанавливают различные связи между понятиями. Так, отношение параллельности на множестве прямых, определяется через неопределяемое отношение «принадлежать» или «содержаться». Все необходимые для развития теории свойства неопределяемых понятий и неопределяемых отношений описываются с помощью системы аксиом. Аксиомы — это утверждения о

неопределяемых понятиях, которые мы заранее (т.е. по определению) считаем истинными. Так, по Гильберту[1], в геометрии существуют три неопределяемых понятия и три неопределяемых отношения, которые описываются двадцатью аксиомами.

При построении теории натуральных чисел мы позаимствуем из теории множеств понятие множества (которое является там неопределяемым), понятия отношения и отображения. Все эти понятия подробно обсуждаются в следующей главе. Единственным неопределяемым отношением в теории натуральных чисел является отношение «следовать за». Договоримся, что запись $a' = b$ означает, что элемент b следует за элементом a. Наиболее удачную систему аксиом, описывающую это отношение, предложили Дедекинд (1888) и Пеано[2] («Основания арифметики, изложенные новым способом», 1889). Следующее определение является небольшой модификацией системы Пеано. В этом параграфе, чтобы дать возможность привыкнуть к обозначениям, в квадратных скобках будем приводить сокращенные версии аксиом и утверждений с использованием кванторов.

Определение. *Множеством натуральных чисел называется множество* $\mathbb{N}$, *для некоторых элементов которого задано отношение «следовать за», которое удовлетворяет следующим аксиомам:*

П1. Существует в $\mathbb{N}$ *элемент (который называется единицей), который не следует ни за каким другим* $[\exists 1 \in \mathbb{N} : \forall a \in \mathbb{N} \Rightarrow a' \neq 1]$.

П2. Для каждого элемента из $\mathbb{N}$ *определен следующий, причем только один* $[\forall a \in \mathbb{N}\ \exists!\ a']$.

П3. Любой элемент из $\mathbb{N}$ *может следовать не более чем за одним элементом из* $\mathbb{N}$ $[\forall a, b, c \in \mathbb{N}$ *из условия* $(c = a' \,\&\, c = b') \Rightarrow a = b]$.

П4 (аксиома полной индукции). Любое множество $M \subseteq \mathbb{N}$, *которое одновременно содержит единицу и замкнуто относительно взятия следующего, совпадает с* $\mathbb{N}$ $[\forall M \subseteq \mathbb{N}$ *из двух условий (а)* $1 \in M$ *& (б)* $\forall a \in M \Rightarrow a' \in M$ *следует, что* $M = \mathbb{N}]$.

Натуральным числом называется произвольный элемент из $\mathbb{N}$. Выведем из аксиом Пеано несколько простых утверждений.

[1] Давид Гильберт (1862–1943) — немецкий математик, создатель важнейшего математического центра в Гёттингене; основные исследования относятся к теории инвариантов, интегральному исчислению, функциональному анализу, математической логике; в книге «Основания геометрии» (1899) дал полную систему аксиом евклидовой геометрии.

[2] Джузеппе Пеано (1858–1932) — итальянский математик, был одним из основателей математической логики и теории множеств; построил непрерывную кривую, целиком заполняющую квадрат (кривая Пеано).

Теорема 1.1. *Для любых двух различных натуральных чисел выполняется, что следующие за ними также различны* $[\forall a, b \in \mathbb{N}(a \neq b) \Rightarrow a' \neq b']$.

Доказательство. О/п: предположим, что $a' = b'$. Тогда по П3 получим, что $a = b$. $\lightning$.

■

Теорема 1.2. *Для любого натурального числа выполняется: оно не может быть равно своему следующему* $[\forall a \in \mathbb{N} \Rightarrow a \neq a']$.

Доказательство. Обозначим через $M = \{a \in \mathbb{N} : a \neq a'\}$. Из П1 сразу следует, что $1 \in M$, поэтому свойство (а) аксиомы П4 выполнено, проверим (б). Предположим, что $a \in M$, тогда по определению множества M , имеем $a \neq a'$. Применяя предыдущую теорему, получим $a' \neq (a')'$. Последнее означает, что $a' \in M$ и свойство (б) доказано. Теперь из П4 следует, что $M = \mathbb{N}$.

■

Теорема 1.3. *Любое натуральное число, за исключением единицы, следует за другим натуральным числом* $[\forall a \in \mathbb{N}(a \neq 1)\ \exists k \in \mathbb{N} : k' = a]$.

Доказательство. Пусть $M = \{a \in \mathbb{N} : a = 1$ или $a = k'$ для некоторого $k \in \mathbb{N}\}$. Сразу из определения этого множества следует, что $1 \in M$, поэтому свойство (а) аксиомы П4 выполнено, проверим (б). Если $a \in M$, то $a' \in M$, поскольку $k = a$ — искомое. Из П4 следует, что $M = \mathbb{N}$.

■

Далее рассмотрим несколько примеров конкретных множеств и отношения «следовать за» на них, которые удовлетворяют или не удовлетворяют аксиомам Пеано.

П р и м е р 1. Пусть $N = \{a, b\}$ и $a' = b$, $b' = a$. Это множество не удовлетворяет П1.

П р и м е р 2. Пусть $N = \{1, a, b\}$ и $1' = a$, $a' = b$, $b' = a$. Для этого множества выполняются первые две аксиомы, но не выполняется П3.

П р и м е р 3. Путь N содержит все конечные наборы из единиц. Взятие следующего к любому из таких наборов — это приписывание одной единицы слева к такому набору. Нетрудно понять, что все аксиомы П1–П4 для такого множества выполняются. Это множество N называется множеством натуральных чисел, записанных в унарной системе счисления.

П р и м е р 4. Рассмотрим множество $C_0 = \{0, 1, \ldots, 9\}$ — десятиэлементное множество, состоящее из всех десятичных цифр. Определим для

цифр правило взятия следующего десятью соотношениями: $0' = 1$, $1' = 2$, $2' = 3, \ldots,$ $9' = 10$. Теперь в качестве N рассмотрим все такие конечные наборы цифр, у которых старшая (т.е. крайняя левая) цифра не равна нулю. Для любого из таких наборов $ab\ldots pq$ следующий за ним определяется так:

$$ab\ldots pq' = \begin{cases} ab\ldots p(q)', & \text{если} \quad q \neq 9, \\ (ab\ldots p)'0, & \text{если} \quad q = 9. \end{cases}$$

Нетрудно понять, что все аксиомы П1–П4 для такого множества выполняются. Это множество N называется множеством натуральных чисел, записанных в десятичной системе счисления.

Договоримся, что далее под $\mathbb{N}$ будем понимать множество с определенным отношением «следовать за» из предыдущего примера.

П р и м е р 5. Интересный пример множества натуральных чисел средствами теории множеств построили Фреге[3] и Рассел[4]. В этом примере $1 = \{\varnothing\}$ и для каждого уже определенного числа n следующее за ним определяется так: $n' = S(n) = n \cup \{n\}$. Первые числа получаются такими:

$$1 = \{\varnothing\}, \quad 2 = \Big\{\varnothing, \{\varnothing\}\Big\}, \quad 3 = \Big\{\varnothing, \{\varnothing\}, \Big\{\varnothing, \{\varnothing\}\Big\}\Big\} \qquad \text{и т.д.}$$

Минимальное множество, содержащее $1 = \{\varnothing\}$ и замкнутое относительно $S(n)$ (оно существует благодаря одной из аксиом Цермело-Френкеля), и будет искомым множеством, построенным только из пустого множества.

П р и м е р 6. Следующий пример построим в предположении, что вы знаете, что такое координатная плоскость xOy и множество целых чисел $\mathbb{Z}$ (можно вернуться к этому примеру после построения $\mathbb{R}$ в одиннадцатом классе, определений $\mathbb{Z}$ в этой главе и декартового произведения множеств — в следующей). На плоскости xOy выберем множества $M = \{(a, 0) : a \in \mathbb{N}\}$ и $L = \{(0, k) : k \in \mathbb{Z}\}$. Пусть теперь $\widetilde{N} = M \cup L$, определим отношение «следовать за» на $\widetilde{N}$ так: $(a, 0)' = (a + 1, 0)$ и $(0, k)' = (0, k + 1)$. Тогда элемент $(1, 0)$ будет единицей в этом множестве и аксиомы П2 и П3 также будут выполняться, но П4 — нет, поскольку множество M удовлетворяет свойствам (а) и (б), но $M \neq \widetilde{N}$.

[3]Фридрих Фреге (1848–1925) — немецкий математик; основные результаты получил в математической логике; ввел понятие квантора.

[4]Бертран Рассел (1872–1970) — английский математик и философ, сформулировал один из парадоксов теории множеств, что привело его к построению аксиоматической теории множеств; получил в 1950 году Нобелевскую премию по литературе.

1.2. Сложение на множестве натуральных чисел

Операцией $*$ на множестве X называется правило[5], по которому каждой упорядоченной паре (a, b) элементов $a, b \in X$ ставится в соответствие единственный элемент (который обозначается $a * b$) этого же множества. Такие операции называются *бинарными* операциями, поскольку действуют на упорядоченные пары элементов (унарные, тернарные и другие операции, которые действуют на иное количество элементов, не появятся в ближайших параграфах). Нетрудно заметить, что минус (или вычитание) не будет операцией на $\mathbb{N}$, поскольку упорядоченной паре $(1, 2)$ не будет поставлено в соответствие никакое натуральное число (впрочем, на $\mathbb{Z}$ вычитание уже является операцией).

Определение. *Сложением на* $\mathbb{N}$ *называется операция* $+$, *которая удовлетворяет следующим свойствам (которые называются аксиомами сложения):*

C1. $\forall a \in \mathbb{N} \Rightarrow a + 1 = a'$;

C2. $\forall a, b \in \mathbb{N} \Rightarrow a + b' = (a + b)'$.

Из этого определения почти сразу следует, что $2 + 2 = 4$. Действительно, по C1 сначала получим $2 + 2 = 2 + 1'$, затем C2 дает $2 + 1' = (2 + 1)'$. Останется использовать C1 и определение следующего на цифрах (пример 4 предыдущего параграфа): $(2 + 1)' = (2')' = 3' = 4$. В следующей теореме доказывается чуть более общий результат — свойство *ассоциативности* сложения натуральных чисел.

Теорема 2.1. *Для любых* $a, b, c \in \mathbb{N}$ *выполняется* $(a+b)+c = a+(b+c)$.

Доказательство. Определим через

$$M = \{c \in \mathbb{N} : \forall a, b \in \mathbb{N} \Rightarrow (a + b) + c = a + (b + c)\}$$

и докажем, что $M = \mathbb{N}$.

а) применяя последовательно C1, C2 и снова C1 имеем: $(a + b) + 1 = (a + b)' = a + b' = a + (b + 1)$. Отсюда $1 \in M$.

б) пусть $c \in M$. В следующих переходах последовательно применяем C2, $c \in M$,C2 и снова C2:

$$(a + b) + c' = \Big((a + b) + c\Big)' = \Big(a + (b + c)\Big)' = a + (b + c)' = a + (b + c').$$

[5]На языке теории множеств, операция — это отображение $* : X \times X \to X$.

В результате $c' \in M$.

Из (а), (б) и П4 получаем, что $M = \mathbb{N}$.

■

В следующей теореме докажем *коммутативность* сложения натуральных чисел.

Теорема 2.2. *Для любых* $a, b \in \mathbb{N}$ *выполняется* $a + b = b + a$.

Доказательство. Обозначим через $M = \{a \in \mathbb{N} : \forall b \in \mathbb{N} \Rightarrow a+b = b+a\}$ и докажем, что $M = \mathbb{N}$.

а) для того, чтобы доказать, что $1 \in M$, введем вспомогательное множество $M_1 = \{b \in \mathbb{N} : 1 + b = b + 1\}$.

А) очевидно, что $1 \in M_1$.

Б) пусть $b \in M_1$. Применим последовательно С2, $b \in M_1$, С2 и С1:

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

Теперь воспользуемся предыдущей теоремой и переставим скобки: $b + (1 + 1) = (b + 1) + 1 = b' + 1$. Мы доказали, что $b' \in M_1$. Теперь (А), (Б) и П4 дают $M_1 = \mathbb{N}$, что означает $1 \in M$ и (а) доказано.

б) в предположении, что $a \in M$, докажем, что $a' \in M$. В следующих переходах последовательно применяются С1, теорема 2.1, уже доказанный пункт (а) и теорема 2.1:

$$a' + b = (a + 1) + b = a + (1 + b) = a + (b + 1) = (a + b) + 1.$$

Теперь воспользуемся тем, что $a \in M$, теоремой 2.1 и С1:

$$(a + b) + 1 = (b + a) + 1 = b + (a + 1) = b + a'.$$

Мы проверили, что $a' \in M$.

Теперь (а), (б) и П4 дают $M = \mathbb{N}$.

■

В математике часто встречаются равносильные (или эквивалентные) утверждения (например, четырехугольник $ABCD$ является ромбом $\Leftrightarrow$ диагонали делят его углы пополам). Для доказательства равносильности более двух утверждений не доказывают их попарную равносильность, а часто используют следующий прием: $P_1 \Rightarrow P_2 \Rightarrow \ldots \Rightarrow P_n \Rightarrow P_1$. Следующая теорема называется *правилом сокращения для сложения.*

Теорема 2.3. *Следующие условия для* $a, b \in \mathbb{N}$ *равносильны:*

1) $a = b$ *;*

2) для каждого $c \in \mathbb{N}$ *выполняется, что* $a + c = b + c$ *;*

3) найдется хотя бы одно число $c_1 \in \mathbb{N}$ *, для которого* $a + c_1 = b + c_1$ *.*

Доказательство. 1) $\Rightarrow$ 2) обозначим через $M = \{c \in \mathbb{N} : a + c = b + c\}$.

а) из $a = b$ следует (по П2), что $a' = b'$. Поэтому (по С1) $a + 1 = b + 1$ и $1 \in M$.

б) пусть $c \in M$, тогда $a + c = b + c$ и (по П2) $(a + c)' = (b + c)'$ или $a + c' = b + c'$. Мы проверили, что $c' \in M$. Теперь (а), (б) и П4 дают $M = \mathbb{N}$ и (2) доказано.

2) $\Rightarrow$ 3) очевидно.

3) $\Rightarrow$ 1) о/п: предположим, что $a \neq b$. Введем вспомогательное множество $L = \{c \in \mathbb{N} : a + c \neq b + c\}$.

а) из $a \neq b$ и П3 получим $a' \neq b'$ или $a + 1 \neq b + 1$, т.е. $1 \in L$.

б) пусть теперь $c \in L$, т.е. $a + c \neq b + c$ и (снова по П3) $(a + c)' \neq (b + c)'$ или $a + c' \neq b + c'$. Мы проверили, что $c' \in L$.

Теперь (а), (б) и П4 дают $L = \mathbb{N}$, поэтому не найдется число $c_1 \in \mathbb{N}$ со свойством $a + c_1 = b + c_1$. $\lightning$.

■

Предыдущая теорема позволяет сокращать левую и правую часть на одно и то же натуральное число без перенесения из одной части в другую часть (для чего необходим недоступный пока минус) и приведения подобных. Следующая простая теорема поможет нам при изучении свойств порядка на $\mathbb{N}$.

Теорема 2.4. *Для любых* $a, n \in \mathbb{N}$ *выполняется* $a + n \neq n$ *.*

Доказательство. Введем множество $M = \{n \in \mathbb{N} : \forall a \in \mathbb{N} \Rightarrow a + n \neq n\}$ и докажем, что $M = \mathbb{N}$.

а) $a + 1 = a' \neq 1$ (по П1), поэтому $1 \in M$.

б) пусть $n \in M$, тогда $a + n \neq n$ и (по П3) $(a + n)' \neq n'$ или $a + n' \neq n'$. Мы проверили, что $n' \in M$.

Теперь (а), (б) и П4 дают $M = \mathbb{N}$.

■

1.3. Умножение натуральных чисел

Определение. *Умножением на* $\mathbb{N}$ *называется операция* $\cdot$ *(или* $\times$*), которая удовлетворяет следующим свойствам (аксиомам умножения):*

У1. Для любого $a \in \mathbb{N}$ *выполняется* $a \cdot 1 = a$,

У2. Для всех $a, b \in \mathbb{N}$ *верно* $a \cdot b' = a \cdot b + a$.

Привычные договоренности сохраняются, вместо $a \cdot b$ можно писать ab . Из определения можно получить $2 \cdot 2 = 2 \cdot 1' = 2 \cdot 1 + 2 = 2 + 2 = 4$.

Свойство сложения и умножения на $\mathbb{N}$, доказанное в следующей теореме, называется *правой дистрибутивностью.*

Теорема 3.1. *Для любых* $a, b, c \in \mathbb{N}$ *верно* $(a + b)c = ac + bc$.

Доказательство. Пусть $M = \{c \in \mathbb{N} : \forall a, b \in \mathbb{N} \Rightarrow (a + b)c = ac + bc\}$.

а) применяя трижды У1, получим $(a + b) \cdot 1 = a + b = a \cdot 1 + b \cdot 1$, что означает $1 \in M$.

б) предположим, что $c \in M$. Последовательно применим У2, $c \in M$, ассоциативность и коммутативность сложения на $\mathbb{N}$ и, наконец, У2:

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

Мы доказали, что $c' \in M$, теперь (а), (б) и П4 дают $M = \mathbb{N}$.

■

Умножение на $\mathbb{N}$ также обладает свойством *коммутативности*, об этом следующая

Теорема 3.2. *Для любых* $a, b \in \mathbb{N}$ *выполняется* $ab = ba$.

Доказательство. Обозначим через $M = \{a \in \mathbb{N} : \forall b \in \mathbb{N} \Rightarrow ab = ba\}$ и докажем, что $M = \mathbb{N}$.

а) для того, чтобы доказать, что $1 \in M$, введем вспомогательное множество $M_1 = \{b \in \mathbb{N} : 1 \cdot b = b \cdot 1\}$.

А) очевидно, что $1 \in M_1$.

Б) пусть $b \in M_1$. Применим последовательно У2, $b \in M_1$, У1, С1 и У1:

$$1 \cdot b' = 1 \cdot b + 1 = b \cdot 1 + 1 = b + 1 = b' = b' \cdot 1.$$

Мы доказали, что $b' \in M_1$. Теперь (А), (Б) и П4 дают $M_1 = \mathbb{N}$, что означает $1 \in M$ и (а) доказано.

б) в предположении, что $a \in M$, докажем, что $a' \in M$. В следующих переходах последовательно применяются С1, правая дистрибутивность, уже доказанный пункт (а), У1 и У2:

$$a' \cdot b = (a+1)b = ab + 1 \cdot b = ba + b \cdot 1 = ba + b = b \cdot a'.$$

Мы проверили, что $a' \in M$.

Теперь (а), (б) и П4 дают $M = \mathbb{N}$.

■

Следствие. *Для любых* $a, b, c \in \mathbb{N}$ *верно* $c(a+b) = ca + cb$ *(левая дистрибутивность).*

Доказательство. Трижды применяя коммутативность умножения и один раз правую дистрибутивность, получим

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

■

Упражнения

1. Докажите свойство ассоциативности умножения натуральных чисел, т.е. для любых $a, b, c \in \mathbb{N}$ выполняется $(ab)c = a(bc)$.

2. Попробуйте доказать правило сокращения для произведения натуральных чисел, т.е. эквивалентность для $a, b \in \mathbb{N}$ следующих трех условий:

1) $a = b$;

2) для каждого $c \in \mathbb{N}$ выполняется, что $ac = bc$;

3) найдется хотя бы одно число $c_1 \in \mathbb{N}$, для которого $a \cdot c_1 = b \cdot c_1$.

1.4. Порядок на $\mathbb{N}$

С помощью сложения нетрудно ввести строгий ($<$) и нестрогий ($\leqslant$) порядки на $\mathbb{N}$.

Определение. *Пусть* $a, b \in \mathbb{N}$ *тогда* $a < b$, *если найдется такое* $k \in \mathbb{N}$, *что* $a + k = b$. *Выполняется* $a \leqslant b$, *если* $a < b$ *или* $a = b$.

По определению $b > a$, если $a < b$. Также по определению считаем, что $b \geqslant a$, если $a \leqslant b$. В следующей теорема доказываются три простых свойства порядка.

Теорема 4.1. *Пусть* $a, b, c \in \mathbb{N}$. *Тогда:*

1) $a \leqslant a$ *(рефлексивность);*

2) если одновременно выполняются $a \leqslant b$ *и* $b \leqslant a$, *то* $a = b$ *(антисимметричность);*

3) если одновременно выполняются $a \leqslant b$ *и* $b \leqslant c$, *то* $a \leqslant c$ *(транзитивность).*

Доказательство. 1) следует из определения нестрогого порядка.

2) о/п: $a < b$ и $b < a$. Тогда найдутся такие $k, k_1 \in \mathbb{N}$, что $a + k = b$ и $b + k_1 = a$. Подставив b, получим $a + k + k_1 = a$. Коммутативность позволяет записать $k + k_1 + a = a$, что противоречит теореме 2.4.

3) если $a = b$ или $b = c$, то утверждение очевидно, поэтому будем считать, что $a < b$ и $b < c$. По определению найдем такие $k, l \in \mathbb{N}$, что $a + k = b$ и $b + l = c$, откуда $a + (k + l) = c$, что влечет $a < c$.

■

В следующей теореме доказывается *линейность* порядка на $\mathbb{N}$.

Теорема 4.2. *Для любых* $a, b \in \mathbb{N}$ *выполняется ровно одно из следующих утверждений: 1)* $a = b$; *2)* $a < b$; *3)* $b < a$.

Доказательство. I. Сначала докажем, что хотя бы одно из этих утверждений выполняется. Для этого введем множество

$$M = \{a \in \mathbb{N} : \forall b \in \mathbb{N} \text{ для } a \text{ и } b \text{ выполнено } (1) \vee (2) \vee (3)\}.$$

а) по теореме 1.3 для любого $b \in \mathbb{N}$ справедливо: $b = 1$ или $b = k'$, где $k \in \mathbb{N}$. Равенства $b = 1$ или $b = 1 + k$ дают $1 \leqslant b$, поэтому $1 \in M$ (так как для 1 и b выполняется (1) или (2)).

б) теперь предположим, что $a \in M$ и рассмотрим произвольное число $b \in \mathbb{N}$. Для a и b по предположению выполнено хотя бы одно из трех соотношений. Рассмотрим три случая.

1-й случай: $a = b$. Тогда $a' = b + 1$, что дает $b < a'$ и для пары a' и b выполняется (3).

2-й случай: $a < b$. По определению найдется такое натуральное k, что $a + k = b$. Если $k = 1$, то $a' = b$ и для этих элементов выполнено (1). При $k \neq 1$ по теореме 1.3 найдем $l \in \mathbb{N}$, что $k = l' = l + 1$, отсюда $b = a + 1 + l = a' + l$, т.е. $a' < b$ и для a' и b выполняется (2).

3-й случай: $b < a$. По определению найдем такое $p \in \mathbb{N}$, что $b + p = a$. Переходя к следующему, получим $a' = (b + p)' = b + p'$,что дает $b < a'$ и для a' и b выполняется (3).

Таким образом, $a' \in M$. Применяя теперь П4, получим $M = \mathbb{N}$.

II. Теперь докажем, что одновременно не могут быть справедливы сразу два (и тем более три) утверждения. Предположим противное и рассмотрим несколько случаев.

1-й случай: $a = b \ \& \ a < b$. Тогда одновременно $a = b$ и $a + k = b$ (для некоторого натурального k). Отсюда $k + a = a$, что противоречит теореме 2.4.

2-й случай: $a = b \ \& \ b < a$. Аналогично предыдущему случаю приходим к равенству $k + b = b$, которое противоречит теореме 2.4.

3-й случай: $a < b \ \& \ b < a$. Противоречие было получено при доказательстве свойства антисимметричности в предыдущей теореме.

■

Порядок на $\mathbb{N}$ и операции сложения и умножения связаны многочисленными свойствами. Перечислим некоторые из них в следующей теореме.

Теорема 4.3. *Для любых $a, b, c, d \in \mathbb{N}$ выполняются следующие свойства:*

1) если $a \leqslant b$, то $a + c \leqslant b + c$ (если $a < b$, то $a + c < b + c$);

2) если $a \leqslant b$ и $c \leqslant d$, то $a + c \leqslant b + d$ (если $a < b$ и $c \leqslant d$, то $a + c < b + d$);

3) если $a \leqslant b$, то $ac \leqslant bc$ (если $a < b$, то $ac < bc$);

4) если $a \leqslant b$ и $c \leqslant d$, то $ac \leqslant bd$ (если $a < b$ и $c \leqslant d$, то $ac < bd$);

5) найдется такое $k \in \mathbb{N}$, что $b < ak$ (свойство Архимеда).

Доказательство. 1) при $a = b$ это следует из теоремы о сокращении для сложения (теорема 2.3). Путь теперь $a < b$, тогда для некоторого $k \in \mathbb{N}$ верно $a+k = b$. Из теоремы 2.3 получим $a+k+c = b+c$ или $a+c+k = b+c$, что дает $a + c < b + c$.

2) при $a = b$ или $c = d$ достаточно применить уже доказанное (1). Пусть $a < b$ и $c < d$. Дважды применим свойство (1), получим: $a + c < b + c$ и $c + b < d + b$. По транзитивности имеем $a + c < b + d$.

3) 1-й случай: $a = b$. Пусть $M = \{c \in \mathbb{N} : ac = bc\}$.

а) из $a = b$ и С1 получим $a \cdot 1 = b \cdot 1$ и $1 \in M$.

б) если $c \in M$, то $ac = bc$ и теорема 2.3 дает $ac+a = bc+b$, т.е. $ac' = bc'$ и $c' \in M$. Из (а), (б) и П4 получим $M = \mathbb{N}$ и первый случай рассмотрен.

2-й случай: $a < b$. Тогда для некоторого $k \in \mathbb{N}$ верно $a + k = b$ и из первого случая и дистрибутивности имеем: $(a + k)c = bc$ или $ac + kc = bc$. Последнее означает, что $ac < bc$.

4) при $a = b$ или $c = d$ достаточно применить уже доказанное (3). Пусть $a < b$ и $c < d$. Дважды применим свойство (3), получим: $ac < bc$ и $cb < db$. По транзитивности имеем $ac < bd$.

5) применив к неравенствам $1 \leqslant a$ и $b < b'$ доказанное только что свойство (4), получим $1 \cdot b < a \cdot b'$. Поэтому $k = b'$ является искомым числом.

■

Следствие. *(Правило сокращения для произведения). Для $a, b \in \mathbb{N}$ равносильны следующие условия:*

1) $a = b$;

2) для каждого $c \in \mathbb{N}$ выполняется, что $ac = bc$;

3) найдется хотя бы одно число $c_1 \in \mathbb{N}$, для которого $a \cdot c_1 = b \cdot c_1$.

Доказательство. 1) $\Rightarrow$ 2) это утверждение доказано в предыдущей теореме (см. (3), первый случай).

2) $\Rightarrow$ 3) очевидно выполняется.

3) $\Rightarrow$ 1) о/п: пусть $a \neq b$. Тогда из линейности порядка на $\mathbb{N}$ верно одно из двух неравенств: $a < b$ или $b < a$. Из свойства (3) предыдущей теоремы получим справедливость одного из двух неравенств: $ac_1 < bc_1$ или $bc_1 < ac_1$. Это противоречит условию $a \cdot c_1 = b \cdot c_1$.

■

1.5. Полнота порядка на $\mathbb{N}$, математическая индукция

В этом параграфе продолжим изучение свойств порядка на $\mathbb{N}$ и докажем его полноту. Существование минимального элемента в любом непустом подмножестве на $\mathbb{N}$ позволит нам обосновать метод математической индукции. Начнем с того, что в одном определении введем сразу два понятия: наименьшего и наибольшего элемента. То, что относится ко второму из терминов, записано в скобках.

Определение. *Пусть $A \subseteq \mathbb{N}$ и $A \neq \varnothing$. Число a^* называется наименьшим (наибольшим) в A, если*

1) $a^* \in A$;

2) для всех $b \in A$ выполняется $a^* \leqslant b$ ($b \leqslant a^*$).

В линейно упорядоченных множествах понятия минимального элемента и наименьшего совпадают, поэтому допустимо использовать в отношении a^* термин минимального элемента обозначать его $a^* = \min A$ (наибольший элемент в A обозначается $a^* = \max A$).

Свойство, доказанное в следующей теореме, называется *полнотой* порядка.

Теорема 5.1. *В любом непустом подмножестве натуральных чисел найдется минимальный элемент.*

Доказательство. Пусть $A \subseteq \mathbb{N}$ и $A \neq \varnothing$. Обозначим через

$$M = \{b \in \mathbb{N} : \forall a \in A \Rightarrow b \leqslant a\}.$$

Поскольку для любого $c \in \mathbb{N}$ верно $1 \leqslant c$, получаем $1 \in M$. Если бы для каждого $b \in M$ выполнялось $b' \in M$, то П4 дало бы $M = \mathbb{N}$, а этого быть не может (действительно, если $a \in A$, то $b_1 = a' > a$ и поэтому $b_1 \notin M$). Значит, существует такое $b_0 \in M$, что $b_0' \notin M$. Осталось доказать, что $b_0 = \min A$.

Из определения множества M следует, что $b_0 \leqslant a$ для каждого $a \in A$, поэтому свойство (2) определения минимального элемента выполняется.

Проверим, что $b_0 \in A$. Предположим противное, тогда все нестрогие неравенства $b_0 \leqslant a$ превращаются в строгие неравенства $b_0 < a$, из которых следует $b_0' \leqslant a$ для всех $a \in A$ (действительно, переписывая $b_0 < a$ в виде $b_0 + k = a$ для некоторого $k \in \mathbb{N}$, приходим к $b_0' \leqslant a$). Последнее означает, что $b_0' \in M$, что противоречит выбору b_0. Свойство (1) минимального элемента также доказано. Таким образом, $a^* = b_0$ — искомое число.

■

Определение. *Пусть $A \subseteq \mathbb{N}$ и $A \neq \varnothing$. Множество A называется ограниченным сверху, если найдется такое $b \in \mathbb{N}$, что для всех $a \in A$ выполняется $a \leqslant b$. Такое число b называется верхней границей множества A.*

Ясно, что если в A есть наибольший элемент, то A ограничено сверху. Оказывается, верно и обратное утверждение.

Следствие. *Пусть $A \subseteq \mathbb{N}$ и $A \neq \varnothing$. Если A ограниченно сверху, то существует $b^* = \max A$.*

Доказательство. Рассмотрим множество

$$B = \{b \in \mathbb{N} : b \text{ является верхней границей для } A\}.$$

По условию $B \neq \varnothing$, поэтому найдется $b^* = \min B$. Докажем, что одновременно $b^* = \max A$. Из $b^* \in B$ следует, что для всех $a \in A$ выполняется $a \leqslant b^*$. Осталось показать, что $b^* \in A$. О/п: $b^* \notin A$. Тогда для всех $a \in A$ выполняется $a < b^*$. Из условия $A \neq \varnothing$ и этих строгих неравенств, получим, что $b^* > 1$ и найдется такое $c \in \mathbb{N}$, что $c' = b^*$. Строгие неравенства

$a < b^*$ превратятся в $a \leqslant c$ для всех $a \in A$. Поэтому $c \in B$, $c < b^*$, а это противоречит условию $b^* = \min B$.

■

Перед формулировкой теоремы *о математической индукции* рассмотрим пример.

П р и м е р 1. Доказать, что для любого $n \in \mathbb{N}$ выполняется формула:

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2.$$

Эта формула очевидно верна при $n = 1$ (мы проверили базу индукции). Предположим теперь, что эта формула верна для $n = k$ (сделали предположение индукции) и проверим, что она верна и для $n = k+1$. Нам необходимо доказать следующее равенство:

$$1 + 3 + 5 + \ldots + (2k - 1) + (2k + 1) = (k + 1)^2.$$

Все слагаемые в левой части, кроме последнего, заменим на k^2 (используем предположение индукции), приходим в левой части к $k^2 + (2k + 1)$, что сворачивается в $(k+1)^2$. Поэтому утверждение для $n = k+1$ проверено (мы доказали шаг индукции). Следующая теорема обосновывает правильность таких рассуждений.

Теорема 5.2. *Пусть $n \in \mathbb{N}$ и $T(n)$ — некоторое утверждение (для любого $n \in \mathbb{N} \Rightarrow T(n) \in \{И, Л\}$, т.е. $T(n)$ принимает одно из двух значений: истина или ложь), для которого доказаны следующие два свойства:*

1)(Б.И. — база индукции) $T(1) = И$;

2)(Ш.И. — шаг индукции) в предположении, что $T(n)$ истинно для всех $n \leqslant k$ доказано, что $T(k + 1) = И$.

Тогда $T(n)$ истинно для всех $n \in \mathbb{N}$.

Доказательство. О/п: пусть найдется такое $n_0 \in \mathbb{N}$, что $T(n_0) = Л$. Обозначим через $A = \{a \in \mathbb{N} : T(a) = Л\}$ и заметим, что $A \subseteq \mathbb{N}$ и $A \neq \varnothing$ (так как $n_0 \in A$). По предыдущей теореме найдется $a^* = \min A$. Тогда возможны два случая.

1-й случай: $a^* = 1$. Но (по Б.И.) $T(1) = И$, что противоречит условию $1 = a^* \in A$.

2-й случай: $a^* > 1$. Тогда $a^* = k'$ для некоторого $k \in \mathbb{N}$. При всех $n \leqslant k$ выполняется $n < a^*$, поэтому $n \notin A$ и $T(n)$ истинно. Поскольку доказан Ш.И., выполняется $T(k+1) = И$ или $T(a^*) = И$, а это противоречит условию $a^* \in A$.

■

Если всё еще остались сомнения в правильности метода математической индукции, обратите внимание на то, как связка Б.И. + Ш.И. действует на первые натуральные числа. Ясно, что $T(1) = \text{И}$. Теперь $T(2) = \text{И}$, поскольку для всех предыдущих к двойке (это только 1) утверждение выполняется и можно применить шаг индукции. Далее, утверждение верно для 1 и 2, поэтому снова можно применить Ш.И. и получить, что $T(3) = \text{И}$ и т.д.

Существует несколько модификаций метода математической индукции. Например, в Ш.И. вместо «$T(n)$ истинно для всех $n \leqslant k$» можно требовать, что только «$T(k)$ истино». Доказательство теоремы почти не поменяется. Кстати, в примере 1 мы использовали именно такой вариант метода. Также нужно быть готовым, что утверждение будет сформулировано не для всех натуральных чисел, а только начиная с некоторого — n_0, тогда в Б.И. надо будет доказывать, что $T(n_0) = \text{И}$. Или утверждение $T(n)$ сформулировано только для подмножества A натуральных чисел, а не для всего $\mathbb{N}$. Например, если A — все четные натуральные числа, то в Б.И. надо будет проверить $T(2) = \text{И}$, а в шаге индукции, предполагая $T(k) = \text{И}$, доказать, что $T(k+2) = \text{И}$. Рассмотрим несколько примеров.

П р и м е р 2. Некоторое время назад выпускались банкноты достоинством 3 и 5 рублей. Делалось это не случайно, поскольку любое целое количество рублей n, начиная с 8, можно было разменять банкнотами только этих номиналов. Докажем это утверждение.

Б.И. $n = 8 = 3 + 5$ — верно.

Ш.И. Предположим, что для $n = k \geqslant 8$ размен возможен, т.е. $k = 3p+5q$. Если $q \geqslant 1$, то $k + 1 = 3(p + 2) + 5(q - 1)$ (мы одну пятирублевую купюру заменили на две трехрублевых). Если $q = 0$, то $k = 3p$ (и $p \geqslant 3$). Тогда $k + 1 = 3(p - 3) + 5(q + 2)$ (мы три трехрублевых купюры заменили на две пятирублевых). Шаг индукции доказан.

П р и м е р 3. Математикам давно известна последовательность Фибоначчи[6] — a_n ($n \in \mathbb{N}$), которая задается так: $a_1 = a_2 = 1$ и $a_{n+2} = a_{n+1} + a_n$ при $n \in \mathbb{N}$ (*рекуррентное* соотношение, позволяющее находить следующие члены последовательности через предыдущие). Эта последовательность, имеющая важное применение в кролиководстве, обладает рядом любопытных свойств[7], одно из которых следующее: a_n делится на 3 тогда и только тогда, когда n кратно 4. Докажем это утверждение по индукции. Легко найти, что $a_3 = 2$,

[6]Леонардо Пизанский, или Фибоначчи (1170–1250) — итальянский математик, первый выдающийся математик средневековой Европы.

[7]Самое важное из которых: $\lim\limits_{n\to\infty}(a_{n+1}/a_n) = \varphi$, где φ — золотое сечение.

$a_4 = 3$. Поэтому Б.И. проверена, поскольку a_1, a_2, a_3 не делятся на 3, а a_4 кратно трем. Для доказательства шага предположим, что a_n кратно трем, а a_{n-1}, a_{n-2}, a_{n-3} — нет. Тогда $a_{n+1} = a_n + a_{n-1}$ и $a_{n+2} = a_{n+1} + a_n$ не делятся на три (так как одно из слагаемых кратно трем, а второе — точно нет). Для следующего элемента получим

$$a_{n+3} = a_{n+2} + a_{n+1} = (a_{n+1} + a_n) + a_{n+1} = 2a_{n+1} + a_n.$$

В итоговой сумме ровно одно слагаемое делится на 3, а другое —нет, поэтому a_{n+3} не кратно трем. Наконец,

$$a_{n+4} = a_{n+3} + a_{n+2} = (2a_{n+1} + a_n) + (a_{n+1} + a_n) = 3 \cdot a_{n+1} + 2a_n.$$

Это число кратно трем, поскольку каждое их двух слагаемых делится на три ($3 \cdot a_{n+1}$ — очевидно, $2a_n$ — по предположению). Шаг индукции доказан. В этом примере мы делали переход от n к $n+4$, рассматривая четверки чисел.

П р и м е р 4. Докажем неравенство Бернулли[8]: $(1+x)^n \geqslant 1 + nx$ при всех $n \in \mathbb{N}$ и $x \in [-1; \infty)$.

Б.И. При $n = 1$ получим верное неравенство $1 + x \geqslant 1 + x$.

Ш.И. Предположим, что для $n = k$ выполняется $(1+x)^k \geqslant 1 + kx$. Домножим обе части этого неравенства на неотрицательное число $1 + x$, получим

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

Последний переход можно сделать, так как $kx^2 \geqslant 0$. Шаг индукции доказан. Кстати, при $n \geqslant 2$ и $x \in (-1; 0) \cup (0; \infty)$ аналогично можно доказать строгое неравенство.

Приведем несколько упражнений на совершенно разные направления применимости метода математической индукции.

[8] Якоб Бернулли (1655–1705) — швейцарский математик, один из основателей математического анализа и теории вероятностей, ввел термин «интеграл».

Упражнения

1. Докажите, для любого $n \in \mathbb{N}$ выполняется формула:

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

2. Докажите, что при всех $n \in \mathbb{N}$, являющихся степенью двойки (т.е. $n \in \{2, 4, 8, 16, \ldots\}$), среднее геометрическое n неотрицательных чисел не превосходит их среднего арифметического:

$$\sqrt[n]{x_1 \cdot x_2 \cdot \ldots \cdot x_n} \leqslant \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

3. Доказать, что любое натуральное число можно представить в виде суммы нескольких (возможно, одного) различных чисел Фибоначчи.

4. *Задача о Ханойской башне.* Имеется три блюдца, на первом из них расположена стопка из n дисков, диаметр которых тем меньше, чем выше в стопке расположен диск (Ханойская башня), остальные блюдца пусты. За один ход разрешено взять верхний диск из любой стопки и переложить его на пустое блюдце или на верх другой стопки; при этом запрещено класть бóльший диск на меньший. Требуется за несколько ходов переложить все диски на третье блюдце. Доказать, что задача разрешима, и найти минимальное число ходов, которое требуется для ее решения.

5. На плоскости даны n прямых. Доказать, что области, на которые эти прямые разбивают плоскость, можно так закрасить двумя красками, что никакие две соседние (т.е. области, соприкасающиеся по нетривиальному отрезку прямой) не будут закрашены одной и той же краской.

6. Доказать, что для всех натуральных $n > 5$ квадратный торт можно разрезать на n квадратных (не обязательно равных между собой) кусков.

7. *Формула Пика.* Доказать, что площадь многоугольника, вершины которого лежат в узлах клетчатой бумаги, равна $a + b/2 - 1$, где a — число узлов, лежащих внутри многоугольника, b — число узлов на его сторонах.

8. Пусть на плоскости задана сеть линий, соединяющих между собой какие-то точки и не имеющих других общих точек; мы будем считать еще, что эта сеть линий состоит «из одного куска», т.е., что из каждой из точек можно попасть в другую, двигаясь только вдоль линий сети (свойство связности). Такую сеть линий мы будем называть *картой*, заданные точки — ее *вершинами*, отрезки кривых между двумя смежными вершинами — *границами* карты, части плоскости, на которые она разбивается границами (в том числе и бесконечную внешнюю область), — *странами* карты. Обозначим число стран произвольной карты через s, число ее границ — через l, и число вершин — через p. Докажите, что $s + p = l + 2$ (*формула Эйлера*[9]).

[9]Леонард Эйлер (1707–1783) — швейцарский, немецкий и российский математик и механик, автор бо-

9. На краю пустыни имеется большой (т.е. неограниченный) запас бензина и машина, которая при полной заправке может проехать 50 километров. Имеются (в неограниченном количестве) канистры, в которые можно сливать бензин из бензобака машины и оставлять на хранение (в любой точке пустыни). Доказать, что машина может проехать любое расстояние (канистры с бензином возить не разрешается, пустые можно возить в любом количестве).

1.6. Делимость на $\mathbb{N}$. Деление с остатком

Определение. *Пусть* $a, b \in \mathbb{N}$. *Число* a *делится на* b, *если найдется такое* $c \in \mathbb{N}$, *что* $a = b \cdot c$.

Обозначается факт делимости так: $a \vdots b$ или $b \mid a$ (последнее обозначение читается «b делит a»). В следующей теореме докажем простые свойства делимости.

Теорема 6.1. *Пусть* $a, b, c, d \in \mathbb{N}$, *тогда выполняются следующие свойства:*

1) $a \vdots a$ *(рефлексивность);*

2) если одновременно $a \vdots b$ *и* $b \vdots a$, *то* $a = b$ *(антисимметричность);*

3) если одновременно $a \vdots b$ *и* $b \vdots c$, *то* $a \vdots c$ *(транзитивность);*

4) если $a + b = c$ *и два числа из трех* $\{a, b, c\}$ *делятся на* d, *то и третье число делится на* d *(линейность).*

Доказательство. 1) очевидно, так как $a = a \cdot 1$.

2) по определению найдутся такие $k, l \in \mathbb{N}$, что $a = b \cdot k$ и $b = a \cdot l$, откуда $a = a \cdot (k \cdot l)$ или, по правилу сокращения для произведения, $1 = k \cdot l$. Из последнего равенства получаем $k = l = 1$ и $a = b$ (если бы, например $k > 1$ и $l \geqslant 1$, то по теореме 4.3 получилось бы противоречивое неравенство $1 = k \cdot l > 1$).

3) по определению найдутся такие $k, l \in \mathbb{N}$, что $a = b \cdot k$ и $b = c \cdot l$, откуда $a = c \cdot (k \cdot l)$ или $a \vdots c$.

4) в случае, если $a, b \vdots d$, находим такие $k, l \in \mathbb{N}$, что $a = d \cdot k$ и $b = d \cdot l$ и с помощью дистрибутивности быстро получаем $c = a + b = d(k + l) \vdots d$.

Оставшиеся два случая между собой похожи, поэтому без ограничении

лее 850 научных работ; в возрасте 24 лет стал профессором математики Петербургской академии наук; Эйлер оставил важнейшие труды по самым различным отраслям математики, механики, физики, астрономии; познания Эйлера были энциклопедичны: кроме математики, он глубоко изучал ботанику, медицину, химию, теорию музыки, множество европейских и древних языков.

общности (далее будем использовать сокращение б.о.о.) считаем, что $a, c \vdots d$. Находим такие $k, p \in \mathbb{N}$, что $a = d \cdot k$ и $c = d \cdot p$. Заметим, что из данного равенства $a + b = c$ следует $a < c$, откуда по теореме 4.3 получим $k < p$ (если бы $k \geqslant p$, то $a = kd \geqslant pd = c$). Последнее неравенство дает нам $k+l = p$ для некоторого $l \in \mathbb{N}$. Теперь равенство $a+b = c$ можно переписать в виде $kd + b = (k + l)d = kd + ld$. Правило сокращения для сложения дает нам $b = ld \vdots d$.

■

П р и м е р 1. Пусть $a, b, c \in \mathbb{N}$ выбраны так, что число $k = 5a+7b+12c$ делится на 13. Докажем, что число $l = 8a + 32b + 14c$ также делится на 13. Заметим, что число $k + l = 13a + 39b + 26c \vdots 13$. Учитывая, что $k \vdots 13$, свойство линейности дает нам, что $l \vdots 13$.

Определение. *Число $p \in \mathbb{N}$ называется простым, если оно имеет ровно два делителя: 1 и p. Через P обозначим множество всех простых чисел. Натуральные числа, имеющие более двух делителей, называются составными.*

Число 1 не является ни простым, ни составным. Заметим, что 2 — первое простое число и единственное простое среди четных чисел,

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, \ldots\}.$$

Возникают несколько вопросов о множестве P. Это множество бесконечно? Есть ли быстрый способ определить: число p является простым или нет? Есть ли несложная формула, с помощью которой можно получить все простые числа (или бесконечно много простых чисел)?

Теорема 6.2. *Пусть $a \in \mathbb{N}$ и a — составное число. Если d — наименьший, отличный от 1, делитель числа a, то*

1) $d \in P$;

2) $d \cdot d \leqslant a$.

Доказательство. 1) из-за того, что a — составное число, множество $A = \{b \in \mathbb{N} : b \neq 1 \,\&\, a \vdots b\}$ не пусто, и по теореме о полноте порядка (теорема 5.1) найдется $d = \min A$. Докажем, что $d \in P$. О/п: число d составное, поэтому найдется такое натуральное k, что $1 < k < d$ и $d \vdots k$. Две делимости ($a \vdots d$ и $d \vdots k$) и транзитивность дают $a \vdots k$, что противоречит $d = \min A$.

2) условие $a \vdots d$ дает $a = d \cdot c$ для некоторого $c \in \mathbb{N}$. Из последнего равенства мы получаем очевидное $a \vdots c$, а условие $d = \min A$ дает нам

$d \leqslant c$. Умножив последнее неравенство на d, придем к $d \cdot d \leqslant d \cdot c = a$.

■

По определению считают, что $d^2 = d \cdot d$. Следующее правило сформулируем в предположении, что вам известно понятие квадратного корня из неотрицательного числа и понятие целой части $x \in \mathbb{R}$ (целой частью $x \in \mathbb{R}$ называется наибольшее целое число $k = [x]$, которое не превосходит x). Так, например, $[\pi] = 3$, $[-\pi] = -4$. Правило, которое следует из предыдущей теоремы: *натуральное число $p > 1$ является простым тогда и только тогда, когда среди простых чисел от 2 до $[\sqrt{p}]$ нет делителей числа p*. Действительно, если бы p было составным числом, то наименьший его делитель d, который отличен от 1, был бы одновременно простым числом и лежал бы в диапазоне от 2 до $[\sqrt{p}]$. Теперь почти очевидно, что $113 \in P$, поскольку 2, 3, 5 и 7 не являются делителями этого числа.

На этой же идее основано *решето Эратосфена*[10], которое предназначено для поиска всех простых чисел в диапазоне от 1 до $n \in \mathbb{N}$, где $n > 1$. Правило Эратосфена работает так: выпишем все числа от 1 до n, сразу вычеркнем единицу; первое невычеркнутое число, т.е. двойка, является простым числом; затем вычеркиваем каждое второе число; первое невычеркнутое число, т.е. тройка, является простым; далее вычеркиваем каждое третье число и т.д. Получив после очередного вычеркивания новое наименьшее число k, не проверяем его простоту (это гарантируется предыдущей теоремой) и вычеркиваем следующие за k числа, идущие через k. Применяя метод Эратосфена, не пугаемся, если некоторые числа вычеркиваются несколько раз (30, например, вычеркнется три раза). Кроме того, процесс можно оборвать, когда достигнем числа $[\sqrt{n}]$, поскольку все невычеркнутые числа (по предыдущей теореме) будут простыми.

Следующая теорема называется *теоремой Евклида*[11].

Теорема 6.3. *Простых чисел бесконечно много.*

Доказательство. Предположим, что их конечно, т.е. p_1, $p_2, \ldots, p_n$ — все простые числа. Рассмотри число $a^* = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 = \prod_{i=1}^{n} p_i + 1$. Если это число простое, то сразу получаем противоречие, поскольку a^* больше

[10]Эратосфен Киренский (276 до н.э.–194 до н.э.) — греческий математик, астроном, географ; с 235 г. до н.э. — глава Александрийской библиотеки; первый ученый, вычисливший длину радиуса Земли; ввел термин «география».

[11]Евклид или Эвклид (около 325 до н.э.– до 265 до н.э.) — древнегреческий математик; его «Начала», состоящие из 13 книг, подвели итог предшествующему развитию математики (планиметрии, алгебры, начал стереометрии) и задали направление движения математики на два тысячелетия; Евклид занимался коническими сечениями, оптикой, элементарной теорией музыки.

любого из p_i. Пусть теперь a^* — составное число и d — его наименьший делитель, отличный от 1. Предыдущая теорема дает нам, что d — простое число, поэтому является одним из p_1, $p_2, \ldots,$ p_n. Таким образом, одновременно $a^* \vdots d$ и $p_1 \cdot p_2 \cdot \ldots \cdot p_n \vdots d$, тогда свойство линейности, примененное к равенству $a^* = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$, дает, что $1 \vdots d$. $\lightning$.

■

Определение. *Множеством целых чисел называется* $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \widetilde{\mathbb{N}}$, *где* $\widetilde{\mathbb{N}} = \{-n : n \in \mathbb{N}\}$, $-n \neq -k$ *при всех различных* $n, k \in \mathbb{N}$, *а также* $\mathbb{N} \cap \widetilde{\mathbb{N}} = \varnothing$ *и элемент* 0, *который называется нулем, не принадлежит* $\widetilde{\mathbb{N}} \cup \mathbb{N}$.

Элементы множества $\mathbb{Z}$ называются *целыми* числами. На множестве $\mathbb{N}$ введены операции сложения и умножения, а также порядок. Наша ближайшая задача — доопределить их на множество $\mathbb{Z}$. Начнем с произведения.

Определение. *Для всех* $n, k \in \mathbb{N}$ *будем считать, что*

1) $n \cdot (-k) = -k \cdot n = -(nk)$;

2) $(-n) \cdot (-k) = nk$;

3) $n \cdot 0 = 0 \cdot n = 0 \cdot (-k) = (-k) \cdot 0 = 0$.

Нетрудно заметить, что произведение на $\mathbb{Z}$ также обладает свойствами коммутативности и ассоциативности.

Определение. *Если* $a, b, c \in \mathbb{N}$ *и* $a + b = c$, *то число* b *называется разностью* c *и* a, *обозначается через* $c - a$.

Ясно, что разность для натуральных чисел c и a определена только в случае $a < c$. Кроме того, разность определена однозначно, поскольку из равенства $a + b = c = a + b_1$ и правила сокращения для сложения следует, что $b = b_1$.

Определение. *Для всех* $n, k \in \mathbb{N}$ *и* $l \in \mathbb{Z}$ *будем считать, что*

1) $(-n) + (-k) = -(n + k)$;

2) $$n + (-k) = (-k) + n = \begin{cases} 0, & \text{если} \quad n = k, \\ n - k, & \text{если} \quad n > k, \\ -(k - n), & \text{если} \quad n < k; \end{cases}$$

3) $l + 0 = 0 + l = l$.

В качестве упражнения можете проверить, что сложение на $\mathbb{Z}$ обладает свойствами коммутативности и ассоциативности, а сложение и умножение на $\mathbb{Z}$ — дистрибутивностью (т.е. для всех $x, y, z \in \mathbb{Z}$ верно $(x+y)z = xz+yz$). Вместо рассмотрения большого количества случаев для доказательства этих свойств, мы позже, при построении $\mathbb{Z}$ и $\mathbb{Q}$, воспользуемся конструкцией *алгебраического расширения*, с помощью которой свойства сложения и умно-

жения на $\mathbb{N}$, доказанные в предыдущих параграфах, автоматически перенесутся на сложение и умножение на $\mathbb{Z}$ и $\mathbb{Q}$.

Определение. *Для всех $n, k \in \mathbb{N}$ будем считать, что*

1) $-n < 0 < k$;

2) $(-n) < (-k)$, если $k < n$.

Для любых $l, m \in \mathbb{Z}$ выполняется $l \leqslant m$, если $l < m$ или $l = m$.

Снова, в качестве упражнения можете проверить, что продолженный порядок на $\mathbb{Z}$ также обладает свойствами: рефлексивностью, антисимметричностью, транзитивностью и линейностью. Кстати, «новый» порядок перестает быть полным, поскольку в $\mathbb{Z}$ нет минимального элемента.

Определение. *Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Число a можно разделить с остатком на b, если найдется такая пара $q \in \mathbb{Z}$ и $r \in \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$, что выполняется равенство*

$$a = bq + r, \quad 0 \leqslant r < b.$$

Например, при делении на 3 чисел 5 и -5 получаются такие представления: $5 = 3 \cdot 1 + 2$, $-5 = 3 \cdot (-2) + 1$. Обратите внимание, что по определению остаток не может быть отрицателен.

Теорема 6.4. *Для любых $a \in \mathbb{Z}$, $b \in \mathbb{N}$ число a можно разделить с остатком на b, причем единственным образом.*

Доказательство. I. Докажем сначала существование пары чисел $q \in \mathbb{Z}$ и $r \in \mathbb{Z}^+$, удовлетворяющей определению.

1-й случай: $a \in \mathbb{N}$. Будем использовать метод математической индукции по переменной a.

Б.И. $a = 1$. Если $b = 1$, то $1 = 1 \cdot 1 + 0$ — искомое представление. При $b > 1$ искомым будет $1 = b \cdot 0 + 1$.

Ш.И. Предположим, что все натуральные числа, меньшие a, можно разделить с остатком на b и докажем, что число a также можно разделить с остатком на b. Если $a < b$, искомым представлением будет $a = b \cdot 0 + a$. При $a = b$, равенство $a = b \cdot 1 + 0$ удовлетворяет условию. Осталось рассмотреть случай $a > b$. Перепишем это неравенство в виде $a = b + a_1$, где $a_1 \in \mathbb{N}$. Очевидно, что $a_1 < a$, поэтому можно воспользоваться предположением индукции и получить равенство $a_1 = b \cdot q_1 + r_1$, где $q_1 \in \mathbb{Z}$, $r_1 \in \mathbb{Z}^+$ и $0 \leqslant r_1 < b$. Тогда, используя коммутативность, ассоциативность и дистрибутивность, получим

$$a = a_1 + b = b \cdot q_1 + r_1 + b = b(q_1 + 1) + r_1.$$

Очевидно, что $q = q_1 + 1$ и $r = r_1$ удовлетворяют определению. Шаг индукции доказан.

2-й случай: $a = 0$. Тогда $0 = b \cdot 0 + 0$ — искомое представление.

3-й случай: $a = -n$, где $n \in \mathbb{N}$. По первому случаю, можно найти такую пару $q_1 \in \mathbb{Z}$, $r_1 \in \mathbb{Z}^+$, что $n = b \cdot q_1 + r_1$, и $0 \leqslant r_1 < b$. Если $r_1 = 0$, то $a = -n = b \cdot (-q) + 0$ — искомое представление. Остается случай $0 < r_1 < b$. Используя дистрибутивность для $\mathbb{Z}$ и определение сложения на $\mathbb{Z}$, получим

$$a = -n = b \cdot (-q_1) - r_1 = b \cdot (-q_1) - b + b - r_1 = b(-q_1 - 1) + (b - r_1).$$

Нетрудно заметить, что $q = -q_1 - 1 \in \mathbb{Z}$, а также $r = b - r_1$ удовлетворяет условию $0 < r < b$.

II. Докажем, что такое представление единственно. О/п: нашлось другое представление $a = bq^* + r^*$ и также выполняются условия $q^* \in \mathbb{Z}$, $r^* \in \mathbb{Z}^+$, $0 \leqslant r^* < b$. Если $r = r^*$, то, применяя правила сокращения для сложения и для умножения, из равенства $bq + r = bq^* + r^*$ получим $q = q^*$, что противоречит предположению. Осталось рассмотреть случай $r \neq r^*$. Из линейности порядка следует, что какой-то из этих двух остатков больше. Будем считать (б.о.о.), что $r > r^*$. Из равенства $bq + r = bq^* + r^*$ получим $r - r^* = b(q^* - q) \vdots b$. Если натуральное число $r - r^*$ делится на натуральное число b, то $r - r^* \geqslant b$, но $r - r^* \leqslant r < b$. $\lightning$.

■

1.7. НОД и НОК. Основная теорема арифметики

Определение. *Для произвольных $a, b \in \mathbb{N}$ их наибольшим общим делителем называется наибольшее $c \in \mathbb{N}$, для которого одновременно $a \vdots c$ и $b \vdots c$. Это число обозначается НОД(a, b) или (a, b). Если $(a, b) = 1$, то числа a и b называются взаимно простыми. Наименьшим общим кратным a и b, или НОК(a, b), называется наименьшее число $c^* \in \mathbb{N}$, которое одновременно делится и на a, и на b.*

Обозначим через $A = \{d \in \mathbb{N} \mid a \vdots d \,\&\, b \vdots d\}$. Множество $A \neq \varnothing$ (поскольку $1 \in A$) и оно ограничено сверху (например, числом a), поэтому (по следствию из теоремы о полноте порядка) найдется $c = \max A$. Мы доказали существование наибольшего общего делителя для любой пары натуральных чисел. Пусть $E = \{e \in \mathbb{N} \mid e \vdots a \,\&\, e \vdots b\}$, тогда $E \neq \varnothing$, поскольку $a \cdot b \in E$, и по теореме о полноте порядка существует $c^* = \min E$. Из определения следует,

что $c^* = \text{НОК}\,(a,b)$. То, что (a,b) и $\text{НОК}\,(a,b)$ определяются однозначно, сразу следует из линейности порядка на $\mathbb{N}$.

Лемма 7.1. *Пусть $a,b,d^* \in \mathbb{N}$ и число d^* удовлетворяет двум условиям:*

1) $a \vdots d^*$ и $b \vdots d^*$,

2) для любого $d \in \mathbb{N}$, для которого $a \vdots d$ и $b \vdots d$, выполняется $d^* \vdots d$.

Тогда $d^* = (a,b)$.

Доказательство. О/п: предположим, что $d_0 = (a,b) > d^*$. Поскольку $a,b \vdots d_0$, свойство (2) гарантирует, что $d^* \vdots d_0$, откуда $d^* \geqslant d_0$. $\lightning$.

■

Метод поиска (a,b), изложенный в следующей теореме, называется *алгоритмом Евклида.*

Теорема 7.2. *Пусть $a,b \in \mathbb{N}$ и $a \geqslant b$. Последовательно делим одно число на другое с остатком до тех пор, пока остаток не станет равным нулю:*

1) $a = bq + r$, $\quad 0 < r < b$, $\quad q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$;

2) $b = rq_1 + r_1$, $\quad 0 < r_1 < r$, $\quad q_1 \in \mathbb{Z}$, $r_1 \in \mathbb{Z}^+$;

3) $r = r_1q_2 + r_2$, $\quad 0 < r_2 < r_1$, $\quad q_2 \in \mathbb{Z}$, $r_2 \in \mathbb{Z}^+$;

и т.д.....

$n+1$) $r_{n-2} = r_{n-1}q_n + r_n$, $\quad 0 < r_n < r_{n-1}$, $\quad q_n \in \mathbb{Z}$, $r_n \in \mathbb{Z}^+$;

$n+2$) $r_{n-1} = r_nq_{n+1} + 0$, $\quad q_{n+1} \in \mathbb{Z}$.

Тогда $r_n = (a,b)$.

Доказательство. Сразу заметим, что процесс деления с остатком будет конечным, поскольку $b > r > r_1 > r_2 > \ldots$, и последний ненулевой остаток будет получен менее чем за b шагов (считаем, что один шаг — это одно деление с остатком). Поэтому r_n определен корректно.

1) докажем, что $a,b \vdots r_n$. Рассуждать будем, начиная с последнего уравнения, поднимаясь вверх (*метод подъема*). Из последнего уравнения сразу следует, что $r_n \mid r_{n-1}$. Учитывая, что $r_n \mid r_n$, $r_n \mid r_{n-1}$, предпоследнее уравнение и свойство линейности нам дают $r_n \mid r_{n-2}$. Аналогично рассуждая, приходим к $r_n \mid r_1, r \Rightarrow r_n \mid b$, и, наконец, из первого уравнения и условий $r_n \mid r$, $r_n \mid b$ получим, что $r_n \mid a$.

2) теперь рассмотрим произвольное число $d \in \mathbb{N}$, для которого $a \vdots d$ и $b \vdots d$. На этот раз начнем рассуждать с первого уравнения, двигаясь вниз (*метод спуска*). Из первого уравнения и свойства линейности получим, что

$r \vdots d$. Далее, второе уравнение и условия $b \vdots d$ и $r \vdots d$ дают нам, что $r_1 \vdots d$. Повторив такие рассуждения еще $n-1$ раз, получим $r_n \vdots d$.

Поскольку r_n удовлетворяет свойствам (1) и (2) предыдущей леммы, заключаем, что $r_n = (a, b)$.

■

Пример 1. Найдем $(387, 81)$. По алгоритму Евклида будем делить числа с остатком: $387 = 81{\cdot}4{+}63$, $81 = 63{\cdot}1{+}18$, $63 = 18{\cdot}3{+}9$, $18 = 9{\cdot}2{+}0$. Последний отличный от нуля остаток равен 9, поэтому $9 = (387, 81)$.

Следующее утверждение называется *теоремой о представлении НОД*.

Теорема 7.3. *Пусть $a, b \in \mathbb{N}$ и $c = (a, b)$. Тогда найдутся такие $x_0, y_0 \in \mathbb{Z}$, что $c = x_0 \cdot a + y_0 \cdot b$.*

Доказательство. Рассмотрим множество

$$A = \{n \in \mathbb{N} : \text{ найдутся такие } x, y \in \mathbb{Z}, \text{ что } n = x \cdot a + y \cdot b\}.$$

Сразу отметим, что $A \neq \varnothing$, поскольку $a = a \cdot 1 + b \cdot 0$ является элементом этого множества. По теореме о полноте порядка найдется $d^* = \min A$. Из условия $d^* \in A$ мы получим представление $d^* = x^* \cdot a + y^* \cdot b$ для некоторых $x^*, y^* \in \mathbb{Z}$.

1) докажем, что $d^* \mid a$ и $d^* \mid b$. Рассуждения аналогичны, поэтому проверим только первое утверждение. Предположим противное, нацело a на d^* не делится, тогда поделим с остатком: $a = d^* \cdot q + r$, где $q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$ и $0 < r < d^*$. Выражая r, получим

$$r = a - d^* \cdot q = a - (x^* \cdot a + y^* \cdot b)q = (1 - x^*q) \cdot a + (-y^*q) \cdot b.$$

Нетрудно заметить, что в скобках стоят целые числа, $r \in \mathbb{N}$, поэтому $r \in A$. Условие $r < d^*$ противоречит $d^* = \min A$.

2) возьмем произвольное $d \in \mathbb{N}$, для которого одновременно $a \vdots d$ и $b \vdots d$, тогда правая часть равенства $d^* = x^* \cdot a + y^* \cdot b$ делится на d по свойству линейности, поэтому $d^* \vdots d$.

Учитывая (1), (2) и результат леммы, получим, что $d^* = (a, b)$ и представление $c = x^* \cdot a + y^* \cdot b$ — искомое.

■

Следствие 1. *Пусть $a, b, c \in \mathbb{N}$ и $(a \cdot b) \vdots c$. Если $(a, c) = 1$, то $b \vdots c$.*

Доказательство. По предыдущей теореме найдутся такие $x, y \in \mathbb{Z}$, что $ax + cy = 1$. Умножим обе части этого равенства на b и получим представ-

ление $b = (ab) \cdot x + c \cdot (yb)$. Оба слагаемых в правой части делятся на c, поэтому, применив свойство линейности, получим $b \vdots c$.

■

Следствие 2. *Пусть* $a, b \in \mathbb{N}$ *и* $p \in P$. *Если* $(a \cdot b) \vdots p$, *то* $a \vdots p$ *или* $b \vdots p$.

Доказательство. Поскольку p — простое число, a и p могут иметь только два общих делителя: p и 1. В первом случае получим $a \vdots p$. Во втором — $(a, p) = 1$ и по предыдущему следствию $b \vdots p$.

■

Следствие 3. *Пусть* $a, b, c \in \mathbb{N}$ *и одновременно выполняются условия:* $c \vdots a$ *и* $c \vdots b$. *Если* $(a, b) = 1$, *то* $c \vdots (a \cdot b)$.

Доказательство. Из условия $c \vdots a$ найдем такое $k \in \mathbb{N}$, что $c = ak$. Учитывая, что $c = ak \vdots b$ и $(a, b) = 1$, по первому следствию получим $k \vdots b$, т.е. $k = b \cdot l$ для некоторого $l \in \mathbb{N}$. Таким образом, $c = (ab) \cdot l \vdots (a \cdot b)$.

■

Определение. *Если* $a, b, c \in \mathbb{N}$ *и* $a = b \cdot c$, *то* b *называют частным от деления* a *на* c *и обозначают* $b = \frac{a}{c} = a/c$.

В последнем следствии докажем формулу, связывающую между собой (a, b) и НОК (a, b).

Следствие 4. *Пусть* $a, b \in \mathbb{N}$. *Тогда* $НОК(a, b) = \dfrac{a \cdot b}{(a, b)}$.

Доказательство. Пусть $d^* = (a, b)$, $a = d^* \cdot a_1$, $b = d^* \cdot b_1$ для некоторых $a_1, b_1 \in \mathbb{N}$ (причем нетрудно заметить, что $(a_1, b_1) = 1$). Тогда

$$k^* = \frac{a \cdot b}{(a, b)} = \frac{(d^* \cdot a_1) \cdot (d^* \cdot b_1)}{d^*} = a_1 \cdot b_1 \cdot d^* = (a_1 \cdot d^*)b_1 = a_1(b_1 \cdot d^*).$$

Из последних двух представлений получим, что $k^* \vdots a$ и $k^* \vdots b$, т.е. является общим кратным чисел a и b. Осталось проверить, что это минимальное из всех общих кратных.

Рассмотри теперь k — произвольное общее кратное чисел a и b. Из условия $k \vdots a$ найдем такое $l \in \mathbb{N}$, что $k = a \cdot l$. Учитывая теперь, что $k = (a_1 \cdot d^*)l \vdots b$ или $(a_1 \cdot d^*)l \vdots (b_1 \cdot d^*)$, приходим к $(a_1 \cdot l) \vdots b_1$. Вспомним наше замечание, что $(a_1, b_1) = 1$, поэтому первое следствие нам дает $l \vdots b_1$, т.е. $l = b_1 \cdot m$ для некоторого $m \in \mathbb{N}$. В результате $k = (a_1 \cdot d^* \cdot b_1)m = k^* \cdot m$, т.е. $k \geqslant k^*$, и минимальность k^* доказана.

■

Следующий несложный результат громко называется *основной теоремой арифметики.*

Теорема 7.4. *Произвольное натуральное число* n, *большее единицы, можно представить в виде произведения простых множителей (возможно, одного), причем такое представление единственно с точностью до перестановки сомножителей.*

Доказательство. I. Существование такого представления докажем индукцией по n.

Б.И. $n = 2$. Представление $n = 2$ уже является искомым.

Ш.И. Предположим, что утверждение верно для всех меньших чем n натуральных чисел. Докажем его для n. Если n является простым числом p, то представление $n = p$ — искомое. Рассмотрим теперь случай составного числа n. Обозначим через p_1 его наименьший делитель, который отличен от 1, тогда по теореме 6.2 получим, что $p_1 \in P$, $n = p_1 \cdot k$, где $k \in \mathbb{N}$. Учитывая, что $k < n$, можно воспользоваться предположением индукции и записать $k = p_2 \cdot \ldots \cdot p_m$, где $p_i \in P$ при всех $i \in \{2, \ldots, m\}$. В итоге, $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$ — искомое представление.

II. Докажем единственность такого представления с точностью до перестановки сомножителей. О/п: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ — два различных разложения на простые множители. Из условий $q_1 \cdot q_2 \cdot \ldots \cdot q_l \vdots p_1$, $p_1 \in P$, применяя второе следствие, найдем такое q_i, что $q_i \vdots p_1$. Но $q_i \in P$, поэтому такая делимость возможна только в случае $q_i = p_1$. Мы можем переставлять сомножители, поэтому, не ограничивая общности, считаем, что $q_1 = p_1$ (просто перенумеруем множители второго представления). К равенству $p_1 \cdot p_2 \cdot \ldots \cdot p_m = p_1 \cdot q_2 \cdot \ldots \cdot q_l$ применим правило сокращения для произведения и получим $p_2 \cdot \ldots \cdot p_m = q_2 \cdot \ldots \cdot q_l$. Рассуждая аналогично, получим $p_2 = q_2$ и т.д. Осталось только проверить, что $m = l$. Если, например, $m < l$, то после сокращения, придем к равенству $1 = q_{m+1} \cdot \ldots \cdot q_l$, что невозможно. Таким образом, доказано, что $p_1 \cdot p_2 \cdot \ldots \cdot p_m$ и $q_1 \cdot q_2 \cdot \ldots \cdot q_l$ могут отличаться только порядком сомножителей. $\nleftrightarrow$.

■

Определение. *Каноническим представлением* $n \in \mathbb{N}$, $n > 1$ *называется запись* $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_l^{k_l}$, *где* $p_i \in P$, $k_i \in \mathbb{N}$ *при всех* $i \in \{1, 2, \ldots, l\}$ *и* $p_i \neq p_j$ *при* $i \neq j$.

Пример 2. Выражения 10^6 или $2^2 \cdot 5^6 \cdot 2^4$ не являются каноническими представлениями миллиона, а $2^6 \cdot 5^6$ или $5^6 \cdot 2^6$ — являются.

Каноническое представление поможет нам при выводе формулы Эйлера и для определения количества делителей произвольного натурального числа. Здесь же ограничимся только парой упражнений.

Упражнения

Пусть натуральные числа a и b представлены в канонической форме:

$$a = p_1^{x_1} \cdot p_2^{x_2} \cdot \ldots \cdot p_l^{x_l} \cdot q_1^{y_1} \cdot \ldots \cdot q_m^{y_m}, \quad b = p_1^{z_1} \cdot p_2^{z_2} \cdot \ldots \cdot p_l^{z_l} \cdot s_1^{t_1} \cdot \ldots \cdot s_n^{t_n},$$

где $\{p_1, p_2, \ldots, p_l\}$ — все общие (для a и b) простые делители, т.е. выполняется $\{q_1, \ldots, q_m\} \cap \{s_1, \ldots, s_n\} = \varnothing$.

1. Докажите, что

$$\text{НОД}(a, b) = p_1^{\min\{x_1,\, z_1\}} \cdot p_2^{\min\{x_2,\, z_2\}} \cdot \ldots \cdot p_l^{\min\{x_l,\, z_l\}}.$$

2. Докажите, что

$$\text{НОК}(a, b) = p_1^{\max\{x_1,\, z_1\}} \cdot p_2^{\max\{x_2,\, z_2\}} \cdot \ldots \cdot p_l^{\max\{x_l,\, z_l\}} \cdot q_1^{y_1} \cdot \ldots \cdot q_m^{y_m} \cdot s_1^{t_1} \cdot \ldots \cdot s_n^{t_n}.$$

3. Найдите $d(a)$ — количество всех натуральных делителей числа a (включая 1 и a).

4. Найдите сумму всех натуральных делителей числа a.

1.8. Сравнения по модулю и их свойства

Определение. *Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ и $m \geqslant 2$. Если при делении на m числа a и b дают один и тот же остаток, то a и b называются сравнимыми друг с другом по модулю m (обозначение: $a \equiv b \pmod m$ или $a \equiv_m b$).*

Например, $-25 \equiv 17 \pmod 7$ (каждое из этих чисел дает остаток 3 при делении на 7: $-25 = 7 \cdot (-4) + 3$, $17 = 7 \cdot 2 + 3$), но $-25 \not\equiv 17 \pmod 5$ (остатки 0 и 2 соответственно).

В проверке сравнимы ли два целых числа между собой поможет следующая теорема.

Теорема 8.1. *Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ и $m \geqslant 2$. Тогда следующие условия равносильны:*

1) $a \equiv b \pmod m$;

2) $(a - b) \vdots m$;

3) найдется такое $q \in \mathbb{Z}$, *что* $a = b + mq$.

Доказательство. 1) $\Rightarrow$ 2) из $a \equiv b \pmod m$ следует, что $a = mq_1 + r$ и $b = mq_2 + r$, где $q_1, q_2 \in \mathbb{Z}$. Поэтому $a - b = m(q_1 - q_2) \vdots m$.

2) $\Rightarrow$ 3) поскольку $(a - b) \vdots m$, найдется такое $q \in \mathbb{Z}$, что $a - b = mq$, откуда $a = b + mq$.

3) $\Rightarrow$ 1) разделим b на m с остатком: $b = mq^* + r$, где $q^* \in \mathbb{Z}$, $r \in \mathbb{Z}^+$, $0 \leqslant r < m$. Подставляя в равенство $a = b + mq$, получим $a = m(q^* + q) + r$, причем $(q^* + q) \in \mathbb{Z}$, $r \in \mathbb{Z}^+$, $0 \leqslant r < m$. Из теоремы о делении с остатком следует, что частное и остаток определяются единственным образом, поэтому a при делении на m, так же как и b, дает остаток r.

■

Сравнения по обладают многими полезными свойствами. Перечислим некоторые из них. Во всех этих свойствах считаем, что $m \in \mathbb{N}$ и $m \geqslant 2$.

I. Для любого $a \in \mathbb{Z}$ выполняется $a \equiv a \pmod m$ (рефлексивность).

Доказательство. Сразу следует из определения и единственности определения остатка.

■

II. Пусть $a, b \in \mathbb{Z}$. Тогда $a \equiv b \pmod m \Leftrightarrow b \equiv a \pmod m$ (симметричность).

Доказательство. Также следует из определения и единственности определения остатка.

■

III. Пусть $a, b, c \in \mathbb{Z}$. Тогда если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, то $a \equiv c \pmod m$ (транзитивность).

Доказательство. Аналогично доказательству предыдущего свойства.

■

IV. Пусть $a, b, a_1, b_1 \in \mathbb{Z}$ и $a \equiv b \pmod m$. Тогда $a_1 \equiv b_1 \pmod m \Leftrightarrow a + a_1 \equiv b + b_1 \pmod m$.

Доказательство. Согласно первой теореме нам дано, что $(a - b) \vdots m$. Теперь $(a_1 - b_1) \vdots m$ тогда и только тогда, когда $\Big((a-b)+(a_1-b_1)\Big) \vdots m$ (свойство (4) теоремы 6.1). Последнее перепишем в виде $\Big((a+a_1)-(b+b_1)\Big) \vdots m$, а это, по первой теореме, равносильно $a + a_1 \equiv b + b_1 \pmod m$.

■

V. Пусть $a, b, c \in \mathbb{Z}$. Тогда $a \equiv b \pmod{m} \Leftrightarrow a + c \equiv b + c \pmod{m}$.

Доказательство. Следует из предыдущего свойства и $c \equiv c \pmod{m}$.

■

VI. Пусть $a, b, q \in \mathbb{Z}$. Тогда $a \equiv b \pmod{m} \Leftrightarrow a + mq \equiv b \pmod{m}$.

Доказательство. Аналогично предыдущему свойству, но с учетом очевидного сравнения $mq \equiv 0 \pmod{m}$.

■

VII. Пусть $a, b, a_1, b_1 \in \mathbb{Z}$, $a \equiv b \pmod{m}$ и $a_1 \equiv b_1 \pmod{m}$. Тогда $a \cdot a_1 \equiv b \cdot b_1 \pmod{m}$.

Доказательство. Немного преобразуем разность

$$aa_1 - bb_1 = aa_1 - a_1b + a_1b - bb_1 = a_1(a - b) + b(a_1 - b_1).$$

По условию и первой теореме оба выражения в скобках делятся на m. Следовательно $aa_1 - bb_1 \vdots m$. Применяя первую теорему, получим $a \cdot a_1 \equiv b \cdot b_1 \pmod{m}$.

■

Заметим, что предыдущее утверждение действует только в одну сторону: умножать сравнения по одному модулю друг на друга можно, а вот делить (в общем случае) — нет. Сравнения $4 \equiv 2 \pmod{2}$ и $2 \equiv 2 \pmod{2}$ выполняются, но после деления получим $2 \not\equiv 1 \pmod{2}$.

Натуральная степень произвольного целого числа a легко определяется по индукции: $a^1 = a$ и $a^{n+1} = a^n \cdot a$. Кроме того, для положительных чисел по определению считают, что $a^0 = 1$.

VIII. Пусть $a, b \in \mathbb{Z}$ и $a \equiv b \pmod{m}$. Тогда для любого $n \in \mathbb{N}$ выполняется $a^n \equiv b^n \pmod{m}$.

Доказательство. Достаточно воспользоваться предыдущим свойством n раз.

■

Обратить это свойство также не получится: извлекать корни из сравнений нельзя ($9 \equiv 1 \pmod{8}$ и $3 \not\equiv 1 \pmod{8}$).

Следующее свойство позволяет делить обе части сравнения и модуль на одно и то же натуральное число.

IX. Пусть $a, b, a_1, b_1 \in \mathbb{Z}$, $d, m_1 \in \mathbb{N}$, $a, b, m \vdots d$ и $a = d \cdot a_1$, $b = d \cdot b_1$, $m = d \cdot m_1$. Тогда $a \equiv b \pmod{m} \Leftrightarrow a_1 \equiv b_1 \pmod{m_1}$.

Доказательство. По первой теореме условие $a \equiv b \pmod{m}$ равносильно $(a - b) \vdots m$ или $(da_1 - db_1) \vdots (dm_1)$. По определению найдется такое

$k \in \mathbb{Z}$, что $(da_1 - db_1) = k \cdot (dm_1)$. Правило сокращения для произведения приведет нас к равносильному условию $a_1 - b_1 = k \cdot m_1$, которое по определению означает $(a_1 - b_1) \vdots m_1$. По первой теореме это равносильно тому, что выполняется $a_1 \equiv b_1 \pmod{m_1}$.

■

Если в предыдущем свойстве условие $m \vdots d$ заменить условием $(m, d) = 1$, то можно сократить на d обе части сравнения, а модуль оставить прежним.

X. Пусть $a, b, a_1, b_1 \in \mathbb{Z}$, $d \in \mathbb{N}$, $a, b \vdots d$, $(m, d) = 1$ и $a = d \cdot a_1$, $b = d \cdot b_1$. Тогда $a \equiv b \pmod{m} \Leftrightarrow a_1 \equiv b_1 \pmod{m}$.

Доказательство. $\Rightarrow$) переходим от $a \equiv b \pmod{m}$ к равносильному условию $d(a_1 - b_1) \vdots m$. Учитывая, что $(m, d) = 1$, по следствию 1 из теоремы 7.3 получим $(a_1 - b_1) \vdots m$, что равносильно $a_1 \equiv b_1 \pmod{m}$.

$\Leftarrow$) если $(a_1 - b_1) \vdots m$, то тем более $d(a_1 - b_1) \vdots m$. Последнее равносильно $a \equiv b \pmod{m}$.

■

XI. Пусть $a, b \in \mathbb{Z}$ и $a \equiv b \pmod{m}$. Тогда $(a, m) = (b, m)$.

Доказательство. Введем обозначения: $d_1 = (a, m)$ и $d_2 = (b, m)$. По первой теореме условие $a \equiv b \pmod{m}$ перепишем в виде

$$(*) \qquad a = b + mq, \quad \text{для некоторого} \quad q \in \mathbb{Z}.$$

1) из $a, m \vdots d_1$ и уравнения $(*)$ получим, что $b \vdots d_1$. Раз $b, m \vdots d_1$, а $d_2 = (b, m)$, получим $d_2 \geqslant d_1$.

2) аналогично рассуждая, из $b, m \vdots d_2$ и уравнения $(*)$ получим, что $a \vdots d_2$. Раз $a, m \vdots d_2$, а $d_1 = (a, m)$, получим $d_1 \geqslant d_2$.

Антисимметричность порядка и результаты (1) и (2) дают $d_1 = d_2$.

■

Нередко мы будем использовать частный случай предыдущего результата:

Следствие. *Пусть* $a, b \in \mathbb{Z}$ *и* $a \equiv b \pmod{m}$. *Тогда* $(a, m) = 1 \Leftrightarrow (b, m) = 1$.

Доказательство. Сразу следует из предыдущего свойства.

■

Напомним, что *десятичная запись* натурального числа $n = \overline{a_k a_{k-1} \ldots a_2 a_1}$, где $a_i \in C_0 = \{0, 1, 2, \ldots, 9\}$, $i \in \{1, \ldots, k\}$, $a_k \neq 0$, является сокращением

представления

$$n = a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + \ldots + a_k \cdot 10^{k-1} = \sum_{i=1}^{k} a_i \cdot 10^{i-1}.$$

Черта сверху в записи n означает, что a_i не перемножаются, а являются цифрами в позиционной системе счисления (в которой смысл a_i зависит от разряда, который занимает эта цифра). При этом *суммой цифр* числа $n \in \mathbb{N}$ называется функция $s(n) = a_1 + a_2 + \ldots + a_k = \sum\limits_{i=1}^{k} a_i$. *Знакопеременной суммой цифр* числа $n \in \mathbb{N}$ называется функция

$$s_-^+(n) = a_1 - a_2 + a_3 - \ldots + (-1)^{k+1} a_k = \sum_{i=1}^{k} (-1)^{i+1} a_i.$$

Первые простые критерии делимости описывают делимость натурального числа $n = \overline{a_k a_{k-1} \ldots a_2 a_1}$ на 2^p ($p \in \mathbb{N}$ и $p \leqslant k$). Учитывая, что $10^p \vdots 2^p$ и представление

$$n = a_1 + a_2 \cdot 10 + \ldots + a_p \cdot 10^{p-1} + \ldots + a_k \cdot 10^{k-1} = \overline{a_p \ldots a_2 a_1} + 10^p \cdot \overline{a_k a_{k-1} \ldots a_{p+1}}$$

из свойства линейности получаем, что $n \vdots 2^p$ тогда и только тогда, когда число, образованное его последними p цифрами (т.е. $\overline{a_p \ldots a_2 a_1}$) делится на 2^p. Чуть более сложные критерии делимости могут быть получены из следующей теоремы.

Теорема 8.2. *Если* $\overline{a_k a_{k-1} \ldots a_2 a_1}$ *— десятичная запись* $n \in \mathbb{N}$, *то*

1) $n \equiv s(n) \pmod 3$;

2) $n \equiv s(n) \pmod 9$;

3) $n \equiv s_-^+(n) \pmod{11}$.

Доказательство. 1) из сравнения $10 \equiv 1 \pmod 3$ по свойству VIII получим $10^{i-1} \equiv 1 \pmod 3$. Умножим (используя VII) это сравнение на $a_i \equiv a_i \pmod 3$, получим $a_i \cdot 10^{i-1} \equiv a_i \pmod 3$. Теперь сложим (используя IV) все получившиеся сравнения при $i \in \{1, 2, \ldots, k\}$. Имеем

$$n = \sum_{i=1}^{k} a_i \cdot 10^{i-1} \equiv \sum_{i=1}^{k} a_i \pmod 3.$$

2) доказывается аналогично предыдущему свойству, заменой модуля на 9.

3) проводим доказательство аналогично (1) с учетом $10 \equiv -1 \pmod{11}$ по свойству VIII получим $10^{i-1} \equiv (-1)^{i-1} \pmod{11}$. Очевидно, что $(-1)^{i-1}$ можно заменить на равное ему число $(-1)^{i+1}$, поэтому

$$n = \sum_{i=1}^{k} a_i \cdot 10^{i-1} \equiv \sum_{i=1}^{k} (-1)^{i+1} a_i \pmod{11}.$$

■

Следствие. *Если* $\overline{a_k a_{k-1} \dots a_2 a_1}$ *— десятичная запись* $n \in \mathbb{N}$, *то*

1) $n \vdots 3 \Leftrightarrow s(n) \vdots 3$;

2) $n \vdots 9 \Leftrightarrow s(n) \vdots 9$;

3) $n \vdots 11 \Leftrightarrow s^{+}_{-}(n) \vdots 11$.

Доказательство. Утверждения (1)–(3) являются частными случаями результатов (1)–(3) (соответственно) предыдущей теоремы, поскольку делимость легко переписывается в виде сравнения: $n \vdots m \Leftrightarrow n \equiv 0 \pmod{m}$ для любого $m \in \mathbb{N}$, $m \geqslant 2$.

■

Пример 1. Выясним, делится ли на 11 число $n = \overline{187096162938773}$. Для этого найдем

$$s^{+}_{-}(n) = 3 - 7 + 7 - 8 + 3 - 9 + 2 - 6 + 1 - 6 + 9 - 0 + 7 - 8 + 1 = -11 \vdots 11.$$

Поэтому $n \vdots 11$.

Пример 2. Найдем цифры a и b, если число $n = \overline{5b4567a} \vdots 45$. Представим $45 = 5 \cdot 9$, и, учитывая взаимную простоту 5 и 9, проверим делимость n на 5 и на 9. Из $n \vdots 5$ следует, что $a = 5$ или $a = 0$. Делимость на 9 равносильна делимости $s(n) = (27 + a + b) \vdots 9$ или $(a + b) \vdots 9$. Если $a = 5$, то единственной подходящей цифрой будет $b = 4$. При $a = 0$ подойдут две цифры: $b = 0$ и $b = 9$. В результате, искомыми числами будут: 5445675, 5045670, 5945670.

1.9. Полная система вычетов. Теорема Ферма

Определение. *Пусть* $m \in \mathbb{N}$, $m \geqslant 2$. *Множество всех целых чисел, дающих один и тот же остаток при делении на* m, *называется классом вычетов по модулю* m. *Класс вычетов* $K_m(r)$ *состоит из всех целых чисел, дающих при делении на* m *остаток* r, *где* $r \in \{0, 1, \ldots, m-1\}$.

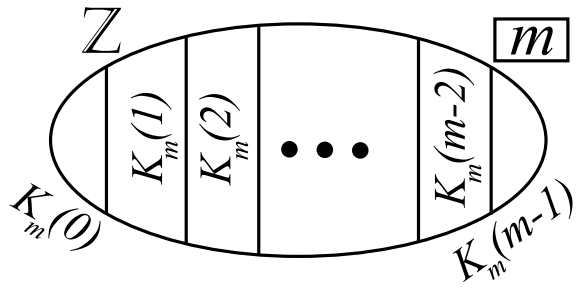

Рис. 1

Из определения следует существование ровно m классов вычетов по модулю m. Мы доказывали, что остаток при делении на m определяется однозначно (теорема 6.4), поэтому различные классы вычетов по модулю m не пересекаются между собой. Разбиение множества $\mathbb{Z}$ на классы вычетов изображено на рис. 1 и называется «батоном по модулю m». По теореме 8.1 все элементы класса $K_m(r)$ можно задать простой формулой:

$$a \in K_m(r) \Leftrightarrow a = mq + r \quad \text{для некоторого} \quad q \in \mathbb{Z}.$$

Определение. *Если из каждого класса вычетов по модулю* m *выбрать ровно по одному элементу, то полученное множество* x_1, x_2, $\ldots$, x_m *называют полной системой вычетов по модулю* m *(обозначение — ПСВ*$_m$*).*

Пример 1. Если $m = 5$, то $\{0, 1, 2, 3, 4\}$, $\{-5, 6, 12, -2, -6\}$ являются ПСВ$_5$. Часто мы будем предпочитать первую из них, состоящую из остатков от деления на модуль. Такие системы специально называются.

Определение. *Если из каждого класса вычетов по модулю* m *выбрать наименьшее неотрицательное число, то полученное множество, состоящее из* 0, 1, $\ldots$, $(m-1)$, *называют полной системой наименьших неотрицательных вычетов по модулю* m *(обозначение — ПСННВ*$_m$*).*

При фиксированном модуле m существует бесконечно много ПСВ$_m$, но только одна ПСННВ$_m$. Установим несколько свойств ПСВ$_m$.

Лемма 9.1. *Пусть* $y_1, y_2, \ldots, y_m \in \mathbb{Z}$ *и* $y_i \not\equiv y_j \pmod m$ *при* $i \neq j$. *Тогда* $\{y_1, y_2, \ldots, y_m\}$ *является ПСВ*$_m$.

Доказательство. Так как $y_i \not\equiv y_j \pmod m$ при $i \neq j$, то y_i и y_j лежат в разных классах вычетов по модулю m. С другой стороны, существует всего m различных классов для модуля m, поэтому во множестве

$\{y_1, y_2, \ldots, y_m\}$ будут представители всех классов.

■

Целые числа a и b называются взаимно простыми (используем привычное обозначение $(a, b) = 1$), если 1 является единственным их общим натуральным делителем. При этом $a \in \mathbb{Z}$ делится на $n \in \mathbb{N}$, если остаток от деления a на n равен нулю.

Лемма 9.2. *Пусть* $\{x_1, x_2, \ldots, x_m\}$ — *ПСВ* $_m$, $(a, m) = 1$ *и* b — *произвольное целое число. Тогда* $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ — *ПСВ* $_m$.

Доказательство. Обозначим через $y_i = ax_i + b$ для всех $i \in \{1, 2, \ldots, m\}$. Согласно предыдущей лемме достаточно показать, что $y_i \not\equiv y_j \pmod m$ при $i \neq j$. О/п: нашлась такая пара различных индексов, что $y_i \equiv y_j \pmod m$. Воспользуемся свойствами IV и X сравнений и получим

$$ax_i + b \equiv ax_j + b \pmod m \Leftrightarrow ax_i \equiv ax_j \pmod m \Leftrightarrow x_i \equiv x_j \pmod m.$$

Последнее противоречит тому, что x_i и x_j выбирались из разных классов вычетов по модулю m.

■

Следующее утверждение называется теоремой Ферма[12] (или, точнее, *Малой теоремой Ферма*[13]).

Теорема 9.3. *Пусть* p — *простое число,* $a \in \mathbb{Z}$ *и* p *не делит* a. *Тогда* $a^{p-1} \equiv 1 \pmod p$.

Доказательство. Рассмотрим $\{0, 1, 2, \ldots, p-1\}$ — ПСННВ $_p$. Так как p — простое число и p не делит a, то $(a, p) = 1$. По предыдущей лемме множество $\{0, a, 2a, \ldots, (p-1)a\}$ является ПСВ $_p$. Разделим каждый элемент этой системы на p с остатком: $0 = 0 \cdot p + 0$; $1 \cdot a = pq_1 + r_1$, $q_1 \in \mathbb{Z}$, $0 < r_1 < p$; $2 \cdot a = pq_2 + r_2$, $q_2 \in \mathbb{Z}$, $0 < r_2 < p$; $\ldots$; $(p-1) \cdot a = pq_{p-1} + r_{p-1}$, $q_{p-1} \in \mathbb{Z}$, $0 < r_{p-1} < p$. Учитывая, что $i \cdot a - r_i = pq_i \vdots p$, эти равенства можно переписать в виде p штук сравнений:

0) $0 \cdot a \equiv 0 \pmod p$;
1) $1 \cdot a \equiv r_1 \pmod p$, $0 < r_1 < p$;
2) $2 \cdot a \equiv r_2 \pmod p$ $0 < r_2 < p$;
$\vdots$

[12] Пьер Ферма (1601–1665) — французский математик, юрист по профессии; один из основоположников теории чисел и математического анализа; вывел формулы интегрирования по частям; сформулировал Великую теорему Ферма, которую не могли доказать более 350 лет, и Малую теорему Ферма.

[13] Мы приводим ее доказательство, принадлежащее шотландскому математику Джеймсу Айвори (1765–1842) и опубликованное в 1806 году.

i) $i \cdot a \equiv r_i \pmod{p} \qquad 0 < r_i < p\,;$

$\vdots$

$p-1\,)\quad (p-1)\cdot a \equiv r_{p-1} \pmod{p} \qquad 0 < r_{p-1} < p\,.$

Заметим, что в левой части этих сравнений стоят числа, которые образуют ПСВ $_p$. Элементы в правой части выбираются из тех же классов, поэтому они также образуют ПСВ $_p$. Этим объясняется неравенство $r_i \neq 0$ при $i \geqslant 1$ (ведь остаток 0 получен в первом уравнении). Далее, раз все r_i удовлетворяют двойному неравенству $0 < r_i < p$, то $\{0, r_1, r_2, \ldots, r_{p-1}\}$ — ПСННВ $_p$. С учетом того, что ПСННВ $_p$ существует только одна, получим равенство двух множеств: $\{0, 1, 2, \ldots, p-1\} = \{0, r_1, r_2, \ldots, r_{p-1}\}$ (будьте осторожны, порядок чисел в этих системах может быть разным и r_5 может совпасть, например с 1, а r_1 — с 2). Исключив ноль из этих двух множеств, получим условие, которое обозначим звездочкой:

$$\{1, 2, \ldots, p-1\} = \{r_1, r_2, \ldots, r_{p-1}\}. \qquad (*)$$

Теперь перемножим (это можно сделать по свойству VII) сравнения с номерами от (1) до $(\,p-1\,)$ и придем к сравнению

$$\Big(1 \cdot 2 \cdot \ldots \cdot (p-1)\Big) \cdot a^{p-1} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \pmod{p}.$$

Из-за простоты p, все меньшие p натуральные числа будут взаимно простыми с p, поэтому $(r_i, p) = 1$ для каждого индекса $i \leqslant (p-1)$. Учитывая равенство $(*)$, каждый множитель r_i будет присутствовать в скобках в левой части, поэтому на него можно сократить (используем свойство X сравнений). После $(p-1)$-го таких сокращений, получим $a^{p-1} \equiv 1 \pmod{p}$.

■

Следствие. *Пусть p — простое число, $a \in \mathbb{Z}$. Тогда $a^p \equiv a \pmod{p}$.*

Доказательство. Если $a \vdots p$, то сравнение $a^p \equiv a \pmod{p}$ выполняется, так как обе его части сравнимы с нулем.

Пусть a не делится на p, тогда по теореме Ферма имеем $a^{p-1} \equiv 1 \pmod{p}$. Домножая это сравнение на $a \equiv a \pmod{p}$, получим требуемое.

■

Пример 2. Найдем остаток от деления 2020^{2100} на 43. Ясно, что $43 \in P$ и 43 не делит 2020 (так как $2020 = 2^2 \cdot 5 \cdot 101$ — каноническое представление). По теореме Ферма получим $2020^{42} \equiv 1 \pmod{43}$. Возведем это сравнение в 50-ю степень и получим $2020^{2100} \equiv 1 \pmod{43}$. В результате, искомый остаток равен единице.

1.10. Функция Эйлера. Теорема Эйлера

Определение. *Пусть* $n \in \mathbb{N}$. *Функцией Эйлера от* n *называется число* $\varphi(n)$, *равное количеству натуральных чисел в диапазоне от* 1 *до* n, *которые являются взаимно простыми с* n.

П р и м е р 1. В следующей таблице приведем для первой дюжины натуральных n список всех чисел, которые не превосходят n и взаимно простые с n, а также значения $\varphi(n)$.

n	числа от 1 до n и взаимно простые с n	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	10
12	1, 5, 7, 11	4

Наша цель — найти формулу для $\varphi(n)$. Начнем с простого вспомогательного утверждения.

Лемма 10.1. *Пусть* $a, b, c \in \mathbb{N}$. *Тогда выполняется* $(a \cdot b, c) = 1$ *тогда и только тогда, когда одновременно* $(a, c) = 1$ *и* $(b, c) = 1$.

Доказательство. $\Rightarrow$) о/п: б.о.о. предположим, что $(a, c) = d > 1$. Тогда $a \cdot b \vdots d$ и $c \vdots d$, поэтому $(a \cdot b, c) \geqslant d$. $\lightning$.

$\Leftarrow$) о/п: предположим, что $(a \cdot b, c) = d > 1$ и p — простой делитель d (если d — простое число, то $p = d$; иначе применим теорему 6.2). Тогда $a \cdot b \vdots p$ и $c \vdots p$. Из первого условия получим $a \vdots p$ или $b \vdots p$, что дает $(a, c) \geqslant p$ или $(b, c) \geqslant p$. $\lightning$.

■

Определение. *Класс вычетов* $K_m(r)$ *называется* m*-простым классом, если все его элементы взаимно простые с модулем* m.

Сразу заметим, что если один элемент a класса $K_m(r)$ взаимно прост с модулем m, то и остальные элементы $K_m(r)$ также взаимно просты с модулем (по следствию из свойства XI сравнений).

Следствие 1. *Количество m-простых классов равно $\varphi(m)$.*

Доказательство. Из замечания выше следует, что $K_m(r)$ является m-простым классом тогда и только тогда, когда $(r, m) = 1$. Поэтому количество m-простых классов совпадает с количеством натуральных чисел от 1 до m, которые взаимно простые с m (элемент m мы выбрали из класса $K_m(0)$). Последнее количество по определению равно $\varphi(m)$.

■

Определение. *Пусть $m \in \mathbb{N}$, $m > 1$. Если из каждого m-простого класса выбрать ровно по одному числу, то полученное множество называется приведенной системой вычетов по модулю m (ПрСВ$_m$). Если из каждого m-простого класса выбрать наименьшее натуральное число, то полученное множество называется приведенной системой наименьших неотрицательных вычетов по модулю m (ПрСННВ$_m$).*

Следствие 2. *1) любая ПрСВ$_m$ содержит $\varphi(m)$ элементов.*

2) в любой ПСВ$_m$ можно выбрать ровно $\varphi(m)$ элементов, которые образуют ПрСВ$_m$.

Доказательство. 1) сразу следует из предыдущего следствия, так как количество m-простых классов равно $\varphi(m)$ и в каждой ПрСВ$_m$ есть ровно один представитель каждого m-простого класса.

2) в любой ПСВ$_m$ есть по одному представителю каждого классов вычетов. Выбираем из них только те элементы, которые лежат в m-простых классах. Их $\varphi(m)$ штук и они образуют ПрСВ$_m$.

■

Пример 2. Пусть $m = 6$. Для этого модуля $\varphi(6) = 2$ существует только два 6-простых класса: $K_6(1)$ и $K_6(5)$. Множества $\{-5, -7\}$ и $\{7, -1\}$ являются двумя примерами (из бесконечного множества) приведенных систем вычетов по модулю 6. Единственной ПрСННВ$_6$ будет $\{1, 5\}$.

В следующей теореме докажем некоторые свойства функции $\varphi(m)$, которых окажется достаточно для вывода формулы для $\varphi(m)$.

Теорема 10.2.

1) для любого $p \in P$ *выполняется, что* $\varphi(p) = p - 1$ *;*

2) для любого $p \in P$ *и для каждого* $k \in \mathbb{N}$ *верно, что* $\varphi(p^k) = p^k - p^{k-1}$ *;*

3) если $(a, b) = 1$ *, то* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *(мультипликативность функции Эйлера).*

Доказательство. 1) если p — простое число, то все меньшие его натуральные числа — 1 , 2 , $\ldots$, $p-1$ — будут взаимно простыми с p , поэтому $\varphi(p) = p - 1$.

2) всего натуральных чисел от 1 до p^k ровно p^k штук. Определим, сколько из них **не** будут взаимно простыми с p^k . Натуральное a удовлетворяет условиям $a \leqslant p^k$ и $(a, p^k) = d > 1$ тогда и только тогда, когда $a \leqslant p^k$ и $a \vdots p$. Последнее равносильно $a \leqslant p^k$ и $a = p \cdot l$ для некоторого $l \in \mathbb{N}$. Получим $p \cdot l \leqslant p^k$ или $l \leqslant p^{k-1}$, поэтому $l \in \{1, 2, 3, \ldots, p^{k-1}\}$. Последнее означает, что для любого не взаимно простого с p^k числа a справедливо $a \in \{1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^{k-1} \cdot p\}$. В последнем множестве ровно p^{k-1} чисел, поэтому, вычитая это число из общего количества рассматриваемых чисел, приходим к формуле $\varphi(p^k) = p^k - p^{k-1}$.

3) все натуральные числа от 1 до $a \cdot b$ запишем в виде следующей прямоугольной таблицы[14] с b строчками и a столбцами:

1-й столбец	2-й столбец	3-й столбец	$\ldots$	i-й столбец	$\ldots$	a-й столбец
1	2	3	$\ldots$	i	$\ldots$	a
$a+1$	$a+2$	$a+3$	$\ldots$	$a+i$	$\ldots$	$2a$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$(j-1)a+1$	$(j-1)a+2$	$(j-1)a+3$	$\ldots$	$(j-1)a+i$	$\ldots$	ja
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$
$(b-1)a+1$	$(b-1)a+2$	$(b-1)a+3$	$\ldots$	$(b-1)a+i$	$\ldots$	ba

По предыдущей лемме нам достаточно определить количество чисел от 1 до $a \cdot b$, которые одновременно взаимно просты и с a , и с b .

I. Выясним сначала, как расположены в этой таблице числа, которые взаимно простые с a . Заметим, что числа в одном столбце дают одинаковый остаток при делении на a (поскольку имеют вид $qa + i$). Это означает, что как только одно число такого столбца окажется взаимно простым с a , то

[14] Она называется матрицей с b строчками и a столбцами или $b \times a$ -матрицей.

все будет взаимно простыми с a. Такой столбец, состоящий из чисел, которые взаимно простые с a, будем называть a-подходящим. По определению функции Эйлера, в первой строке — $1, 2, 3, \ldots, i, \ldots, a$ — находится ровно $\varphi(a)$ чисел, которые взаимно простые с a. Таким образом, числа, которые взаимно простые с a, расположены только в a-подходящих столбцах, и количество таких столбцов равно $\varphi(a)$.

II. Теперь рассмотрим произвольный i-й столбец: $0 \cdot a + i$, $1 \cdot a + i$, $2 \cdot a + i$, $\ldots$, $(b-1)a + i$. Докажем, что он является ПСВ$_b$. Если все элементы ПСННВ$_b$ (т.е. $0, 1, 2, \ldots, (b-1)$) умножить на a, которое по условию взаимно простое с b, и прибавить одно и то же число i, то по лемме 9.2 получим, что множество $\{0 \cdot a + i, 1 \cdot a + i, 2 \cdot a + i, \ldots, (b-1)a + i\}$ является ПСВ$_b$. По следствию 2 из определения имеем: в каждом столбце $\varphi(b)$ чисел, которые взаимно простые с b.

Итак, количество чисел, которые взаимно простые и с a, и с b одновременно, равно $\varphi(a) \cdot \varphi(b)$ (количество a-подходящих столбцов умножить на количество элементов в них, которые взаимно простые с b). Мы доказали, что если $(a, b) = 1$, то $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

■

Заметим, что в общем случае (без дополнительного предположения о том, что $(a, b) = 1$) мультипликативность функции Эйлера не выполняется. Например, $4 = \varphi(8) \neq \varphi(4)\varphi(2) = 2 \cdot 1 = 2$.

Следствие 1. *Пусть* $a = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ — *каноническое представление* $a \in \mathbb{N}$. *Тогда*

$$\varphi(a) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdot \ldots \cdot \left(p_n^{k_n} - p_n^{k_n-1}\right).$$

Доказательство. Если простые числа p и q различны, то не только $(p, q) = 1$, но и для любых их натуральных степеней выполняется равенство $(p^k, q^l) = 1$ (иначе последовательно получим $q^l \vdots p$, $q \vdots p$, $q = p$). Поэтому можно использовать свойства (3) и (2) предыдущей теоремы:

$$\varphi(a) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_n^{k_n}) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdot \ldots \cdot \left(p_n^{k_n} - p_n^{k_n-1}\right).$$

■

Пример 3. Определим $\varphi(360)$. Для этого найдем канонический вид $360 = 2^3 \cdot 3^2 \cdot 5$. Подставляя в формулу, получим

$$\varphi(360) = \left(2^3 - 2^2\right)\left(3^2 - 3^1\right) \cdot \left(5^1 - 5^0\right) = 4 \cdot 6 \cdot 4 = 96.$$

Следствие 2. *Путь* $a = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ — *каноническое представление* $a \in \mathbb{N}$. *Тогда*

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right).$$

Доказательство. В формуле предыдущего следствия из i-ой скобки выносим $p_i^{k_i}$, тогда перед скобками получим канонический вид числа a.

■

Пример 4. Второй вариант формулы Эйлера можно использовать в отношении такого числа a, для которого мы знаем все его простые делители и по какой-то причине не хотим определять степень, с которой они входят в каноническое разложение. Определим значение $\varphi(10^n)$ для любого $n \in \mathbb{N}$. Очевидно, что 10^n делят только два простых числа: 2 и 5. По следствию 2 получим

$$\varphi(10^n) = 10^n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10^n \cdot \frac{1}{2} \cdot \frac{4}{5} = 4 \cdot 10^{n-1}.$$

Так, например, $\varphi(100) = 40$, $\varphi(1000) = 400$.

Лемма 10.3. *Пусть* $m \in \mathbb{N}$, $m \geqslant 2$.

1) если $x_1, \ldots, x_{\varphi(m)} \in \mathbb{Z}$, $(x_i, m) = 1$ $(\forall i \in \{1, 2, \ldots, \varphi(m)\})$ *и* $x_i \not\equiv x_j \pmod m$ *при* $i \neq j$, *то множество* $\{x_1, \ldots, x_{\varphi(m)}\}$ *является ПрСВ* $_m$.

2) пусть $\{x_1, \ldots, x_{\varphi(m)}\}$ — *ПрСВ* $_m$ *и* $(a, m) = 1$, *тогда* $\{ax_1, \ldots, ax_{\varphi(m)}\}$ *также будет ПрСВ* $_m$.

Доказательство. 1) элементы этого множества выбираются из разных классов вычетов по модулю m, поскольку $x_i \not\equiv x_j \pmod m$ при $i \neq j$. Условие $(x_i, m) = 1$ дает, что каждый элемент этой системы лежит в m-простом классе. Всего m-простых классов $\varphi(m)$ штук, что совпадает с количеством элементов в системе $\{x_1, \ldots, x_{\varphi(m)}\}$. Таким образом, это множество удовлетворяет определению ПрСВ $_m$.

2) поскольку $(a, m) = 1$ и $(x_i, m) = 1$, по первой лемме получим, что $(ax_i, m) = 1$. С учетом (1) осталось доказать, что $ax_i \not\equiv ax_j \pmod m$ при $i \neq j$. О/п: для некоторых различных индексов i и j выполняется $ax_i \equiv ax_j \pmod m$. Сократим обе части этого сравнения на число a, которое взаимно простое с m, и получим $x_i \equiv x_j \pmod m$. Это противоречит тому, что x_i и x_j выбирались из разных классов вычетов.

■

Следующая теорема была доказана Леонардом Эйлером в 1763 году.

Теорема 10.4. *Пусть* $m \in \mathbb{N}$, $m \geqslant 2$. *Если* $a \in \mathbb{Z}$ *и* $(a, m) = 1$, *то* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказательство. Пусть $\{x_1, \ldots, x_{\varphi(m)}\}$ — ПрСННВ$_m$ (напомним, такая система определяется единственным образом). Из условия $(a, m) = 1$ и предыдущей леммы получим, что $\{ax_1, \ldots, ax_{\varphi(m)}\}$ — ПрСВ$_m$. Разделим каждый элемент этой системы на m с остатком: $ax_1 = mq_1 + r_1$, $q_1 \in \mathbb{Z}$, $0 < r_1 < m$; $ax_2 = mq_2 + r_2$, $q_2 \in \mathbb{Z}$, $0 < r_2 < m$; $\ldots$, $ax_{\varphi(m)} = mq_{\varphi(m)} + r_{\varphi(m)}$, $q_{\varphi(m)} \in \mathbb{Z}$, $0 < r_{\varphi(m)} < m$.

Учитывая, что $ax_i - r_i = mq_i \vdots m$, можно переписать эти равенства в виде сравнений:

$1)$ $\quad ax_1 \equiv r_1 \pmod{m}$, $\quad 0 < r_1 < m$;
$2)$ $\quad ax_2 \equiv r_2 \pmod{m}$, $\quad 0 < r_2 < m$;
$\vdots$
$\varphi(m))$ $\quad ax_{\varphi(m)} \equiv r_{\varphi(m)} \pmod{m}$, $\quad 0 < r_{\varphi(m)} < m$.

Поскольку r_i выбирается из того же класса, что и ax_i, заключаем, что $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ — ПрСВ$_m$. Двойные неравенства $0 < r_i < m$ усиливают предыдущий результат: $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ — ПрСННВ$_m$. Вспомним, что такая система определяется однозначно, поэтому справедливо

$$\{x_1, \ldots, x_{\varphi(m)}\} = \{r_1, r_2, \ldots, r_{\varphi(m)}\}. \qquad (*)$$

Порядок элементов в этих системах может быть разным (например $x_1 = r_5$), но наше доказательство от этого не будет зависеть.

Перемножив (по свойству VII) сравнения (1)–($\varphi(m)$), получим

$$a^{\varphi(m)} \cdot (x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \pmod{m}.$$

Теперь, учитывая $(*)$, для каждого множителя справа найдется равный ему множитель в скобках слева, кроме того, эти числа взаимно просты с модулем. Применяя $\varphi(m)$ раз свойство сравнений X, после сокращения получим $a^{\varphi(m)} \equiv 1 \pmod{m}$.

■

П р и м е р 5. Определим последние две цифры числа 2021^{2042}. Это означает, что нам надо найти остаток x от деления этого числа на 100. Переформулируем эту задачу с использованием сравнений: найдем такое $x \in \mathbb{Z}$, что $0 \leqslant x < 100$ и $2021^{2042} \equiv x \pmod{100}$. Перед применением теоремы Эйлера заметим, что $(2021, 100) = 1$ (так как 2021 не делится ни на 2, ни на 5) и $\varphi(100) = 40$ (см. предыдущий пример). Тогда $2021^{40} \equiv 1 \pmod{100}$.

Возведем это сравнение в 51-ю степень и получим $2021^{2040} \equiv 1 \pmod{100}$. Отсюда

$$x \equiv 2021^2 \pmod{100} \Rightarrow x \equiv 21^2 \pmod{100} \Rightarrow x \equiv 41 \pmod{100}.$$

В результате, последние две цифры 2021^{2042} образуют число 41.

1.11. Сравнения с одним неизвестным. Линейные диофантовы уравнения

Определение. *Многочленом степени $n \in \mathbb{Z}^+$ с целыми коэффициентами называется $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, где $a_i \in \mathbb{Z}$ при всех $i \in \{0, 1, \ldots, n\}$, причем $a_n \neq 0$. Число a_n называется старшим коэффициентом многочлена $f(x)$. Нулевым многочленом называется $f(x) = 0$, он имеет нулевую степень. Множество всех многочленов с целыми коэффициентами обозначается через $\mathbb{Z}[x]$.*

Определение. *Сравнением n-ой степени с одним неизвестным называется $f(x) \equiv 0 \pmod{m}$, где $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ и его старший коэффициент a_n не делится на модуль m.*

Пример 1. Сравнение $-12x^3 + 8x^2 - 3x + 15 \equiv 0 \pmod{4}$ имеет первую степень, поскольку коэффициенты -12, 8 делятся на 4, а первый коэффициент, не делящийся на 4, встречается у первой степени. Объясним причину возникновения такой терминологии. Далее (в этом параграфе) вместо переменной x мы будем подставлять только целые числа, поэтому при всех целых x справедливы $-12x^3 \equiv 0 \pmod{4}$ и $8x^2 \equiv 0 \pmod{4}$, что позволяет от исходного сравнения сразу перейти к $-3x + 15 \equiv 0 \pmod{4}$, которое очевидно имеет первую степень.

Теорема 11.1. *Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ и $f(x) \equiv 0 \pmod{m}$ — сравнение n-ой степени. Если для $x_0 \in \mathbb{Z}$ выполняется $f(x_0) \equiv 0 \pmod{m}$, то сразу для всех $x \in K_m(x_0)$ будет справедливо $f(x) \equiv 0 \pmod{m}$.*

Доказательство. Условие $x \in K_m(x_0)$ перепишем в виде сравнения $x \equiv x_0 \pmod{m}$ и сразу возведем его в степень $i \in \mathbb{N}$ и получим $x^i \equiv x_0^i \pmod{m}$. Умножив это сравнение на очевидное $a_i \equiv a_i \pmod{m}$, приходим к $a_i x^i \equiv a_i x_0^i \pmod{m}$. Сложив эти сравнения при $i \in \{1, 2, \ldots, n\}$, и

добавив в финале $a_0 \equiv a_0 \pmod m$, получим

$$f(x) = \sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} a_i x_0^i = f(x_0) \equiv 0 \pmod m.$$

По транзитивности получим $f(x) \equiv 0 \pmod m$.

■

Определение. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *и* $f(x) \equiv 0 \pmod m$ *— сравнение* n*-ой степени. Если для* $x_0 \in \mathbb{Z}$ *выполняется* $f(x_0) \equiv 0 \pmod m$, *то класс* $K_m(x_0)$ *называется решением сравнения* $f(x) \equiv 0 \pmod m$.

Замечание. 1) корректность этого определения проверена в предыдущей теореме: вслед за одним числом из класса, все остальные его элементы также удовлетворяют этому сравнению.

2) различных решений у сравнения по модулю m может быть не более чем m, поскольку существует только m различных классов вычетов по этому модулю.

3) для нахождения всех решений сравнения достаточно взять одну ПСВ$_m$ и подставить все ее элементы в сравнение. Затем выбрать классы тех элементов, которые этому сравнению удовлетворяют.

П р и м е р 2. Найдем все решения сравнения $x^4 + 4 \equiv 0 \pmod 5$. Выберем ПСВ$_5$, состоящую из близких к нулю целых чисел: $\{-2, -1, 0, 1, 2\}$. Подстановкой быстро убеждаемся, что -2, -1, 1 и 2 удовлетворяют этому сравнению. Поэтому сравнение имеет четыре решения: $K_5(-2)$, $K_5(-1)$, $K_5(1)$, $K_5(2)$.

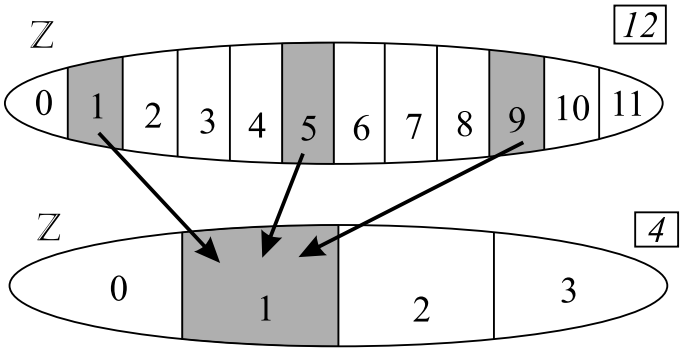

Рис. 2

При достаточно большом модуле m подстановка элементов ПСВ$_m$ займет много времени, поэтому дальше обсудим более эффективные способы поиска решений и определения их количества. Сделано это будет для сравнений первой степени. Но сначала выясним, как связаны между собой классы вычетов по кратным модулям. На рис. 2 изображены «батоны» по модулям 12 и 4. Стрелками показано, что класс вы-

четов $K_4(1)$ является объединением трех классов по модулю 12: $K_{12}(1) \cup K_{12}(5) \cup K_{12}(9)$. В общем случае справедлив следующий результат.

Лемма 11.2. *Пусть $m, m_1, d \in \mathbb{N}$, $m_1 \geqslant 2$, $m = m_1 \cdot d$. Тогда каждый класс вычетов по модулю m_1 распадается на d классов вычетов по модулю m. Точнее, для любого $x_0 \in \mathbb{Z}$*

$$K_{m_1}(x_0) = K_m(x_0) \cup K_m(x_0 + m_1) \cup K_m(x_0 + 2m_1) \cup \ldots \cup K_m\Big(x_0 + (d-1)m_1\Big).$$

Доказательство. Условие $x \in K_{m_1}(x_0)$ равносильно $x = x_0 + m_1 q$, где $q \in \mathbb{Z}$. Разделим число q на d с остатком: $q = dq_1 + r$, где $q_1 \in \mathbb{Z}$ и $0 \leqslant r \leqslant (d-1)$. Получим $x = (x_0 + m_1 r) + (m_1 d)q_1$ или $x = (x_0 + m_1 r) + mq_1$, а последнее равносильно $x \in K_m(x_0 + m_1 r)$. В результате, $x \in K_{m_1}(x_0) \Leftrightarrow$ $\Leftrightarrow x \in K_m(x_0 + m_1 r)$ для некоторого $0 \leqslant r \leqslant (d-1)$. Равенство множеств доказано.

■

Теорема 11.3. *Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \geqslant 2$. Обозначим через $\heartsuit$ сравнение первой степени: $ax \equiv b \pmod m$.*

1) если $(a, m) = 1$, то $\heartsuit$ имеет единственное решение, $K_m(x_0)$, причем x_0 может быть найдено по формуле $x_0 = b \cdot a^{\varphi(m)-1}$.

2) если $(a, m) = d > 1$ и b не делится на d, то $\heartsuit$ не имеет решений.

3) если $(a, m) = d > 1$ и $b \vdots d$, то $\heartsuit$ имеет в точности d решений.

Доказательство. 1) рассмотрим $\{x_1, x_2, \ldots, x_m\}$ — ПСВ$_m$. Учитывая, что $(a, m) = 1$, множество $\{ax_1, ax_2, \ldots, ax_m\}$ также является ПСВ$_m$. Целое число b попадает ровно в один класс вычетов по модулю m, поэтому существует единственный представитель ПСВ$_m$, который попадает в этот же класс. Мы доказали существование и единственность такого $i \in \{1, 2, \ldots, m\}$, что $ax_i \equiv b \pmod m$. То, что конкретное x_0 удовлетворяет сравнению $\heartsuit$, доказывается подстановкой и применением теоремы Эйлера:

$$a\Big(b \cdot a^{\varphi(m)-1}\Big) = b \cdot \Big(a^{\varphi(m)}\Big) \equiv b \pmod m.$$

2) о/п: найдется такое $x^* \in \mathbb{Z}$, что $ax^* \equiv b \pmod m$. Тогда $(ax^* - b) \vdots m$ и $(ax^* - b) \vdots d$. С учетом $ax^* \vdots d$, получим $b \vdots d$. $\lightning$.

3) пусть $(a, m) = d > 1$ и $b \vdots d$. Найдем такие $m_1 \in \mathbb{N}$ и $a_1, b_1 \in \mathbb{Z}$, что $a = da_1$, $b = db_1$ и $m = dm_1$. Сразу заметим, что после деления на НОД, получится $(a_1, m_1) = 1$. Теперь воспользуемся свойством IX сравнений: $ax \equiv b \pmod m \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$. В последнем сравнении выполняется $(a_1, m_1) = 1$, поэтому оно (по уже доказанному (1)) имеет только

одно решение — некоторый класс вычетов $K_{m_1}(x_0)$. По предыдущей лемме этот класс распадается ровно на d классов вычетов по модулю m, поэтому $\heartsuit$ имеет d решений.

■

Пример 3. Решим сравнение $7x \equiv 1 \pmod 4$. Ясно, что $(7,4) = 1$ и $x = -1$ удовлетворяет этому сравнению, поэтому по (1) предыдущей теоремы получим единственное решение этого сравнения — класс $K_4(-1)$.

Пример 4. Сравнение $27x \equiv 6 \pmod{18}$ не имеет решений, поскольку $(27, 18) = 9$ и 6 не делится на 9 (см. (2) предыдущей теоремы).

Пример 5. Найдем все решения сравнения $27x \equiv 15 \pmod{12}$. Поскольку $(27, 12) = 3$ и $15 \vdots 3$, это сравнение имеет три решения. Сократив на 3, приходим к $9x \equiv 5 \pmod 4$ или $x \equiv 1 \pmod 4$. Решением этого сравнения будет класс $K_4(1)$. Мы уже знаем, что он распадается на три класса по модулю 12 (именно классы по такому модулю являются решениями исходного сравнения): $K_{12}(1)$, $K_{12}(5)$, $K_{12}(9)$.

Определение. *Пусть $a, b, m \in \mathbb{Z}$. Обозначим через $\diamondsuit$ уравнение вида $ax + my = b$. Оно называется линейным диофантовым*[15] *уравнением от двух переменных. Решить диофантово уравнение — это значит найти все целочисленные (или натуральные) решения.*

Далее опишем, как можно найти все целочисленные решения $\diamondsuit$. Сразу заметим, что если коэффициент m в $\diamondsuit$ отрицателен, то можно перейти к равносильному (т.е. с тем же самым множеством решений) уравнению $(-a)x + (-m)y = (-b)$, в котором $-m > 0$. Поэтому далее считаем, что $m \geqslant 0$.

I. Начнем со случая $m = 0$. Уравнение $\diamondsuit$ примет вид $ax = b$. Если b не делится на a, то это уравнение не имеет целочисленных решений. Если же b делится на a и $b = b_1 \cdot a$ для некоторого $b_1 \in \mathbb{Z}$, то $\diamondsuit$ равносильно уравнению $x = b_1$, отсюда множеством всех целочисленных решений $\diamondsuit$ будет $\{(b_1, y) : y \in \mathbb{Z}\}$.

II. Продолжим случаем $m = 1$. Уравнение $\diamondsuit$ примет вид $ax + y = b$ или $y = -ax + b$. Отсюда множеством всех целочисленных решений $\diamondsuit$ будет $\{(x, -ax + b) : x \in \mathbb{Z}\}$.

[15] Диофант Александрийский (точные даты жизни неизвестны, примерно III в. н. э.) — древнегреческий математик, последний из великих математиков античности; сохранились только два его сочинения — «Арифметика» (6 томов из 13) и «О многоугольных числах»; его работы в теории чисел стали основанием для дальнейших исследований П. Ферма и Л. Эйлера.

III. Основной случай: $m \geqslant 2$ и $(a, m) = 1$. Переписав уравнение $\diamondsuit$ в виде $ax - b = -my$ заключаем, что пара целых чисел x, y удовлетворяет этому уравнению тогда и только тогда, когда $(ax - b) \vdots m$, что равносильно $ax \equiv b \pmod{m}$. Решением этого сравнения является единственный класс $K_m(x_0)$, где x_0 — одно из целых чисел, которые удовлетворяют этому сравнению (и совсем необязательно находить x_0 по формуле из предыдущей теоремы). Учитывая, что $(ax_0 - b) \vdots m$, найдем такое $t_0 \in \mathbb{Z}$, что $(ax_0 - b) = mt_0$. Итак, уравнению $\diamondsuit$ могут удовлетворять только целые x вида $x_0 + tm$, где $t \in \mathbb{Z}$ (так описываются все числа из класса $K_m(x_0)$). Подставив эти x в $\diamondsuit$, получим

$$a(x_0 + tm) - b = -my \Leftrightarrow amt + (ax_0 - b) = -my \Leftrightarrow amt + mt_0 = -my \Leftrightarrow$$

$$\Leftrightarrow y = -t_0 - at.$$

Все найденные целочисленные решения $\diamondsuit$ можно записать в виде системы:

$$\begin{cases} x = x_0 + mt, \\ y = -t_0 - at, \end{cases} \quad \text{где} \quad t \in \mathbb{Z}.$$

При этом x_0 — любое целое число, которое удовлетворяет сравнению $ax \equiv b \pmod{m}$, а t_0 находится через x_0 по формуле $t_0 = (ax_0 - b)/m$.

IV. Пусть теперь $m \geqslant 2$ и $(a, m) = d$ и d **не** делит b. Но тогда при всех целых x и y левая часть уравнения $\diamondsuit$ делится на d. Отсюда $b \vdots d$. $\lightning$. Делаем вывод: $\diamondsuit$ не имеет целочисленных решений.

V. Последний случай: $m \geqslant 2$, $(a, m) = d$ и d делит b. Найдем такие $m_1 \in \mathbb{N}$ и $a_1, b_1 \in \mathbb{Z}$, что $a = da_1$, $b = db_1$ и $m = dm_1$. Сразу заметим, что после деления на НОД, получится $(a_1, m_1) = 1$. Уравнение $\diamondsuit$ равносильно уравнению $a_1x + m_1y = b_1$, которое уже можно решать так, как это описано в пункте III.

П р и м е р 6. Решим диофантово уравнение $14x - 6y = 8$. Быстро преобразуем его к равносильному $-7x + 3y = -4$ ($a = -7$, $m = 3$, $b = -4$) и найдем решение сравнения $-7x \equiv -4 \pmod{3}$. Умножив его на $-1 \equiv -1 \pmod{3}$, получим $7x \equiv 4 \pmod{3}$, которому удовлетворяет только один класс. Нетрудно заметить, что $7 \cdot 1 \equiv 4 \pmod{3}$, поэтому можно взять в качестве $x_0 = 1$, тогда по формуле $t_0 = (ax_0 - b)/m = (-7 + 4)/3 = -1$, и все решения исходного диофантового уравнения описываются системой

$$\begin{cases} x = 1 + 3t, \\ y = 1 + 7t, \end{cases} \quad \text{где} \quad t \in \mathbb{Z}.$$

1.12. Некоторые проблемы теории чисел

I. *Большая теорема Ферма (БТФ) или Великая теорема Ферма.*

Хорошо известно, что уравнение $x^2 + y^2 = z^2$ имеет бесконечно много решений в натуральных числах. Ясно, что если тройка натуральных чисел (x_0, y_0, z_0) удовлетворяет, этому уравнению, то для любого натурального k тройка (kx_0, ky_0, kz_0) также ему удовлетворяет. Пифагоровы тройки, состоящие из взаимно простых чисел, называются примитивными (нетрудно заметить, что именно они порождают все пифагоровы тройки). Еще Евклид нашел формулы, содержащие все примитивные тройки.

В 1637 году Пьер Ферма на полях «Арифметики» Диофанта сформулировал несколько результатов, среди которых было следующее утверждение: уравнение $x^n + y^n = z^n$ при $n \in \mathbb{N}$ и $n > 2$ не имеет решений в натуральных (и даже целых ненулевых) числах (БТФ). К этому утверждению Ферма добавил: «Я нашел этому поистине чудесное доказательство, но поля книги слишком узки для него». Более 350 лет математики пытались доказать эту теорему (поскольку остальные утверждения Ферма были проверены, БТФ часто называют последней теоремой Ферма — FLT). В 1993 году английский и американский профессор Эндрю Уайлс опубликовал 130-страничное доказательство этой теоремы. Это доказательство содержало некоторые пробелы, которые Уайлс совместно с Ричардом Тейлором устранили в статье 1995 года. **Статус** БТФ: **доказана**.

С БТФ связано много утверждений, одно из них называется гипотезой Била (Эндрю Бил, 1993): если $a, b, c, x, y, z \in \mathbb{N}$, $x, y, z > 2$ и выполняется $a^x + b^y = c^z$, то a, b и c имеют общий простой делитель. Из гипотезы Била следует БТФ. **Статус** гипотезы Била: **открыта**. Эндрю Билом обещана (в 2013 году) премия 1 млн. долларов за доказательство его гипотезы.

II. *Проблема близнецов (ПБ).* Если p и $p + 2$ одновременно являются простыми числами, они называются близнецами. Например, 3 и 5, или 821 и 823 (в сентябре 2016 года были найдены близнецы $2996863034895 \cdot 2^{1290000} \pm 1$). ПБ: бесконечно ли множество близнецов? **Статус** ПБ: **открыта**.

III. *Числа Софи Жермен*[16]. Простое число p называется числом Софи Жермен, если $2p+1$ — простое. Для всех таких показателей p Софи Жермен доказала БТФ. Гипотеза (ЧСЖ): чисел Софи Жермен бесконечно много. **Статус** ЧСЖ: **открыта**.

[16]Софи Жермен (1776–1831) — французский математик, механик, философ; внесла весомый вклад в дифференциальную геометрию, теорию чисел и механику; стала первой женщиной, получившей право участия в заседаниях Парижской Академии наук.

IV. *Проблемы Гольдбаха.* В 1742 г немецкий математик Кристиан Гольдбах в письме к Эйлеру высказал следующее предположение: каждое нечетное число, большее пяти, можно представить в виде суммы трех простых чисел (тернарная проблема Гольдбаха). Эйлер в ответ выдвинул более сильную гипотезу: каждое четное число, большее двух, можно представить в виде суммы двух простых (бинарная проблема Гольдбаха или проблема Эйлера). В 1937 году советский математик И. М. Виноградов доказал, что, начиная с некоторого числа n^*, любое нечетное число может быть представлено в виде суммы трех простых. Далее оценки n^* постоянно уменьшались, пока в 2013 году она не была окончательно доказана перуанским математиком Харольдом Гельфготтом. **Статус** тернарной проблемы Гольдбаха: **доказана**. На апрель 2012 года бинарная гипотеза Гольдбаха была проверена для всех четных чисел, не превышающих $4 \cdot 10^{18}$. **Статус** бинарной проблемы Гольдбаха: **открыта**.

V. *Совершенный кубоид.* Пифагоровы тройки описывают прямоугольные треугольники с целочисленными сторонами. Перейдем к пространственным фигурам. Прямоугольные параллелепипеды, у которых ребра и диагонали граней являются целыми числами, называются *эйлеровыми*. Два семейства таких параллелепипедов описал Эйлер. В 1719 году Пауль Хальке построил самый маленький из таких параллелепипедов (240, 117, 44). *Совершенным кубоидом* называется эйлеров параллелепипед с целой главной диагональю. ПСК: существует ли совершенный кубоид? **Статус** ПСК: **открыта**.

VI. *Многочлены и простые числа.* Будем рассматривать многочлен $f(x) \in \mathbb{Z}[x]$ (т.е. с целыми коэффициентами), чья степень не меньше 2. Нетрудно доказать, что такой многочлен не может в любом натуральном числе давать значение, которое является простым числом. Эйлер привел пример многочлена $f(x) = x^2 + x + 41$, который при $x \in \{0, 1, \ldots, 39\}$ принимает простые значения. Проблема многочлена Эйлера (ПМЭ): для натуральных x многочлен Эйлера дает бесконечно много простых чисел? Существует ли такой многочлен (с целыми коэффициентами и степени не меньше двух), который для натуральных значений переменной дает бесконечное множество простых чисел (МПЧ)? **Статус** ПМЭ и МПЧ: **открыты**.

VII. *Гипотеза Лежандра.*[17] В 1808 году Лежандр сформулировал гипотезу (ГЛ): для любого $n \in \mathbb{N}$ между n^2 и $(n+1)^2$ найдется хотя бы одно простое число. **Статус** ГЛ: **открыта**.

[17] Андриен Лежандр (1752–1833) — французский математик; исследования посвящены математическому анализу, теории чисел, небесной механике; доказал БТФ для $n = 5$; сформулировал закон распределения простых чисел.

Глава 2

Введение в теорию множеств

2.1. Множество и его элементы. Способы задания множеств

Единственным неопределяемым понятием в теории множеств является понятие множества. В качестве синонимов множеству мы будем использовать «совокупность элементов» или «класс элементов». Смысл множества интуитивно ясен — множество объединяет некоторые, вполне определенные, элементы в одно целое. Трудно найти объекты, которые не являются множествами. Так, эта страница является множеством, состоящим из строк, каждая строка — множество, состоящее из некоторых символов, каждый символ — множество точек на плоскости.

Множества мы будем обозначать большими буквами (A , B , X , $Y, \dots$), его элементы — малыми (a , b , x , $y, \dots$). Тот факт, что a является элементом множества A , будем обозначать $a \in A$ (читается: a принадлежит множеству A). Знак $\in$ был введен Пеано и является сокращением греческого слова $\epsilon\sigma\tau\iota$ — «быть». Запись $a \notin A$ означает, что a не является элементом множества A .

Множество полностью определяется своими элементами. Это означает, что множества совпадают в том и только в том случае, когда они состоят из одних и тех же элементов. Символьная запись определения равенства двух множеств такова: $A = B \Leftrightarrow$ (для любого $a \in A \Rightarrow a \in B$, и для любого $b \in B \Rightarrow b \in A$).

Существует два основных способа задания множеств. Для конечных множеств, содержащих небольшое количество элементов, часто просто перечисляют все входящие в него элементы. Так, например, $A = \{a, b, c\}$ — это множество, элементами которого являются только a, b и c .

Самым распространенным является задание множества с помощью некоторого условия $P(a)$, которому удовлетворяют все элементы этого множества и только они. Иными словами, условие $P(a)$ истинно во всех случаях, когда элемент a должен принадлежать определяемому множеству, и ложно для всех элементов, не участвующих в образовании этого множества. Запись $A = \{a : P(a)\}$ означает, что множество A состоит из всех элементов, которые удовлетворяют условию $P(a)$ (знак «:» означает «такие, что»). Например, $\mathbb{N}_2 = \{n : n \in \mathbb{N}$ и существует некоторое $k \in \mathbb{N}$, что $n = 2k\}$ — множество всех четных натуральных чисел; множество $\mathbb{R}^+ = \{x : x \in \mathbb{R}$ и $x \geqslant 0\}$ состоит из всех неотрицательных действительных (или вещественных) чисел, $B = \{b : b$ является выпуклым четырехугольником$\}$ — множество, состоящее из всех выпуклых четырехугольников, или такое экзотичное множество, как $Y = \{y : y$ – крокодил, обитающий в море Лаптевых$\}$. Для сокращения записи вместо $A = \{a : a \in B$ и $P(a)\}$ будем использовать запись $A = \{a \in B : P(a)\}$.

Множества могут являться частью других множеств. Так, множество натуральных чисел $\mathbb{N}$ содержится во множестве всех целых чисел $\mathbb{Z}$, последнее — во множестве рациональных чисел $\mathbb{Q}$, и, наконец, множество $\mathbb{Q}$ содержится во множестве вещественных чисел $\mathbb{R}$.

Определение. *Множество A содержится во множестве B (обозначается $A \subseteq B$), если каждый элемент множества A является элементом множества B (рис. 3).*

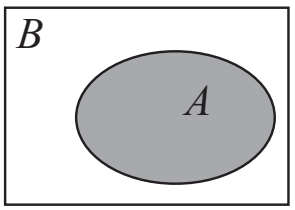

Рис. 3

Попытайтесь доказать следующую простую теорему.

Теорема 1.1. *$A = B$ тогда и только тогда, когда одновременно $A \subseteq B$ и $B \subseteq A$ (т.е. $A = B \Leftrightarrow A \subseteq B$ и $B \subseteq A$).*

Бывают случаи, когда условие $P(a)$ определено таким образом, что нет ни одного элемента, который бы удовлетворял этому условию. Например, $P(a) =$ «a является четным и одновременно нечетным натуральным числом». Множество, не содержащее ни одного элемента, обозначается $\varnothing$ и называется пустым множеством. Его можно определить еще и таким образом: $\varnothing = \{x : x$ — множество и $x \neq x\}$. Сделаем одно важное замечание о пустом множестве. Предположим, необходимо доказать, что каждый элемент x данного множества A удовлетворяет некоторому свойству $P'(x)$. В случае,

когда множество A не содержит элементов, т.е. является пустым, принято считать, что каждый его элемент удовлетворяет свойству $P'(x)$.

Упражнения

1. Назовите три неопределяемых геометрических понятия.

2. Сколько элементов содержит множество людей, знающих определение множества?

3. Доказать, что $\varnothing$ содержится в любом множестве.

4. Доказать, что пустое множество единственно.

5. Принадлежит ли $\varnothing$ множествам $\{\varnothing, 1\}, \Big\{\{\varnothing\}\Big\}, \Big\{\varnothing, \{\varnothing\}\Big\}$?

6. Равны ли между собой множества $\{\varnothing, 1\}$ и $\{1\}$; $\{\varnothing\}$ и $\varnothing$?

7. Доказать, что $\{y : y$ – крокодил, обитающий в море Лаптевых $\}$ содержится во множестве простых чисел.

8. Еще раз попытайтесь доказать теорему этого параграфа.

9. Доказать, что $\{a, b\} = \{b, a\}$.

10. Доказать, что $\{a, b, c\} = \{a, a, b, b, c, c\}$.

11. Содержится ли множество простых чисел во множестве нечетных чисел?

12. Покажите, что различных бесконечных множеств бесконечно много.

13. Кому принадлежат следующие слова: «Математика полностью свободна в своем развитии, и ее понятия связаны только необходимостью быть непротиворечивыми и согласованными с понятиями, введенными ранее посредством точных определений» (Леонардо да Винчи, Эдгару По, М.В. Ломоносову, Г. Кантору[1])?

14. Кто из четырех перечисленных выше людей имел математическое образование?

15. Одним из крупнейших специалистов по теории функций в XIX веке был Карл Вейерштрасс[2]. Известно, что Кантор, обучаясь в берлинском университете, слушал лекции Вейерштрасса. Кроме того, именно Вейерштрасс принимал у Кантора докторский экзамен по алгебре и теории функций. Условием этого экзамена было то, что отвечающий должен был давать ответы на вопросы без подготовки. Пришлось ли Кантору подвергаться столь серьезному испытанию и по теории множеств?

16. Действительно ли Г. Кантор родился в Санкт-Петербурге и учился там в начальной школе?

[1]Георг Кантор (1845–1918) — немецкий математик, основоположник теории множеств; основатель и первый президент Германского математического общества (1890–1893); инициатор созыва первого Международного математического конгресса в Цюрихе (1897).

[2]Карл Вейерштрасс (1815—1897) — немецкий математик, «отец современного анализа»; основные работы посвящены математическому анализу, теории аналитических функций, дифференциальной геометрии и линейной алгебре; его учениками были С. В. Ковалевская, Г. Кантор, М. Г. Миттаг-Леффлер и др.

2.2. Операции над множествами и их свойства

Довольно часто новые множества с требуемыми свойствами получаются из ранее построенных с помощью теоретико-множественных операций. Последние имеют своими историческими предшественниками логические операции, свойства которых были хорошо изучены[3] уже к середине XIX века. В этом параграфе изучаются основные теоретико-множественные операции: пересечение, объединение, разность множеств и взятие дополнения.

Определение. *Пересечением множеств* A *и* B *(обозначается* $A \cap B$*) называется множество, состоящее из всех элементов, которые одновременно принадлежат и* A*, и* B*. Символьная запись этого определения такова:* $A \cap B = \{x : x \in A \text{ и } x \in B\}$.

Определение. *Объединением множеств* A *и* B *(обозначается* $A \cup B$*) называется множество, состоящее из всех элементов, принадлежащих или* A*, или* B*. Символьная запись:* $A \cup B = \{x : x \in A \text{ или } x \in B\}$.

Диаграммы Эйлера–Венна[4], изображенные на рис. 3 и 4, являются иллюстрацией для включения множеств, а также операций пересечения и объединения.

Рассмотрим несколько примеров. Если $A = \{1, 2, 3\}$ и $B = \{3, 4\}$, то их пересечением будет множество $A \cap B = \{3\}$, а объединением будет множество $A \cup B = \{1, 2, 3, 4\}$. Пересечение множества, состоящего из всех квадратов плоскости, и множества четырехугольников, не являющихся квадратами, пусто, в то время как их объединение дает множество всех четырехугольников на плоскости. Решением любой системы уравнений является пересечение решений каждого из входящих в систему уравнений. Пересечение двух различных прямых не может содержать более одной точки, а объединение всегда бесконечно, так как содержит каждую из этих прямых.

Перед тем как определить еще одну операцию над множествами, обсудим понятие *универсального* множества. Часто рассматривают множества какого-то определенного типа, т.е. все они одновременно содержатся в некотором «большом» множестве. Такое множество, которое содержит все рассматриваемые множества данного типа, называется универсальным для этого типа

[3]Заслуга в этом принадлежит английскому математику Джорджу Булю (1815–1864). Дж.Буль — один из основателей математической логики; логическое исчисление Буля получило название булевой алгебры и имеет важное значение в развитии вычислительной техники; четверо из его дочерей стали учеными, пятая — Этель Лилиан Войнич, автор «Овода» — прославилась как писатель.

[4]Джон Венн (1834–1923) — английский математик и логик; ввел термин «символическая логика»; его метод диаграмм нашел применение в теории автоматов.

множеством. Так, для знакомого множества крокодилов моря Лаптевых универсальным множеством является множество всех крокодилов. Для четырехугольников универсальным множеством является плоскость. Для числовых множеств — множество всех действительных (или вещественных) чисел $\mathbb{R}$. Далее универсальное множество будем обозначать через $\mathbf{I}$.

Определение. *Разностью множеств B и A (обозначается $B\backslash A$) называется множество, состоящее из всех элементов множества B, не принадлежащих множеству A (т.е. $B\backslash A = \{x : x \in B \text{ и } x \notin A\}$) (рис. 4).*

Определение. *Дополнением множества A (обозначение — $\overline{A}$) называется разность между универсальным множеством $\mathbf{I}$ и множеством A (т.е. $\overline{A} = \{x \in \mathbf{I} : \text{ и } x \notin A\}$) (рис. 4).*

Если по-прежнему $A = \{1, 2, 3\}$ и $B = \{3, 4\}$, то $B\backslash A = \{4\}$, а $A\backslash B = \{1, 2\}$. Разностью между множеством натуральных чисел $\mathbb{N}$ и множеством всех четных натуральных чисел $\mathbb{N}_2$ является множество всех нечетных натуральных чисел.

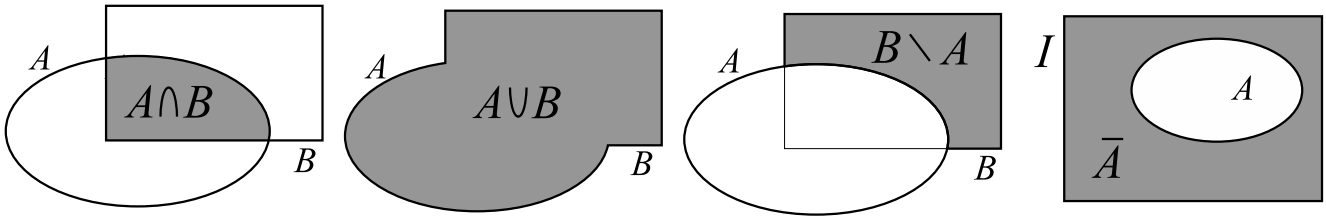

Рис. 4

Операции объединения и пересечения удовлетворяют следующим свойствам.

Теорема 2.1. *Пусть A, B и C — произвольные множества. Тогда справедливы следующие равенства* [5]*:*

1. $A \cup A = A$.	$1'$. $A \cap A = A$.
2. $A \cup B = B \cup A$.	$2'$. $A \cap B = B \cap A$.
3. $(A \cup B) \cup C = A \cup (B \cup C)$.	$3'$. $(A \cap B) \cap C = A \cap (B \cap C)$.
4. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.	$4'$. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Доказательство. Каждое из этих свойств следует из определения операций и из теоремы 1.1. Докажем только 4-е свойство.

[5] Свойства 1 и $1'$ называются идемпотентностью операций $\cup$ и $\cap$, 2 и $2'$ — коммутативностью; 3 и $3'$ — ассоциативностью, 4 и $4'$ — дистрибутивностью.

Обозначим через X и Y левую и правую части в равенстве 4. Покажем, что оба условия теоремы 1.1 выполняются.

$\subseteq$) докажем сначала, что $X \subseteq Y$. Для этого выберем произвольный элемент $x \in X$. Тогда x одновременно принадлежит $A \cup B$ и C. Из условия $x \in A \cup B$ следует, что $x \in A$ или $x \in B$. Если $x \in A$, то $x \in A \cap C$. Если $x \in B$, то $x \in B \cap C$. Следовательно, в любом случае $x \in A \cap C$ или $x \in B \cap C$. Значит, $x \in Y$.

$\supseteq$) докажем, что выполняется и обратное включение ($Y \subseteq X$). Возьмем произвольный $y \in Y$, тогда $y \in (A \cap C) \cup (B \cap C) \Rightarrow y \in A \cap C$ или $y \in B \cap C$. Если $y \in A \cap C \Rightarrow y \in A$ и $y \in C \Rightarrow y \in A \cup B$ и $y \in C \Rightarrow y \in (A \cup B) \cap C = X$. Если $y \in B \cap C \Rightarrow y \in B$ и $y \in C \Rightarrow y \in A \cup B$ и $y \in C \Rightarrow y \in (A \cup B) \cap C = X$. Итак, $y \in X$.

Из теоремы 1.1 теперь следует, что $X = Y$.

Остальные свойства операций проверяются аналогично.

■

Легко заметить, что операции $\cup$ и $\cap$ обладают некоторой симметричностью. Так, при одновременной замене всех $\cup$ на $\cap$ и всех $\cap$ на $\cup$ каждая из приведенных выше формул останется верной. В следующей теореме доказываются основные свойства разности множеств.

Теорема 2.2. *Пусть A и B — произвольные множества. Тогда выполняются следующие свойства* [6]*:*

5. $A \cup \varnothing = A$.	5′. $A \cap \varnothing = \varnothing$.
6. $A \cup \mathbf{I} = \mathbf{I}$.	6′. $A \cap \mathbf{I} = A$.
7. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.	7′. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
8. $\overline{\overline{A}} = A$.	

Доказательство. Свойство 7. Проверять включение будем сразу в обе стороны: $x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A$ и $x \notin B \Leftrightarrow x \in \overline{A} \cap \overline{B}$.

Свойство 8. $x \in \overline{\overline{A}} \Leftrightarrow x \notin \overline{A} \Leftrightarrow x \in A$.

Остальные свойства доказываются аналогично.

■

[6] Свойства 7 и 7′ называются законами де Моргана. Огастес де Морган (1806–1871) — шотландский математик; его работы посвящены основаниям алгебры, арифметике, математическому анализу, логике; один из основоположников формальной алгебры; основатель Лондонского математического общества и его первый президент (с 1866).

Упражнения

1. Доказать, что всегда $A \cap B \subseteq A \cup B$. В каком случае $A \cup B \subseteq A \cap B$?

2. Известно, что $\{a, b\} \subseteq \{c\}$. Что можно сказать об элементах этих множеств?

3. Доказать, что выполняется $A \backslash B = A \backslash (A \cap B)$.

4. В чем сходство и различие свойств операций над множествами $\cup, \cap, \backslash$ и операций над числами $+, \cdot, -$. Найти четыре сходства и два различия.

5. Докажите, что следующие условия эквивалентны:

$$A \subseteq B, \qquad A \cap B = A, \qquad A \cup B = B,$$
$$I \backslash B \subseteq I \backslash A, \qquad A \cap (I \backslash B) = \varnothing, \qquad (I \backslash A) \cup B = I.$$

6. Докажите, что для любых двух множеств A и B выполняется

$$B \backslash (B \backslash A) = B \cap A.$$

7. Правда ли, что теоремы 2.1, 2.2 были доказаны непальским математиком Дж. Булем (1815—1864)?

8. Дано n множеств. Попытаться доказать, что с помощью операций $\cup, \cap, \backslash$ можно получить конечное число различных множеств.

2.3. Декартово произведение множеств. Соответствия

В 1637 году вышел философский трактат «Рассуждение о методе» Рене Декарта[7]. Последняя часть этой работы была посвящена новому геометрическому методу — методу координат. Каждой точке плоскости Декарт поставил в соответствие упорядоченную пару вещественных чисел — ее первую и вторую координаты. При этом многие геометрические фигуры стали описываться с помощью алгебраических уравнений. Координаты каждой точки данной фигуры удовлетворяли соответствующему уравнению, координаты всех остальных точек плоскости не удовлетворяли этому уравнению. Таким образом, многие геометрические задачи были переведены на алгебраический язык и были решены алгебраическими средствами. Эта часть математики, которая возникла на границе геометрии и алгебры, стала называться аналитической геометрией.

Рассмотренное Декартом множество всех упорядоченных пар вещественных чисел является примером произведения множества на себя. Для опреде-

[7]Рене Декарт (1596—1650) — французский философ, математик, физик, физиолог; был на военной службе, много путешествовал; основатель аналитической геометрии, основоположник картезианства; считал алгебраический метод единственным общим методом математики.

ления произведения множеств в общем случае необходимо понятие упорядоченной пары. Пусть A и B — произвольные непустые множества и $a \in A$, $b \in B$. Заметим сразу, что множества[8] $\{a, b\}$ и $\{b, a\}$ равны между собой и поэтому не дают возможности определить, какой из двух элементов пары является первым, а какой — вторым. Последнее важно, так как, например, точки с координатами $(1, 2)$ и $(2, 1)$ различны, в то время как множества $\{1, 2\}$ и $\{2, 1\}$ совпадают. Существует несколько определений упорядоченной пары (a, b), одно из них принадлежит Н. Винеру[9] и К. Куратовскому[10].

Определение. *Пусть $a \in A$, $b \in B$. Упорядоченной парой (a, b) называется множество $\Big\{\{a\}, \{a, b\}\Big\}$, при этом a называется первым элементом упорядоченной пары, а b — вторым.*

Теорема 3.1. $(a, b) = (c, d) \Leftrightarrow a = c \ \ и \ \ b = d$.

Доказательство. $\Leftarrow$) очевидно.

$\Rightarrow$) пусть $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{c\}, \{c, d\}\Big\}$.

1-й случай. $a = b$. Тогда $\{\{a\}, \{a, b\}\} = \{\{a\}\} = \{\{c\}, \{c, d\}\}$. Следовательно, $\{a\} = \{c\} = \{c, d\} \Rightarrow a = c = d$.

2-й случай. $a \neq b$. Из равенства множеств получим, что $\{a\} \in \Big\{\{c\}, \{c, d\}\Big\}$ $\Rightarrow \{a\} = \{c\}$ или $\{a\} = \{c, d\}$.

а) $\{a\} = \{c\}$. Поэтому $a = c$ и $\Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{a\}, \{a, d\}\Big\}$. Заметим, что $\{a, b\} \neq \{a\}$, иначе $a = b$. Следовательно, $\{a, b\} = \{a, d\} \Rightarrow b = d$.

б) $\{a\} = \{c, d\} \Rightarrow c = d = a \Rightarrow \Big\{\{a\}, \{a, b\}\Big\} = \Big\{\{c\}\Big\} \Rightarrow \{a, b\} =$ $= \{a\} \Rightarrow a = b$. Противоречие.

■

Итак, запись (a, b) означает, что пара образована двумя элементами a и b, причем a является первым элементом этой пары. В предыдущей теореме доказано основное свойство упорядоченных пар: две упорядоченные пары совпадают тогда и только тогда, когда совпадают их первые элементы и вторые элементы также равны между собой. Это, в частности, означает, что $(a, b) = (b, a)$ только в исключительном случае: когда $a = b$.

[8] Множество $\{a, b\} = \{b, a\}$ называется неупорядоченной парой.

[9] Норберт Винер (1894–1964) — американский математик, основоположник кибернетики; первые работы относятся к основаниям математики и математическому анализу.

[10] Казимеж Куратовский (1896–1980) — польский математик; основные работы относятся к топологии, теории графов, теории множеств и теории функций действительного переменного; основатель польской топологической школы.

Определение. *Произведением двух множеств* A *и* B *называют множество* $A \times B$, *состоящее из всех упорядоченных пар, первые элементы которых выбираются из* A, *вторые — из* B *(т.е.* $A \times B = \{(a,b) : a \in A \,\&\, b \in B\}$*).*

На рис. 5 изображено произведение множеств $A = \{1,2,3\}$ и $B = \{a,b\}$.

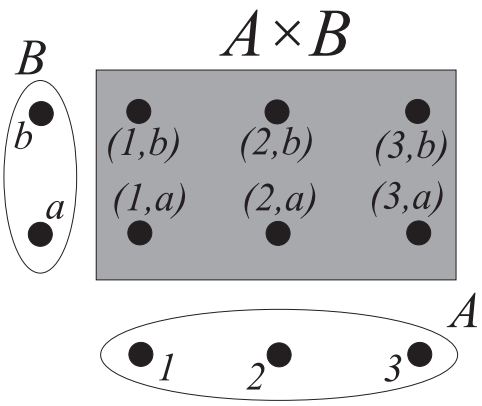

Рис. 5

Произведение двух множеств A и B часто называют декартовым произведением. Заметим, что множества A и B не обязаны быть различными, и в случае их совпадения множество $A \times A$ обозначают через A^2 и называют квадратом (декартовым квадратом) множества A. Так, например, $\mathbb{R}^2$ — декартова плоскость, $\mathbb{Z}^2$ — ее подмножество, состоящее из всех точек с целочисленными координатами.

Заметим, что часто $A \times B \neq B \times A$. Так, $(1,-2) \in \mathbb{N} \times \mathbb{Z}$, но $(1,-2) \notin \mathbb{Z} \times \mathbb{N}$.

Теорема 3.2. *Пусть* A, B *и* C *— произвольные множества, тогда выполняются следующие свойства:*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
1′. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

Доказательство. Обозначим через X и Y левую и правую части равенства 1.

$\subseteq$) если $x \in X \Rightarrow x = (d,c)$, где $d \in A \cup B, c \in C$. Если $d \in A \Rightarrow x \in A \times C$. Аналогично, если $d \in B \Rightarrow x \in B \times C$. Следовательно, $X \subseteq Y$.

$\supseteq$) так как $A \times C$ и $B \times C$ содержатся в X, то $Y \subseteq X$.

По теореме 1.1 множества X и Y совпадают.

Свойство $1'$ доказывается аналогично.

■

Ниже обсудим понятие соответствия.

Определение. *Соответствием* φ *между множествами* A *и* B *называется произвольное подмножество их произведения* $A \times B$ *(т. е.* $\varphi \subseteq A \times B$*)* [11].

Итак, соответствие состоит из упорядоченных пар. Каждая пара $(a,b) \in \varphi$ указывает, что элементу $a \in A$ соответствует элемент $b \in B$ при данном соответствии φ.

Иногда соответствие удобно изображать с помощью стрелок, начало которых указывает первый элемент упорядоченных пар, конец — второй элемент.

[11] Греческие буквы φ, ψ, χ читаются соответственно «фи», «пси», «хи».

Так, рис. 6 является изображением для следующего соответствия:

$$\varphi = \{(1, b),\ (3, a),\ (3, c),\ (4, b)\}.$$

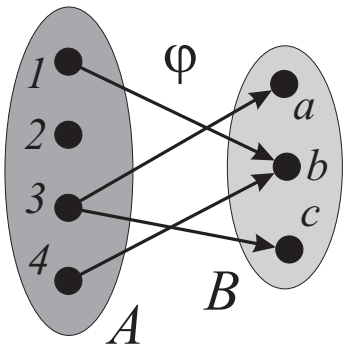

Рис. 6

Заметим, что некоторым элементам из A может соответствовать несколько элементов множества B, а некоторым элементам из A может не соответствовать ни один элемент множества B.

Определение. *Областью определения соответствия* φ *называется множество* $Dom\ \varphi = D(\varphi) = \{a \in A :$ *существует элемент* $b \in B$, *что* $(a, b) \in \varphi\}$ *(т. е. все элементы из* A, *которым соответствует хотя бы один элемент из* B*).*

Определение. *Множеством значений соответствия* φ *называют множество* $Im\ \varphi = E(\varphi) = \{b \in B :$ *существует элемент* $a \in A$, *что* $(a, b) \in \varphi\}$ *(т. е. все элементы из* B, *которые соответствуют хотя бы одному элементу из* A*).*

Пример 1. Для φ, изображенного на рис. 6, $Dom\ \varphi = \{1, 3, 4\}$ и $Im\ \varphi = \{a, b, c\}$.

Для обозначения соответствия φ между множествами A и B будем использовать $A \xrightarrow{\varphi} B$ или $\varphi : A \to B$.

Опишем некоторые типы соответствий.

Определение. *Соответствие* $\varphi : A \to B$ *называется*
1) всюду определенным, если $D(\varphi) = A$;
2) сюръективным, если $E(\varphi) = B$;
3) однозначным, если каждому $a \in D(\varphi)$ *соответствует единственный элемент* b *из* B, *т. е. из* $(a, b) \in \varphi$ *и* $(a, b_1) \in \varphi \Rightarrow b = b_1$;
4) инъективным, если разным элементам из $D(\varphi)$ *соответствуют разные элементы из* B, *т. е. из* $(a, b) \in \varphi$ *и* $(a_1, b) \in \varphi \Rightarrow a = a_1$.

Пример 2. Так, соответствие φ из примера 1 сюръективно, но не всюду определено ($2 \notin D(\varphi)$), не однозначно (так как $(3, a), (3, c) \in \varphi$), не инъективно (так как $(1, b)$, $(4, b) \in \varphi$). Чаще всего мы будем иметь дело с хорошими соответствиями — отображениями и биекциями.

Определение. *Отображением называется всюду определенное и однозначное соответствие (т. е. выполняются свойства 1 и 3). Функцией называют отображение в действительную прямую (т. е.* $B = \mathbb{R}$*).*

Определение. *Биекцией называют всюду определенное, сюръективное, однозначное и инъективное соответствие (т. е. выполняются все свойства 1—4).*

Биекции часто называют *взаимно-однозначными* или *1–1* соответствиями.

Например, квадратичная функция каждому числу $x \in \mathbb{R}$ (поэтому она всюду определена) ставит в соответствие одно число $ax^2 + bx + c$ (она однозначна). Но квадратичная функция не является инъективным соответствием (некоторым различным числам она ставит в соответствие одно и то же число). Поэтому это не биекция. С другой стороны, функция $f(x) = kx + b$ является биекцией при $k \neq 0$.

К соответствиям можно применять две операции — рассматривать обратное соответствие (унарная операция) и брать композицию соответствий.

Определение. *Обратным соответствием к соответствию* $\varphi \subseteq A \times B$ *называют* $\varphi^{-1} = \{(b, a) : (a, b) \in \varphi\}$.

Заметим, что $\varphi^{-1} \subseteq B \times A$, поэтому φ^{-1} — это соответствие уже между B и A. На рис. 7 показано обратное соответствие к φ, изображенному на рис. 6. В этом случае $\varphi^{-1} = \{(b, 1),\ (a, 3),\ (c, 3),\ (b, 4)\}$.

Определение. *Композицией соответствий* $\varphi \subseteq A \times B$ *и* $\psi \subseteq B \times C$ *называют соответствие* $\chi \subseteq A \times C$ *такое, что* $\chi = \{(a, c) :$ *существует такой элемент* $b \in B$, *что* $(a, b) \in \varphi$ *и* $(b, c) \in \psi\}$ *(обозначается композиция так:* $\chi = \psi \circ \varphi$*).*

Композиция соответствий, изображенных на рис. 8, является множеством $\psi \circ \varphi = \{(1, y),\ (3, x),\ (4, y)\}$.

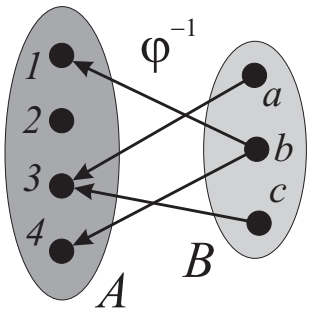

Рис. 7

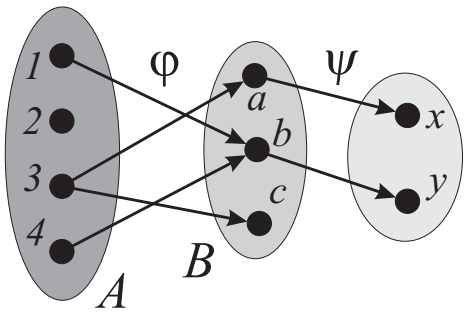

Рис. 8

Биекции устойчивы к операции взятия композиции и перехода к обратному соответствию.

Теорема 3.3. *Если* $\varphi \subseteq A \times B$ *и* $\psi \subseteq B \times C$ *— биекции, то*
1) φ^{-1} *является биекцией между* B *и* A;
2) $\psi \circ \varphi$ *является биекцией между* A *и* C.

Доказательство. 1) так как φ всюду определено, то φ^{-1} сюръективно. Так как φ сюръективно, то φ^{-1} всюду определено. Два оставшихся свойства проверяются аналогично.

2) поскольку φ и ψ всюду определены, их композиция $\psi \circ \varphi$ также будет определена в каждой точке множества A. Так как φ действует на все B и ψ — на все C, то $\psi \circ \varphi$ является сюръективным соответствием. Однозначность и инъективность также легко проверить.

■

Упражнения

1. Найти пересечение множеств $A = \{1, a, 2\}$ и $B = \{a, b, 3\}$; а также $\mathbb{R}$ и $\mathbb{R}^2$.

2. Какая плоская фигура соответствует $\{(x, y) \in \mathbb{R}^2 : Ax + By + C = 0, \text{ где } A, B, C \in \mathbb{R}\}$? Рассмотреть все случаи A, B, C.

3. Какая фигура соответствует множеству $\{(x, y) \in \mathbb{R}^2 : (|x| - |y|)(x^2 + y^2 - 4x) = 0\}$?

4. Известно, что $A \times B = \varnothing$. Что можно сказать о множествах A и B?

5. Пусть для множеств A, B, C имеет место условие $(A \times B) \cup (B \times A) = C \times C$. Доказать, что $A = B = C$.

6. В каком случае $A \times B = B \times A$? Описать все такие случаи.

7. Являются ли биекциями $f(x) = x^3$, $f(x) = \sqrt[3]{x}$, $f(x) = \sqrt{x}$?

8. Если φ — отображение, то соотношение $(a, b) \in \varphi$ будем записывать в виде $b = \varphi(a)$. (Почему это можно сделать только для отображений?) Тогда композицию $\psi \circ \varphi$ можно записать так: $\psi(\varphi(a))$ (т. е. сначала на элемент из A действует φ, а затем на получившийся элемент $\varphi(a) \in B$ действует ψ). Пусть $f(x) = x^2$ и $g(x) = x + 1$, найти $g \circ f$ и $f \circ g$.

9. Пусть $A \xrightarrow{f} A$ и $f \circ f \circ \ldots \circ f = id_A$, где id_A — тождественное соответствие на A, т. е. для любого $a \in A$ выполняется $id_A(a) = a$. Доказать, что f — биекция.

10. Пусть $A \xrightarrow{f} B$ и f всюду определено. Доказать, что f является инъективным соответствием $\Leftrightarrow$ для любых $g, h (g : B \longrightarrow A,\ h : B \longrightarrow A)$ из равенства $f \circ g = f \circ h$ следует $g = h$.

11. Пусть $X \xrightarrow{f} Y$, $X \neq \varnothing$. Доказать, что f — сюръективное соответствие $\Leftrightarrow$ для любых $g, h (g : Y \longrightarrow X,\ h : Y \longrightarrow X)$, из того, что $g \circ f = h \circ f$, следует, что $g = h$.

12. Пусть F — отображение $F : X \longrightarrow Y$. Покажите, что эквивалентны следующие свойства:

1. F — инъективное отображение;
2. $F^{-1}\Big(F(A)\Big) = A$ для любого подмножества $A \subseteq X$;

3. $F(A \cap B) = F(A) \cap F(B)$ для любой пары A, B подмножеств X;
4. $F(A) \cap F(B) = \varnothing$ для любой пары A, B подмножеств X таких, что $A \cap B = \varnothing$;
5. $F(A \backslash B) = F(A) \backslash F(B)$ для любой пары A, B подмножеств X, для которой $B \subseteq A$.

2.4. Конечные множества. Принцип Дирихле

Сравнивать между собой количества элементов двух различных конечных множеств A и B кажется простой задачей. Для этого можно определить число элементов в A, затем в B и сравнить получившиеся два целых числа. Теперь усложним задачу. Попытайтесь представить себе такую ситуацию, что вы разучились считать, но вам необходимо определить: одинаковое количество элементов во множествах A и B или нет. Если вы справились с первой частью задачи, то вторую часть задачи можно решить с помощью биекции. Следует выбирать по элементу из каждого множества, образуя пары (пары соответствия), до тех пор, пока не закончатся элементы хотя бы в одном из этих двух множеств. Если это произойдет одновременно, то получится биекция между этими множествами, и, следовательно, во множествах A и B одинаковое количество элементов.

Определение. *Множества A и B называются равномощными ($A \sim B$), если существует биекция между ними (т.е. существует $A \xrightarrow{\varphi} B$, что φ — биекция).*

Теорема 4.1. *Пусть A, B и C — некоторые множества. Тогда выполняются свойства*[12]*:*

1. $A \sim A$.
2. $A \sim B \Rightarrow B \sim A$.
3. $A \sim B$ и $B \sim C \Rightarrow A \sim C$.

Доказательство. 1. Биекцию A на себя построить легко: пусть по определению $\varphi(a) = a$ для любого $a \in A$[13]. Тогда φ — искомая биекция.

2. Пусть $A \xrightarrow{\varphi} B$ — биекция между A и B, тогда φ^{-1} — биекция между B и A (см. теорему 3.3).

[12] Первое из этих свойств называется рефлексивностью, второе — симметричностью и третье — транзитивностью.

[13] Такая биекция называется тождественным отображением A на себя и обозначается id_A.

3. Пусть $A \xrightarrow{\varphi} B$, $B \xrightarrow{\psi} C$ — биекции между A, B и B, C соответственно, тогда $\psi \circ \varphi$ — биекция между A и C (см. теорему 3.3).

■

Определение. *Пусть $n \in \mathbb{N}$, тогда множество $\mathbb{N}_{\leqslant n} = \{1, 2, \ldots, n\}$ называют начальным отрезком натурального ряда.*

Лемма 4.2.

$\mathbb{N}_{\leqslant n} \sim \mathbb{N}_{\leqslant p} \Leftrightarrow n = p$.

Доказательство. $\Leftarrow$) если $n = p$, то $\mathbb{N}_{\leqslant n} = \mathbb{N}_{\leqslant p}$ и используем первое свойство теоремы 4.1.

$\Rightarrow$) пусть $\mathbb{N}_{\leqslant n} \sim \mathbb{N}_{\leqslant p}$, тогда существует биекция $\mathbb{N}_{\leqslant n} \xrightarrow{\varphi} \mathbb{N}_{\leqslant p}$. Изменим эту биекцию следующим образом. Пусть $\varphi(1) = k$, где $k \leqslant p$, и существует $l \leqslant n$, что $\varphi(l) = 1$. Рассмотрим $\varphi_1 = \Big(\varphi \backslash \{(1, k),\ (l, 1)\}\Big) \cup \cup \{(1, 1),\ (l, k)\}$. Ясно, что φ_1 — биекция, так как мы поменяли местами значения φ на двух элементах (в 1 и l). Заметим, что уже $\varphi_1(1) = 1$. Аналогично построим биекцию φ_2 со свойством $\varphi_2(1) = 1, \varphi_2(2) = 2$ и т.д. В конце концов мы получим φ_n со свойством $\varphi_n(i) = i, \quad i \leqslant n$. Так как φ_n сюръективно и сохраняет порядок, то $\varphi_n(n) = p$, с другой стороны, $\varphi_n(n) = n \Rightarrow n = p$.

■

Определение. *Множество A называется конечным множеством, если $A = \varnothing$ или существует $n \in \mathbb{N}$, что $A \sim \mathbb{N}_{\leqslant n}$. При этом будем говорить, что мощность множества A равна n ($|A| = n$). Если множество пусто, то по определению считаем, что его мощность равна нулю.*

Например, если $\mathrm{A}_{\text{рус}}$ — множество всех букв русского алфавита, то $|\mathrm{A}_{\text{рус}}| = 33$.

Теорема 4.3.

Пусть $|A| = n$ и $|B| = p$. Тогда $A \sim B \Leftrightarrow n = p$.

Доказательство. Для $n = 0$ или $p = 0$ утверждение очевидно. Далее считаем, что $n, p \in \mathbb{N}$.

$\Rightarrow$) из условия $|A| = n$ найдем биекцию $A \xrightarrow{\varphi} \mathbb{N}_{\leqslant n}$. Из определения равномощности A и B найдется биекция $A \xrightarrow{\psi} B$. Тогда соответствие $\varphi \circ \psi^{-1}$ является биекцией между B и $\mathbb{N}_{\leqslant n}$. Следовательно, $p = |B| = n$ (на рис. 9 и 10 изображены *коммутативные диаграммы*, которые являются иллюстрацией к доказательству этой теоремы).

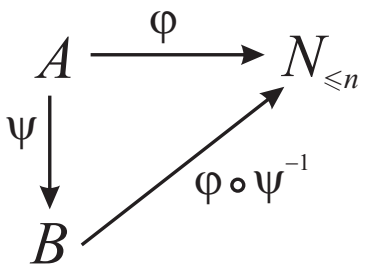

Рис. 9

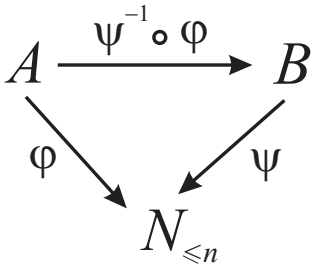

Рис. 10

$\Leftarrow$) пусть $|A| = |B| = n$. Тогда существуют биекции $A \xrightarrow{\varphi} \mathbb{N}_{\leqslant n}$ и $B \xrightarrow{\psi} \mathbb{N}_{\leqslant n}$. Следовательно, $\psi^{-1} \circ \varphi$ — биекция между A и B (рис. 10).

■

Следствие 1. *Пусть $n \in \mathbb{N}$. Тогда $|A| = n \Leftrightarrow$ когда множество A можно представить в виде $\{a_1, \ldots, a_n\}$, где $a_i \neq a_j$, при $i \neq j$.*

Доказательство. Так как существует биекция $A \xrightarrow{\varphi} \mathbb{N}_{\leqslant n}$, то, обозначив $\varphi^{-1}(i)$ через a_i, мы получим искомое представление. Обратно, если такое представление задано, биекцию можно построить так: $\varphi(a_i) = i$.

■

Следствие 2. *Пусть $|A| = n$, $a \in A$, $k, n \in \mathbb{N}$ и $k \leqslant n$. Тогда A можно представить в виде $A = \{a_1, \ldots, a_k, \ldots, a_n\}$, где $a_k = a$. То есть можно занумеровать элементы множества A так, что наперед выбранный элемент a будет иметь номер k.*

Доказательство. Пусть $\varphi : A \to \mathbb{N}_{\leqslant n}$ — биекция. Если $\varphi(a) = k$, то используем предыдущее следствие. Иначе существуют $(a, l), (b, k) \in \varphi$, что $a \neq b$. Определим $\psi = \Big(\varphi \backslash \{(a, l), (b, k)\}\Big) \cup \{(a, k), (b, l)\}$. Это соответствие является искомой биекцией. Осталось применить предыдущее следствие.

■

Следствие 3 *(принцип Дирихле). Пусть $n \neq p$, тогда n кроликов нельзя рассадить в p ящиков так, чтобы в каждом ящике было по одному кролику.*

Доказательство. О/п: пусть это можно сделать, тогда существует биекция между множеством кроликов и множеством ящиков. Из предыдущей теоремы следует, что $n = p$. $\lightning$.

■

П р и м е р 1. В равностороннем треугольнике со стороной 1 расположены пять точек. Доказать, что существует по крайней мере две точки, расстояние между которыми не больше $1/2$. Для решения достаточно заметить, что

средние линии треугольника разбивают его на четыре равносторонних треугольника со стороной $1/2$. По принципу Дирихле две точки попадут в один из этих треугольников. Расстояние между ними будет не больше $1/2$.

Пример 2. Доказать, что существует $n \in \mathbb{N}$ такое, что 7^n оканчивается на 000001. Рассмотрим множество остатков от деления чисел вида 7^n на 1000000. Среди чисел 7^n при натуральных $n \leqslant 1000001$ найдутся (по принципу Дирихле) по крайней мере два числа, дающих при делении на 1000000 одинаковые остатки, т.е. $7^{k_1} \equiv 7^{k_2} \pmod{1000000}$ для некоторых $1 \leqslant k_1 < k_2 \leqslant 1000001$. Следовательно, $7^{k_1}(7^{k_2-k_1} - 1) \vdots 1000000$. Заметим, что 7^{k_1} взаимно просто с числом 1000000, поэтому число $k_2 - k_1$ — искомое.

Теорема 4.4. *Пусть A, B, C, A_1, $A_2, \ldots,$ A_n — конечные множества.*

1) если $A \cap B = \varnothing$, то $|A \cup B| = |A| + |B|$.

2) если A_1, $A_2, \ldots,$ A_n попарно не пересекаются, то $\left|\bigcup\limits_{i=1}^{n} A_i\right| = \sum\limits_{i=1}^{n} |A_i|$.

3) если $C \subseteq B$, то $|B \backslash C| = |B| - |C|$.

4) $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказательство. 1) если хотя бы одно из множеств пусто, то утверждение очевидно. Пусть теперь $|A| = n$, $|B| = p$, $n, p \in \mathbb{N}$ и рассмотрим биекции $A \xrightarrow{\varphi} \mathbb{N}_{\leqslant n}$ и $B \xrightarrow{\psi} \mathbb{N}_{\leqslant p}$. Тогда существует биекция $A \cup B \xrightarrow{\chi} \mathbb{N}_{\leqslant n+p}$, где χ задается по правилу:

$$\chi(c) = \begin{cases} \varphi(c), & \text{если } c \in A; \\ \psi(c) + n, & \text{если } c \in B. \end{cases}$$

2) индукцией по n. Б.И. Случай $n = 1$ очевиден, а $n = 2$ следует из (1). Ш.И. Сразу следует из предположения и базы индукции.

3) случай $C = \varnothing$ очевиден. Пусть $C \subseteq B$ и $|C| = l \in \mathbb{N}$, тогда, применяя l раз второе следствию теоремы 4.3, получим представление $B = \{b_1, \ldots, b_{m-l}, \ b_{m-l+1}, \ldots, b_m\}$, где $C = \{b_{m-l+1}, \ldots, b_m\}$. Следовательно, $B \backslash C = \{b_1, \ldots, b_{m-l}\}$. Используя первое следствие, окончательно получаем $|B \backslash C| = m - l$.

4) представим это объединение в виде двух непересекающихся множеств $A \cup B = A \cup (B \backslash (A \cap B))$. Далее, используя формулу (1), получим $|A \cup B| = |A| + |B \backslash (A \cap B)|$. По формуле (3), $|A \cup B| = |A| + |B| - |A \cap B|$.

■

Следующее утверждение называется *обобщенным принципом Дирихле.*

Следствие. *Пусть* $n, k \in \mathbb{N}$ *и* $|A| > n \cdot k$ *. Если* A *разбито*[14] *на* n *подмножеств, то хотя бы в одном из них будет не менее* $(k+1)$ *-го элемента.*

Доказательство. О/п: $A = \bigcup_{i=1}^{n} A_i$, множества A_1 , $A_2, \ldots,$ A_n попарно не пересекаются, и $|A_i| \leqslant k$ для всех $k \in \{1, 2, \ldots, n\}$. Тогда по второй формуле предыдущей теоремы получим, что $|A| \leqslant k \cdot n$, а это противоречит условию $|A| > n \cdot k$.

■

Следующая теорема усиливает четвертое свойство предыдущей теоремы. Она позволяет найти число элементов объединения произвольного конечного числа конечных множеств. Формула этой теоремы называется формулой *включений и исключений.*

Теорема 4.5. *Пусть* $A_1, \ldots, A_n$ *— конечные множества. Тогда*

$$
\begin{aligned}
&|A_1 \cup A_2 \cup \ldots \cup A_n| = \\
&(|A_1| + |A_2| + \ldots + |A_n|) - \underbrace{(|A_1 \cap A_2| + \ldots + |A_{n-1} \cap A_n|)}_{\text{все попарные пересечения}} + \\
&+ \ldots + (-1)^{k-1} \underbrace{(|A_1 \cap A_2 \cap \ldots \cap A_k| + \ldots + |A_{n-k+1} \cap \ldots \cap A_n|)}_{\text{все пересечения по } k \text{ множеств}} + \\
&+ \ldots + (-1)^{n-1}(|A_1 \cap A_2 \cap \ldots \cap A_n|).
\end{aligned}
$$

Доказательство. Индукция по n . Случай $n = 1$ очевиден, а $n = 2$ доказан в предыдущей теореме. Пусть для любых объединений из k множеств, где $k < n$ и $k \in \mathbb{N}$, формула справедлива, и докажем ее для n . Введем обозначение $A_1 \cup A_2 \cup \ldots \cup A_{n-1} = \Phi$, тогда по базе индукции получаем

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |\Phi| + |A_n| - |\Phi \cap A_n|. \tag{1}$$

По предположению индукции

$$
\begin{aligned}
|\Phi| = &\Big(|A_1| + |A_2| + \ldots + |A_{n-1}|\Big) - \\
- &\underbrace{\Big(|A_1 \cap A_2| + |A_1 \cap A_3| + \ldots + |A_{n-2} \cap A_{n-1}|\Big)}_{\text{все попарные пересечения, в которые не входит } A_n} + \\
&+ \ldots (-1)^{k-1} \underbrace{\Big(|A_1 \cap \ldots \cap A_k| + \ldots + |A_{n-k} \cap A_{n-k+1} \cap \ldots \cap A_{n-1}|\Big)}_{\text{все пересечения по k элементов, в которые не входит } A_n} + \\
&+ \ldots (-1)^{n-2}\Big(|A_1 \cap A_2 \cap \ldots \cap A_{n-1}|\Big).
\end{aligned} \tag{2}
$$

По теореме 2.1 (используем свойство дистрибутивности)

$$\Phi \cap A_n = (A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n).$$

[14] Т.е. оно представлено в виде объединения попарно не пересекающихся множеств.

Заметим, что в объединении участвуют $n-1$ множеств. Снова используем предположение индукции.

$$
\begin{aligned}
|\Phi \cap A_n| = &\Big(|A_1 \cap A_n| + |A_2 \cap A_n| + \ldots + |A_{n-1} \cap A_n|\Big) - \\
- &\underbrace{\Big(|A_1 \cap A_2 \cap A_n| + \ldots + |A_{n-2} \cap A_{n-1} \cap A_n|\Big)}_{\text{все пересечения по три элемента, в которые входит } A_n} + \ldots + \\
&(-1)^{k-1}\underbrace{\Big(|A_1 \cap \ldots \cap A_k \cap A_n| + \ldots + |A_{n-k} \cap A_{n-k+1} \cap \ldots \cap A_{n-1} \cap A_n|\Big)}_{\text{все пересечения по } k+1 \text{ элементу, в которые входит } A_n} + \\
&+ \ldots (-1)^{n-2}\Big(|A_1 \cap A_2 \cap \ldots \cap A_{n-1} \cap A_n|\Big)
\end{aligned}
\tag{3}
$$

Подстановка правых частей уравнений (2) и (3) в уравнение (1) завершает доказательство.

■

Следствие 1. *Для конечных множеств* A_1, A_2 *и* A_3 *выполняется:* $|A_1 \cup A_2 \cup A_3| = (|A_1| + |A_2| + |A_3|) - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + +(|A_1 \cap A_2 \cap A_3|)$.

Доказательство. Следует из предыдущей теоремы при $n = 3$.

■

Следствие 2. *Для множеств* A_1, A_2 *и* A_3, *которые содержатся в конечном универсальном (для них) множестве, выполняется* $|\overline{A_1 \cap A_2 \cap A_3}| = (|\overline{A_1}| + |\overline{A_2}| + |\overline{A_3}|) - (|\overline{A_1} \cap \overline{A_2}| + |\overline{A_1} \cap \overline{A_3}| + |\overline{A_2} \cap \overline{A_3}|) + +(|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}|)$.

Доказательство. Достаточно воспользоваться одной из формул де Моргана: $\overline{A_1 \cap A_2 \cap A_3} = \overline{A_1} \cup \overline{A_2} \cup \overline{A_3}$.

■

Упражнения

1. Определить мощность $A_{\text{лат}}$, где $\mathrm{A}_{\text{лат}}$ — множество, состоящее из всех латинских букв.

2. Пусть $|A| = n \geqslant 2$ и $a \neq b$, $a, b \in A$, тогда множество A можно представить в виде $A = \{a_1, \ldots, a_n\}$, где $a = a_1$, $b = a_n$.

3. Как при доказательстве первого пункта теоремы 4.4 использовалось условие $A \cap B = \varnothing$?

4. Доказать, что если A — конечное множество, то A не равномощно множеству $A \backslash \{a\}$, где $a \in A$.

5. Доказать, что A – конечное множество $\Leftrightarrow$ A не равномощно никакому своему собственному подмножеству B (т.е. $B \subseteq A$ и $B \neq A$ — обозначается через $B \subset A$).

6. Попытаться решить «веселую» задачу Л. Кэрролла[15]: в неравном бою с представителями Вест-Индийской компании из 100 пиратов 90 потеряли руку, 80 — ногу, 70 — глаз. Определить наименьшее количество «счастливчиков», потерявших одновременно и руку, и ногу, и глаз.

2.5. Степень данного множества и его мощность

В предыдущих параграфах не раз встречались множества, элементы которых также являлись множествами. Определение упорядоченной пары дает нам один из возможных примеров. Рассмотрим произвольное множество A. Будем теперь рассматривать новые множества, элементами которых являются подмножества множества A (так как $\varnothing, A \subseteq A$, то среди таких множеств будут $\{\varnothing\}$, $\{A\}$). В этом подразделе нас будет интересовать «максимальное»[16] из множеств, которые конструируются только из подмножеств множества A.

Определение. *Пусть A — произвольное множество. Степенью множества A называется множество (обозначается через $\mathcal{P}(A)$ или 2^A), состоящее из всех подмножеств множества A (т. е. $\mathcal{P}(A) = \{B : B \subseteq A\}$).*

Степень множества также называется *множеством всех подмножеств* множества A или *булеаном* множества A.

Пример 1. Пусть $A = \{a\}$. Тогда $\mathcal{P}(A) = \Big\{\varnothing, \{a\}\Big\}$, $|A| = 1$, $|\mathcal{P}(A)| = 2 = 2^1$.

Заметим, что $\varnothing \in \mathcal{P}(A)$ и $A \in \mathcal{P}(A)$ для любого множества A.

Пример 2. $A = \{1, a, b\}$. Тогда

$$\mathcal{P}(A) = \Big\{\varnothing, \{1\}, \{a\}, \{b\}, \{1, a\}, \{1, b\}, \{a, b\}, \{1, a, b\}\Big\},$$

$|A| = 3$, $|\mathcal{P}(A)| = 8 = 2^3$. Множество $\mathcal{P}(A)$ можно разбить на два —

$$\Big\{\varnothing, \{1\}, \{b\}, \{1, b\}\Big\} \quad \text{и} \quad \Big\{\{a\}, \{1, a\}, \{b, a\}, \{1, b, a\}\Big\}.$$

Заметим, что элементы первого множества не содержат a, а каждый элемент второго множества, напротив, содержит a. Эти два множества равномощны.

[15] Чарльз Доджсон (1832–1898) — английский математик; исследования посвящены теории определителей, математической логике и алгебраической геометрии; автор книг «Алиса в стране чудес» (1865) и «Алиса в Зазеркалье» (1871), написанные им под литературным псевдонимом Льюиса Кэрролла.

[16] В параграфе 2.13 определяются понятия порядка и максимального элемента; там же доказывается, что $\subseteq$ является отношением порядка.

Биекцию легко построить, используя предыдущее замечание: каждому элементу первого множества мы поставим в соответствие это же самое множество, объединенное с $\{a\}$ (а это уже элемент второго множества). Эта идея используется при доказательстве следующей теоремы.

Теорема 5.1. *Пусть* $|A| = n \in \mathbb{Z}^+$. *Тогда* $|\mathcal{P}(A)| = 2^n = 2^{|A|}$.

Доказательство. Индукция по n. Б.И. Если $n = 0$, то $A = \varnothing$, поэтому $\mathcal{P}(A) = \{\varnothing\} \Rightarrow |\mathcal{P}(A)| = 1 = 2^0$. Рассмотрим еще случай $n = 1$, тогда $A = \{a\} \Rightarrow \mathcal{P}(A) = \Big\{\varnothing, \{a\}\Big\} \Rightarrow |\mathcal{P}(A)| = 2^1$.

Ш.И. Предположим, что для любого множества C из условия $|C| = k \Rightarrow |\mathcal{P}(C)| = 2^k$ (предположение индукции). Пусть теперь $|A| = k+1$. Выберем некоторый $a \in A$ и обозначим через $A_1 = A\backslash\{a\}$. Тогда $A = A_1 \cup \{a\}$ и $|A_1| = k$ (теперь для A_1 можно воспользоваться предположением индукции). Выясним, как связаны между собой подмножества из A, и из A_1.

Заметим, что $B \subseteq A \Leftrightarrow B \subseteq A_1$ или существует такое множество $B_1 \subseteq A_1$, что $B = B_1 \cup \{a\}$.

Пусть $X = \{B_1 : B_1 \subseteq A_1\}$, т.е. это все те подмножества множества A, которым не принадлежит элемент a. И $Y = \{B \subseteq A : a \in B\}$ — все остальные подмножества из A.

Используя предыдущее замечание, получаем, что X и Y удовлетворяют следующим свойствам:

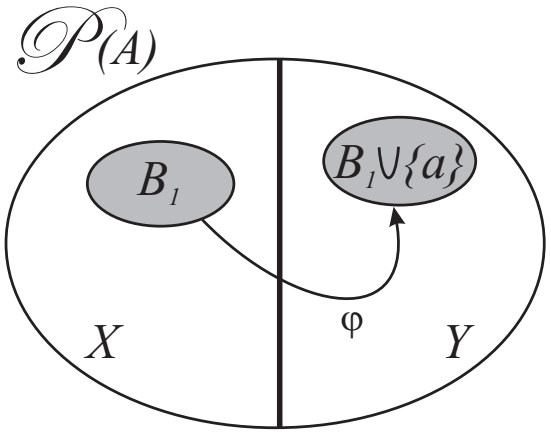

Рис. 11

1. $X = \mathcal{P}(A_1)$.
2. $X \cup Y = \mathcal{P}(A)$.
3. $X \cap Y = \varnothing$.

Множества X и Y равномощны. Биекцию φ можно задать правилом: если $B_1 \in X$, то $\varphi(B_1) = B_1 \cup \{a\}$ (рис. 11). По свойству (1) и по предположению индукции, примененному к A_1, получим $|X| = 2^k$. Из свойств (2) и (3) следует, что $|\mathcal{P}(A)| = |X| + |Y| = 2|X|$. В результате, $|\mathcal{P}(A)| = 2^{k+1}$.

■

Упражнения

1. Попытайтесь представить себе множество всех подмножеств четырехугольника. Принадлежат ли этому множеству стороны этого четырехугольника, его вершины, точка пересечения его диагоналей?

2. Выпишите все элементы множества $\mathcal{P}(\mathbb{N}_{\leqslant 4})$.

3. Пусть A и B — конечные множества. Доказать, что $A = B \Leftrightarrow \mathcal{P}(A) = \mathcal{P}(B)$.

4. Какому из двух множеств, X или Y, в предыдущей теореме принадлежит $\varnothing$?

5. Докажите, что соответствие φ в теореме этого параграфа является биекцией.

6. Что ставит биекция φ в соответствие пустому множеству?

2.6. Отображения конечных множеств. Размещения с повторениями

Напомним, что в параграфе 2.3 было определено отображение между множествами. Всякое отображение из Y в X является подмножеством $Y \times X$ (так как это соответствие), в качестве первых элементов этих пар используются все элементы множества Y (так как отображение всюду определено), и элементы множества Y не могут использоваться в качестве первых элементов пар данного соответствия более одного раза (так как отображение однозначно).

Множество всех отображений одного конечного множества в другое полезно своими комбинаторными[17] приложениями.

Определение.

$$X^Y = \{f : f - \textit{ отображение из } Y \textit{ в } X\}$$

(читается: X в степени Y).

Договоримся использовать символы f, g, h для обозначения отображений.

Пример 1. Пусть $Y = \{a, b, c\}$ и $X = \{1, 2\}$, тогда $f_1 = \{(a, 1), (b, 1), (c, 1)\} \in X^Y$ и $f_2 = \{(a, 1), (b, 1), (c, 2)\} \in X^Y$. Аналогично можно построить шесть оставшихся элементов множества X^Y.

В общем случае какова мощность множества X^Y? Ответ на этот вопрос дает следующая теорема.

[17] Комбинаторикой в первом приближении можно назвать теорию конечных множеств, ее главная задача — определение количества элементов таких множеств.

Теорема 6.1. *Пусть* $|X| = n$, $|Y| = m$, $n, m \in \mathbb{N}$. *Тогда справедлива формула* $|X^Y| = n^m = |X|^{|Y|}$.

Доказательство. Докажем индукцией по m. Пусть $X = \{a_1, \ldots, a_n\}$.

Б.И. $m = 1$. Тогда $Y = \{b\}$. Следовательно, $X^Y = \{f_1, \ldots, f_n\}$, где $f_1 = \{(b, a_1)\}, \ldots, f_n = \{(b, a_n)\}$. Отсюда $|X^Y| = n = n^1$.

Ш.И. Предположим, что для любого множества C из условия $|C| = k$ следует, что $|X^C| = n^k$.

Пусть теперь $|Y| = k + 1$. Выберем $b \in Y$ и обозначим $Y_1 = Y \backslash \{b\}$. Тогда $Y = Y_1 \cup \{b\}$. По предположению $|X^{Y_1}| = n^k$. Выберем произвольное отображение $f \in X^{Y_1}$ (оно не определено в b, поэтому $f \notin X^Y$) и доопределим его на b. Для f существует в точности n различных продолжений (рис. 12):

$$\begin{aligned} f \cup \{(b, a_1)\} &= f_1 \in X^Y, \\ f \cup \{(b, a_2)\} &= f_2 \in X^Y, \\ &\vdots \\ f \cup \{(b, a_n)\} &= f_n \in X^Y. \end{aligned}$$

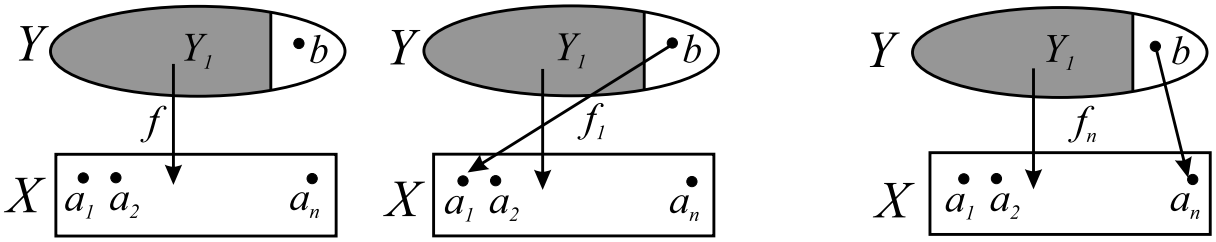

Рис. 12

Нетрудно заметить, что если отображения $f, g \in X^{Y_1}$ различны, то любое продолжение отображения f отличается от любого продолжения отображения g. Поэтому $|X^Y| = |X^{Y_1}| \times$ (количество продолжений) $= n^k \cdot n = n^{k+1}$. ■

Прежде чем ввести новое понятие размещения с повторениями, обсудим понятие упорядоченного k-набора[18] $(a_1, \ldots, a_k)$, состоящего из элементов некоторого множества X. Он отличается от ранее введенного понятия упорядоченной пары (которая является упорядоченным 2-набором) только количеством элементов (конечно, если $k \neq 2$). Основное свойство k-набора такое же: $(a_1, \ldots, a_k) = (b_1, \ldots, b_k) \Leftrightarrow$ одновременно $a_1 = b_1, \ldots, a_k = b_k$. Одно из возможных определений k-набора: $(a_1, \ldots, a_k)$ — это множество $\{(1, a_1), (2, a_2), \ldots, (k, a_k)\}$.

[18]Упорядоченный k-набор также называется k-кортежом.

Пример 2. $(1,a,2)=(b,3,c) \Leftrightarrow 1=b, a=3, 2=c$, но $(1,2,3)\neq$ $\neq(1,3,2)$.

Определение. *Пусть X — конечное множество ($|X|=n\in\mathbb{N}$). Тогда размещением из n элементов по k местам ($k\in\mathbb{N}$) с повторениями называют произвольный упорядоченный k-набор элементов множества X. $\overline{A}_n^k$ — количество всех размещений с повторениями из n элементов по k местам (или коротко: из n по k).*

Пример 3. Пусть $X=\{a,b\}$. Ниже выписаны все размещения по три элемента. Непосредственным подсчетом убеждаемся, что $\overline{A}_2^3=2^3=8$.

$$\begin{array}{cccc}(a,a,a) & (a,a,b) & (a,b,a) & (b,a,a)\\ (b,b,b) & (b,b,a) & (b,a,b) & (a,b,b)\end{array}.$$

Теорема 6.2. *Для любых $n,k\in\mathbb{N}$ выполняется $\overline{A}_n^k=n^k$.*

Доказательство. Достаточно показать, что искомых размещений столько же, сколько элементов во множестве $X^{\mathbb{N}_{\leqslant k}}$. Для этого каждому размещению однозначно поставим в соответствие отображение по следующему правилу:

$$(a_1,\ldots,a_k)\xrightarrow{\varphi}\{(1,a_1),\ldots,(k,a_k)\}=f\in X^{\mathbb{N}_{\leqslant k}}.$$

Легко проверить, что φ — биекция. Поэтому $\overline{A}_n^k=|X^{\mathbb{N}_{\leqslant k}}|=n^k$.

■

Заметим, что в предыдущей теореме мы только используя определение упорядоченного набора построили искомую биекцию. Кстати, другой возможный путь определения k-набора указан в упражнениях к этому параграфу.

Пример 4. Определить количество всевозможных четырехзначных автомобильных номеров для прицепов. Каждый такой номер — это упорядоченный 4-набор (так как порядок цифр важен). Каждая цифра — элемент множества $\{0,1,2,3,4,5,6,7,8,9\}$. Поэтому искомое число равно $\overline{A}_{10}^4=10^4$.

Упражнения

1. Выпишите все восемь отображений из первого примера.

2. Справедлива ли первая теорема этого параграфа, если $Y=\varnothing$?

3. Убедиться в том, что в результате продолжений отображений из X^{Y_1} в первой теореме получатся все элементы множества X^Y.

4. Доказать, что во второй теореме этого параграфа φ действительно является биекцией.

5. Определите упорядоченную тройку следующим образом: $(a,b,c)=((a,b),c)$. Докажите, что $(a,b,c)=(x,y,z)\Leftrightarrow a=x,\ b=y,\ c=z$. Укажите путь строгого определения упорядоченного k-набора.

6. Сколькими способами можно распределить десять бильярдных шаров по шести лузам?

2.7. Взаимно однозначные отображения одного множества в другое

Когда речь идет о биекции между множествами Y и X, часто используют математический синоним: взаимно однозначное отображение Y **на** X. Если число элементов во множестве Y меньше (не больше), чем в X, тогда Y взаимно однозначно можно отобразить только на подмножество из X (сохраняя свойство инъективности, мы не требуем, чтобы отображение было сюръективным). В этом случае мы будем использовать термин — «взаимно однозначное отображение Y в X».

Пример 1. Пусть $Y=\{1,2\}$ и $X=\{a,b,c\}$. Тогда $f_1=\{(1,a),(2,b)\}$, $f_2=\{(1,b),(2,c)\}$, $f_3=\{(1,b),(2,a)\}$, $f_4=\{(1,c),(2,b)\}$, $f_5=\{(1,a),(2,c)\}$ и $f_6=\{(1,c),(2,a)\}$ — примеры всех взаимно однозначных отображений Y в X.

Определение. ${}^YX=\{f: f$ *— взаимно однозначное отображение* Y *в* $X\}$ *(читается* X *в степени* Y *слева).*

Теорема 7.1. *Пусть* $|X|=n$, $|Y|=m$, $n,m\in\mathbb{N}$ *и* $m\leqslant n$. *Тогда*

$$\left|{}^YX\right|=\underbrace{n(n-1)\cdot\ldots\cdot(n-m+1)}_{m\text{ множителей}}.$$

Доказательство. Индукция по m. Пусть $X=\{a_1,\ldots,a_n\}$.

Б.И. Если $m=1$, то $Y=\{b\}$. Обозначим через $f_1=\{(b,a_1)\}$, $\ldots$, $f_n=\{(b,a_n)\}$, тогда ${}^YX=\{f_1,\ldots,f_n\}$. Отсюда $|{}^YX|=n$.

Ш.И. Предположим, что для любого множества C из условия $|C|=k$ следует, что $|{}^CX|=n(n-1)\cdot\ldots\cdot(n-k+1)$.

Пусть теперь $|Y|=k+1$. Выберем $b\in Y$ и обозначим $Y_1=Y\backslash\{b\}$. Тогда $Y=Y_1\cup\{b\}$ и по предположению $|{}^{Y_1}X|=n(n-1)\cdot\ldots\cdot(n-k+1)$. Выберем произвольное отображение $f\in{}^{Y_1}X$ (оно не определено в b, поэтому $f\notin{}^YX$) и доопределим его на b. Заметим, что $|f(Y_1)|=k=|Y_1|$, так как f — биекция между Y_1 и $f(Y_1)$. Следовательно, $|X\backslash f(Y_1)|=n-k$.

Поэтому $X\backslash f(Y_1) = \{c_1, \ldots, c_{n-k}\}$. Теперь легко доопределить взаимно однозначное отображение f на элементе b так, чтобы продолжение также было взаимно однозначным (необходимо элементу b ставить в соответствие один из элементов $X\backslash f(Y_1)$). Существует (рис. 13) в точности $n-k$ различных продолжений отображения f:

$$\begin{aligned} f \cup \{(b, c_1)\} &= f_1 \in {}^{Y}X, \\ f \cup \{(b, c_2)\} &= f_2 \in {}^{Y}X, \\ &\vdots \\ f \cup \{(b, c_{n-k})\} &= f_{n-k} \in {}^{Y}X. \end{aligned}$$

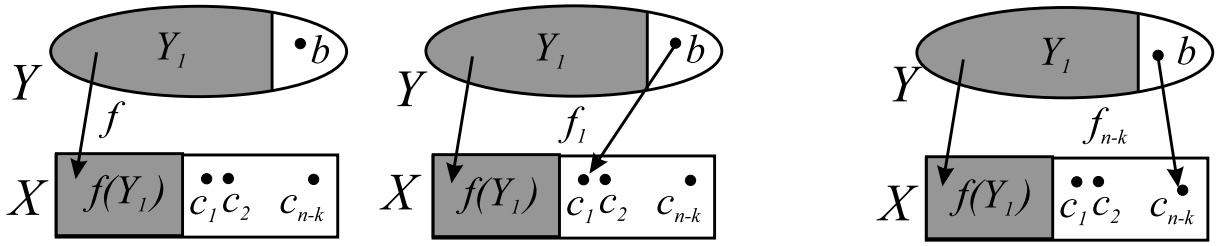

Рис. 13

Нетрудно заметить, что если биекции $f, g \in {}^{Y_1}X$ различны, то любое продолжение биекции f отличается от любого продолжения биекции g. Поэтому

$$\left|{}^{Y}X\right| = \left|{}^{Y_1}X\right| \times (\text{количество продолжений}) =$$

$$= n(n-1)\cdot\ldots\cdot(n-k+1) \times (n-(k+1)+1).$$

■

Следствие. *Пусть* $|X| = n$, $|Y| = m$, $n, m \in \mathbb{N}$ *и* $m \leqslant n$. *Тогда*

$$\left|{}^{Y}X\right| = \frac{n!}{(n-m)!}.$$

Доказательство. Достаточно результат предыдущей теоремы умножить и разделить на $(n-m)!$.

■

Определение. *Пусть* X *— конечное множество (*$|X| = n$, $k, n \in \mathbb{N}$ *и* $k \leqslant n$*). Тогда размещением из* n *элементов по* k *местам называют произвольный упорядоченный* k*-набор различных элементов множества* X*. Число* A_n^k *— это количество всех размещений из* n *по* k*.*

Теорема 7.2.

$$A_n^k = \frac{n!}{(n-k)!}.$$

Доказательство. Достаточно показать, что искомых размещений столько же, сколько элементов во множестве ${}^{\mathbb{N}_{\leqslant k}}X$. Для этого определим биекцию между размещениями и взаимно однозначными отображениями из ${}^{\mathbb{N}_{\leqslant k}}X$ следующим образом:

$$(a_1, \ldots, a_k) \xrightarrow{\varphi} \{(1, a_1), \ldots, (k, a_k)\} = f \in {}^{\mathbb{N}_{\leqslant k}}X.$$

Легко проверить, что φ — биекция. Поэтому $A_n^k = |{}^{\mathbb{N}_{\leqslant k}}X| = \dfrac{n!}{(n-k)!}$.

■

Определение. *Перестановкой n-элементного множества X называется размещение по n местам. P_n — количество всех перестановок.*

Следствие. $P_n = n!$.

Доказательство. Следует из предыдущей теоремы и равенства $0! = 1$.

■

Каждая перестановка элементов множества X задает на этом множестве порядок. Поэтому последняя формула позволяет легко находить число всевозможных упорядочений данного множества.

Пример 2. Сколькими способами можно расставить 10 томов на книжной полке? Из предыдущего замечания — $10!$.

Пример 3. В предыдущей задаче потребуем, чтобы первый и второй тома стояли рядом. Тогда рассуждать можно следующим образом: будем считать тома 1 и 2 за одну книгу, тогда всевозможных расстановок с заданным условием будет $9!$. Но для каждой такой расстановки тома 1 и 2 можно поменять местами, получив еще одну перестановку. Поэтому всего будет $2 \cdot 9!$ расстановок книг таких, что выбранные два тома стоят рядом.

Упражнения

1. Что можно сказать о множестве ${}^{Y}X$, если $|Y| > |X|$?

2. Найдите количество расстановок в последнем примере, если тома 1 и 2 не должны стоять рядом.

3. Сколькими способами можно рассадить n человек за круглым столом? Два способа считаются одинаковыми, если для каждого человека сосед справа и слева остался тем же самым.

4. Сколькими способами можно рассадить n женщин и n мужчин за круглым столом так, чтобы мужчины и женщины чередовались?

5. Сколько существует трехзначных чисел, делящихся на 5, каждое из которых состоит из различных цифр?

2.8. Сочетания. Треугольник Паскаля. Бином Ньютона

Определение. *Пусть* $k \in \mathbb{N}$, $|X| = n \geqslant k$, $k \in \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$. *Сочетанием из* n *элементов по* k *местам называют произвольное* k*-элементное подмножество множества* X. C_n^k *— количество всех сочетаний из* n *по* k.

Не важно, в каком порядке расположены элементы во множестве. Так, например, $\{1, 2, 3\} = \{3, 2, 1\}$. Этим сочетания отличаются от размещений.

П р и м е р 1. Пусть $X = \{a, b, c\}$. Выпишем все размещения по два элемента и все сочетания по два элемента и определим C_3^2:

Размещения		Сочетания
(a, b)	(b, a)	$\{a, b\}$
(a, c)	(c, a)	$\{a, c\}$
(b, c)	(c, b)	$\{b, c\}$

Заметим, что размещения в каждой строке отличаются только порядком элементов, и поэтому они дают только одно сочетание. Отсюда $C_3^2 = A_3^2/2! = 3$. Этим замечанием мы воспользуемся в следующей теореме.

Теорема 8.1.

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Доказательство. Пусть $|X| = n$. Обозначим через R_k множество всех размещений множества X по k местам. Разобьем множество R_k на классы. К одному классу будут относиться те размещения, которые отличаются только порядком элементов. Так, размещения $(b_1, \ldots, b_k)$ и $(c_1, \ldots, c_k)$ попадают в один класс тогда и только тогда, когда $\{b_1, \ldots, b_k\} = \{c_1, \ldots, c_k\}$. Это разбиение удовлетворяет следующим свойствам:

1) количество элементов в каждом классе равно $k!$,

2) классы между собой не пересекаются,

3) каждому классу соответствует в точности одно сочетание,

4) различным классам соответствуют различные сочетания.

Элементами каждого класса являются различные перестановки некоторого k-элементного множества, поэтому выполняется первое свойство. Свойства 2 и 4 следуют из определения классов. В каждом классе перестановки отличаются только порядком элементов, поэтому им соответствует только одно сочетание, состоящее из этих элементов. В результате

$$C_n^k = \frac{A_n^k}{P_k} = \frac{n!}{k!(n-k)!}.$$

■

Теорема 8.2. *Число сочетаний удовлетворяет следующим свойствам:*

1. $C_n^k = C_n^{n-k}$,
2. $C_n^0 + C_n^1 + \ldots + C_n^n = \sum\limits_{k=0}^{n} C_n^k = 2^n$,
3. $C_n^{k-1} + C_n^k = C_{n+1}^k$.

Доказательство. Свойство 1 следует из теоремы 8.1.

2. C_n^k — это число k-элементных подмножеств X, где $(|X| = n)$. Тогда $C_n^0 + C_n^1 + \ldots + C_n^n$ — это число всех подмножеств множества X. По теореме 5.1 о мощности степени множества, получим $\sum\limits_{k=0}^{n} C_n^k = |\mathcal{P}(X)| = 2^n$.

$$3.\quad C_n^{k-1} + C_n^k = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} =$$

$$= \frac{n!(n-k+1) + n! \cdot k}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} = C_{n+1}^k.$$

■

Соотношение 3 называют *основным рекуррентным* свойством числа сочетаний. Оно позволяет легко заполнить первые строчки следующей бесконечной таблицы (она называется треугольником Паскаля[19]). Каждый элемент этой таблицы C_{n+1}^k равен сумме двух соседних элементов C_n^{k-1} и C_n^k, стоящих в предыдущей строке (если они есть).

[19]Блез Паскаль (1623–1662) — французский математик, механик, философ; основные направления исследований — проективная геометрия, анализ бесконечно малых, проектирование вычислительных машин, построил более 50 таких машин; открыл метод полной математической индукции; установил закон распределения давления в жидкостях (закон Паскаля).

Треугольник Паскаля
(нахождение C_n^k)

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10	...
0	1											
1	1	1										
2	1	2	1									
3	1	3	3	1								
4	1	4	6	4	1							
5	1	5	10	10	5	1						
6	1	6	15	20	15	6	1					
7	1	7	21	35	35	21	7	1				
8	1	8	28	56	70	56	28	8	1			
9	1	9	36	84	126	126	84	36	9	1		
10	1	10	45	120	210	252	210	120	45	10	1	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Хорошо известно, что

$(x+y)^1 = 1 \cdot x + 1 \cdot y, \qquad (x+y)^2 = 1 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2,$

$(x+y)^3 = 1 \cdot x^3 + 3 \cdot x^2 y + 3 \cdot xy^2 + 1 \cdot y^3.$

Коэффициенты в правых частях равенств совпадают с числами, стоящими в строчках треугольника Паскаля. Это справедливо и в общем случае. Формула следующей теоремы называется формулой *бинома Ньютона*[20].

Теорема 8.3. *Для любых* $x, y \in \mathbb{R}$, $n \in \mathbb{N}$ *выполняется*

$$(x+y)^n = C_n^0 x^n + C_n^1 x^{n-1} y + \ldots + C_n^k x^{n-k} y^k + \ldots + C_n^n y^n = \sum_{k=0}^{k=n} C_n^k x^{n-k} y^k.$$

Доказательство. Приведем два доказательства этой формулы. Первое будет комбинаторным, второе — по индукции.

1. Представим левую часть формулы в виде произведения n множителей и занумеруем скобки числами от 1 до n:

$$(x+y)^n = \underbrace{(x+y)}_{1}\underbrace{(x+y)}_{2} \cdot \ldots \cdot \underbrace{(x+y)}_{n}.$$

[20]Исаак Ньютон (1643–1727) — английский математик, физик, астроном, основоположник современной механики; открыл закон всемирного тяготения; создал теоретические основания для дифференциального и интегрального исчисления (совместно с Г. В. Лейбницем); президент Лондонского королевского общества (с 1703); директор Лондонского монетного двора (с 1699).

Определим количество слагаемых вида $x^{n-k}y^k$ после раскрытия скобок. Для этого рассмотрим произвольное сочетание по k элементов множества $X = \{1, 2, \ldots, n\}$. Каждое такое сочетание однозначно определяет номера скобок, из которых выбирается y, из остальных выбирается x. Таким образом, каждому такому сочетанию соответствует одно слагаемое вида $x^{n-k}y^k$ и наоборот. Поэтому количество слагаемых $x^{n-k}y^k$ после раскрытия скобок будет равно C_n^k.

2. Индукция по n. Б.И. Случай $n = 1$ очевиден.

Ш.И. Предположим, для n это утверждение выполняется. Докажем справедливость формулы для $n+1$:

$$(x+y)^{n+1} = (x+y)^n(x+y) =$$
$$= (C_n^0x^n + C_n^1x^{n-1}y + \ldots + C_n^{k-1}x^{n+1-k}y^{k-1} + C_n^kx^{n-k}y^k + \ldots + C_n^ny^n)(x+y) =$$
$$= C_n^0x^{n+1} + (C_n^0 + C_n^1)x^ny + \ldots + (C_n^{k-1} + C_n^k)x^{n-k+1}y^k + \ldots + C_n^ny^{n+1} =$$
$$= C_{n+1}^0x^{n+1} + C_{n+1}^1x^ny + \ldots + C_{n+1}^kx^{n-k+1}y^k + \ldots + C_{n+1}^{n+1}y^{n+1}.$$

В последнем переходе мы использовали равенство $C_n^0 = C_{n+1}^0 = C_{n+1}^{n+1} = 1$ и рекуррентное свойство числа сочетаний.

■

Следствие 1. *Для любых $x, y \in \mathbb{R}$, $n \in \mathbb{N}$ выполняется*

$$(x-y)^n = C_n^0x^n - C_n^1x^{n-1}y + \ldots (-1)^kC_n^kx^{n-k}y^k + \ldots (-1)^nC_n^ny^n.$$

Доказательство. Достаточно заметить, что все слагаемые, в которых степень y нечетна, будут со знаком минус.

■

Следствие 2. *(4-е свойство числа сочетаний) Для любых $n \in \mathbb{N}$ выполняется*

$$C_n^0 - C_n^1 + C_n^2 - C_n^3 + \ldots (-1)^kC_n^k + \ldots (-1)^nC_n^n = 0.$$

Доказательство. Достаточно воспользоваться предыдущей формулой для бинома $(1-1)^n$.

■

Упражнения

1. Сравнивая коэффициенты при x^k в обеих частях равенства $(1+x)^m(1+x)^n = (1+x)^{n+m}$, доказать, что

$$C_n^kC_m^0 + C_n^{k-1}C_m^1 + \ldots + C_n^0C_m^k = C_{m+n}^k.$$

2. Доказать, что сумма квадратов биномиальных коэффициентов равна C_{2n}^n (т.е. $\sum_{k=0}^n (C_n^k)^2 = C_{2n}^n$).

3. Доказать, что

$$1 - 10C_{2n}^1 + 10^2C_{2n}^2 - 10^3C_{2n}^3 + \ldots - 10^{2n-1}C_{2n}^1 + 10^{2n} = (81)^n.$$

4. Упростить выражение $P_1 + 2P_2 + \ldots + nP_n$.

2.9. Перестановки и сочетания с повторениями

Название этого параграфа содержит противоречие: в перестановках и сочетаниях элементы не могут повторяться. Но для решения некоторых задач удобно использовать специальные конструкции, которые лучше называть именно таким образом. Рассмотрим примеры таких задач и затем введем необходимые определения.

П р и м е р 1. Сколько существует различных 5-буквенных слов, полученных перестановкой букв слова «потоп» (словом будем называть любой набор букв)? Сделаем несколько полезных замечаний. Порядок букв в словах важен, так, например, «потоп» это не то же самое, что «оптоп». С другой стороны, «оптоп» и «оптоп» совпадают, хотя в них и переставлены местами две буквы «о». Итак, порядок не важен, когда речь идет об одинаковых буквах, и важен в случае, если местами меняются разные буквы. Число всех таких различных 5-буквенных слов будем считать следующим образом: на пять пустых мест будем расставлять сначала буквы одного типа, затем другого и т.д. Количество способов расставить две буквы «о» на 5 пустых мест — это количество способов выбрать 2 места из 5, т.е. C_5^2 . На оставшиеся места для каждой такой расстановки будем размещать две буквы «п»(таких размещений — C_3^2) и, наконец, на оставшееся место поместим «т»(таких размещений — C_1^1). Итак, количество слов равно $C_5^2 \cdot C_3^2 \cdot C_1^1$ (перемножаем, так как для каждой расстановки после первого этапа мы образуем C_3^2 расстановок на втором этапе и т.д.).

Определение. *Пусть дано k_1 элементов 1-го типа, k_2 — 2-го, $\ldots, k_m$ — m -го типа. И $k_1 + k_2 + \ldots + k_m = n$. Тогда перестановкой из n элементов с повторениями $k_1, \ldots, k_m$ называются размещение с повторениями, в котором в точности k_1 элементов 1-го типа, k_2 — 2-го, $\ldots, k_m$ — m -го типа. $\overline{P}_n(k_1, \ldots, k_m)$ — количество всех таких перестановок.*

Так, в предыдущем примере два элемента 1-го типа (две буквы «о»), два элемента 2-го типа (две буквы «п») и один элемент 3-го типа. Мы нашли, что $\overline{P}_5(2, 2, 1) = 30$.

Общий результат выглядит так:

Теорема 9.1.

$$\overline{P}_n(k_1,\ldots,k_m)=\frac{n!}{k_1!k_2!\cdot\ldots\cdot k_m!}\,.$$

Доказательство. Любую такую перестановку с заданным числом повторений можно получить следующим образом:

выбираем места для элементов 1-го типа — их $C_n^{k_1}$;

выбираем места для элементов 2-го типа из оставшихся — их $C_{n-k_1}^{k_2}$;

$$\vdots$$

выбираем места для элементов m-го типа из оставшихся — их $C_{k_m}^{k_m}$.

Число всех размещений равно

$$\overline{P}_n(k_1,\ldots,k_m)=C_n^{k_1}\cdot C_{n-k_1}^{k_2}\cdot\ldots\cdot C_{k_m}^{k_m}=$$

$$=\frac{n!(n-k_1)!(n-k_1-k_2)!\cdot\ldots\cdot k_m!}{k_1!(n-k_1)!k_2!(n-k_1-k_2)!\cdot\ldots\cdot k_m!k_m!(k_m!-k_m!)}=$$

$$=\frac{n!}{k_1!k_2!\cdot\ldots\cdot k_m!}\,.$$

■

Заметим только, что результат будет таким же, если вы будете сначала выбирать места для элементов 2-го типа и т.д.

Теперь о сочетаниях с повторениями. Снова начнем с примера.

П р и м е р 2. Предположим, что вы решили купить 5 (пять!) пирожных трех видов, которые есть в продаже. И предположим (это сделать уже сложнее), что у вас нет привязанности к пирожным какого-то определенного типа. Сколько существует различных вариантов выбора? Обозначим через A, B, C виды пирожных. Тогда могут быть такие варианты: $AAAAA$, $ABBBB$ или $ABCCC$. Снова займемся наблюдениями. Порядок видов пирожных не важен, так, вариант $BABBB$ совпадает с $ABBBB$. Важно только количество пирожных данного типа. Поэтому по каждому выбору будем образовывать перестановку по следующему правилу: ставим k_1 единиц, если выбрано k_1 пирожных первого типа, затем ставим 0 (если пирожных первого типа нет, конечно, сразу ставим 0), далее ставим k_2 единиц, если выбрано k_2 пирожных второго типа, затем снова ставим ноль и, наконец, ставим столько единиц, сколько выбрано пирожных последнего типа. Для выборов выше это будут перестановки с повторениями (1111100), (1011110) и (1010111) соответственно. Итак, 5 единиц и 2 разделяющих нуля. И наоборот, по каждой такой перестановке можно восстановить выбор. Искомое число — $\overline{P}_7(5,2)=21$.

Определение. *Сочетаниями из n различных типов по k элементов с повторениями называются неупорядоченные совокупности, состоящие из k элементов, каждый из которых принадлежит к одному из этих n типов.*

Число всех таких совокупностей будем обозначать через $\overline{C}_n^k$.

Теорема 9.2.

$$\overline{C}_n^k = C_{n-1+k}^k = C_{n-1+k}^{n-1}.$$

Доказательство. Покажем, что таких сочетаний с повторениями столько же, сколько и перестановок с повторениями из k единиц и $n-1$ нулей.

Построение взаимно однозначного соответствия приведено в примере 2. Отличие состоит только в том, что в общем случае будет k единиц и $n-1$ нулей, чтобы отделить один тип элементов от другого. Если сочетания различны, то хотя бы один из разделяющих нулей будет стоять на другой позиции. И наоборот, если один из нулей, скажем, i-го типа, следует после другого количества единиц, это сразу же означает, что выбрано неодинаковое количество элементов этого типа и сочетания получаются различными. Поэтому

$$\overline{C}_n^k = \overline{P}_{n-1+k}(k, n-1) = \frac{(n-1+k)!}{k!(n-1)!} = C_{n-1+k}^k.$$

Последнее равенство следует из второго свойства числа сочетаний.

■

Следуя комбинаторному доказательству формулы бинома Ньютона, можно получить формулу

$$(a_1 + a_2 + \ldots + a_m)^n = \sum_{k_1+\ldots+k_m=n} \overline{P}_n(k_1, k_2, \ldots, k_m) a_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_m^{k_m}.$$

Упражнения

1. Докажите последнюю формулу, занумеровав скобки и определив количество слагаемых вида $a_1^{k_1} a_2^{k_2} \cdot \ldots \cdot a_m^{k_m}$.

2.10. Счетные множества

В этом параграфе мы начинаем изучение бесконечных множеств. Немного забегая вперед, сделаем на первый взгляд странное утверждение: бесконечные множества могут быть по-разному бесконечны. Поэтому мы начнем с самых маленьких из бесконечных — со счетных множеств. Напомним, что при определении конечных множеств мы пользовались начальными отрезками натурального ряда. Теперь нашим эталоном будет все множество натуральных чисел.

Определение. *Счетным множеством называется произвольное множество* A, *равномощное множеству* $\mathbb{N}$ *(как обычно, существует биекция* $A \xrightarrow{\varphi} \mathbb{N}$*).*

Пример 1. Множество всех натуральных чисел, начиная с двойки, т. е. $\mathbb{N}_{\geqslant 2} = \{n \in \mathbb{N} : n \geqslant 2\}$, является счетным множеством. Одна из возможных биекций задается правилом: $\varphi(k) = k - 1, \quad k \in \mathbb{N}_{\geqslant 2}$,

2	3	4	...	n	...	$\mathbb{N}_{\geqslant 2}$
$\downarrow$	$\downarrow$	$\downarrow$	...	$\downarrow$	...	
1	2	3	...	$n-1$	...	$\mathbb{N}$

Пример 2. Множество всех четных натуральных чисел ($\mathbb{N}_2$) также счетно. Биекцию можно задать, например, так: $\varphi(n) = 2n, \quad n \in \mathbb{N}$.

1	2	3	...	n	...	$\mathbb{N}$
$\downarrow$	$\downarrow$	$\downarrow$	...	$\downarrow$	...	
2	4	6	...	$2n$	...	$\mathbb{N}_2$

Лемма 10.1. *Множество* A *счетно в том и только в том случае, когда его можно представить в виде* $A = \{a_1, a_2, \ldots, a_n, \ldots\}$, *где* $a_i \neq a_j$ *для всех различных* $i, j \in \mathbb{N}$.

Доказательство. Действительно, если биекция $A \xrightarrow{\varphi} \mathbb{N}$ существует, то, обозначив через $a_n = \varphi^{-1}(n)$, мы получим искомое представление.

Обратно, если такое представление задано, то биекцию можно задать правилом $\varphi(n) = a_n, \quad n \in \mathbb{N}$.

■

Теорема 10.2. *Любое бесконечное подмножество множества* $\mathbb{N}$ *счетно.*

Доказательство. Пусть $A \subseteq \mathbb{N}$ и A бесконечно. Занумеруем элементы множества A так, что $a_1 = \min A$ и $a_i = \min(A \backslash \{a_1, a_2, \ldots, a_{i-1}\})$ при

$i > 1$. Множество $A\backslash\{a_1, a_2, \ldots, a_{i-1}\}$ непусто, иначе $A \subseteq \{a_1, a_2, \ldots, a_{i-1}\}$ и было бы конечно. Из теоремы о полноте порядка на $\mathbb{N}$ следует, что в любом непустом подмножестве $\mathbb{N}$ найдется минимальный элемент, поэтому определение a_i корректно. Обозначим через $B = \{a_1, a_2, \ldots, a_n, \ldots\}$ — множество всех занумерованных элементов множества A и докажем, что B удовлетворяет условиям предыдущей леммы и $B = A$.

Сначала индукцией по $n \in \mathbb{N}$ проверим выполнение следующих свойств, которыми обладают элементы множества B:

1) $a_1 < a_2 < \ldots < a_n$;

2) $a_i \geqslant i$ для любого $i \leqslant n$;

3) каждый элемент множества $A\backslash\{a_1, a_2, \ldots, a_n\}$ больше любого из a_1, $a_2, \ldots,$ a_n.

Б.И. При $n = 1$ утверждения (1)–(3) очевидно выполняются.

Ш.И. Предположим, что a_1, $a_2, \ldots,$ a_k удовлетворяют (1)–(3). Поскольку a_{k+1} выбран из $A\backslash\{a_1, a_2, \ldots, a_k\}$, из свойства (3) по предположению индукции следует, что $a_k < a_{k+1}$. Поэтому для a_{k+1} справедливо (1).

По предположению индукции $a_k \geqslant k$. Мы уже установили, что выполняется $a_{k+1} > a_k \geqslant k$, откуда следует $a_{k+1} \geqslant k + 1$ и (2) для a_{k+1} доказано.

По определению $a_{k+1} = \min(A\backslash\{a_1, a_2, \ldots, a_k\})$, поэтому для всех $b \in A\backslash\{a_1, a_2, \ldots, a_k, a_{k+1}\}$ следует, что $b \geqslant a_{k+1}$ и $b \neq a_{k+1}$, т. е. (3) для a_{k+1} также доказано.

Теперь докажем равенство $A = B$ включением в обе стороны. Включение $B \subseteq A$ следует из определения множества B, поэтому достаточно доказать, что для любого $a \in A$ следует, что $a \in \{a_1, a_2, \ldots, a_n, \ldots\}$. О/п: пусть существует $a \in A$, что $a \notin \{a_1, a_2, \ldots, a_n, \ldots\}$. Заметим, что $a = m$ для некоторого $m \in \mathbb{N}$. Тогда $a = m \leqslant a_m$. С другой стороны, из третьего свойства следует, что $a \in A\backslash\{a_1, a_2, \ldots, a_m\} \Rightarrow a > a_m$. $\lightning$.

Из свойства (1) и предыдущей леммы следует, что B счетно, поэтому и A — счетное множество.

■

Следствие 1. *Множество простых чисел счетно.*

Доказательство. Верно, поскольку $P \subseteq \mathbb{N}$ и P бесконечно по теореме Евклида.

■

Следствие 2. *Множество* $\mathbb{N}_q = \{q^n : n \in \mathbb{N}\}$, *где* $q \in \mathbb{N}$ *счетно, если* $q > 1$.

Доказательство. Поскольку $q \in \mathbb{N}$ и $q > 1$, из свойств порядка на $\mathbb{N}$ следует, что $q^{n+1} > q^n$. Поэтому $\mathbb{N}_q$ бесконечно и счетно по предыдущей теореме.

■

Следствие 3. *Любое бесконечное подмножество B счетного множества A счетно.*

Доказательство. Пусть $B \subseteq A$ и B — бесконечно. Так как $A \sim \mathbb{N}$, то существует биекция $A \xrightarrow{\varphi} \mathbb{N}$. Тогда $\varphi(B)$ — бесконечное подмножество $\mathbb{N}$. По предыдущей теореме оно счетно. Следовательно, $B \sim \varphi(B) \sim \mathbb{N}$. Поэтому B — счетное множество.

■

В следующей теореме используется операция счетного объединения. До сих пор мы объединяли не более чем конечное число множеств. Пусть теперь дано счетное число множеств $A_1, A_2, \ldots, A_n, \ldots$, тогда

$$\bigcup_{n=1}^{\infty} A_n = \cup_{n=1}^{\infty} A_n = \{a : a \in A_n \text{ хотя бы для одного } n \in \mathbb{N}\}.$$

Например, $\cup_{n=1}^{\infty}\{n\} = \mathbb{N}$ или $\cup_{n=1}^{\infty}\mathbb{N}_{\leqslant n} = \mathbb{N}$. Оказывается, счетные объединения не выводят из класса счетных множеств, т. е., объединяя в счетном числе счетные множества, всегда будет получаться счетное множество.

Теорема 10.3. *Счетное объединение счетных множеств счетно.*

Доказательство. Пусть $A_1, A_2, \ldots, A_n, \ldots$ — счетные множества.

I. Рассмотрим случай, когда эти множества попарно не пересекаются. Выше определялись множества $\mathbb{N}_m$. Мы будем рассматривать множества $\mathbb{N}_{p_n}$, где p_n — n-е по счету простое число. Заметим, что множества $\mathbb{N}_{p_i}$ и $\mathbb{N}_{p_j}$ попарно не пересекаются при $i \neq j$. Иначе $(p_i)^k = (p_j)^l$ при некоторых $k, l \in \mathbb{N}$, но правая и левая части этого равенства имеют различные делители.

Так как множества A_n и $\mathbb{N}_{p_n}$ счетны, то между ними существует биекция $\varphi_n : A_n \longrightarrow \mathbb{N}_{p_n}$. Определим теперь биекцию $\varphi : \cup_{n=1}^{\infty} A_n \longrightarrow \cup_{n=1}^{\infty}\mathbb{N}_{p_n}$ следующим образом:

$$\text{если } a \in A_n, \text{ то } \varphi(a) = \varphi_n(a).$$

Множество $\cup_{n=1}^{\infty}\mathbb{N}_{p_n}$ счетно как бесконечное подмножество $\mathbb{N}$. Следовательно, $\cup_{n=1}^{\infty} A_n$ также счетно.

II. Теперь рассмотрим общий случай, когда A_i и A_j могут пересекаться между собой. Тогда рассмотрим множества $B_1 = A_1$, $B_2 = A_2 \backslash A_1$, $\ldots$, $B_n = A_n \backslash (\cup_{k=1}^{n-1} A_k)$. Заметим, что

- $\cup_{n=1}^{\infty} A_n = \cup_{n=1}^{\infty} B_n$,
- $\cup_{n=1}^{\infty} B_n$ — бесконечно,
- B_i и B_j при различных i и j между собой не пересекаются.

Снова будем рассматривать отображения φ_n , определенные выше, но уже для B_n . Если некоторое B_n окажется конечным, то φ_n — взаимно однозначное отображение B_n в $\mathbb{N}_{p_n}$ (если $B_n = \varnothing$, то и $\varphi_n = \varnothing$). В результате φ также будет взаимно однозначным отображением $\cup_{n=1}^{\infty} B_n$ в $\cup_{n=1}^{\infty} \mathbb{N}_{p_n}$. Следовательно, φ — это биекция между $\cup_{n=1}^{\infty} B_n$ и $\varphi(\cup_{n=1}^{\infty} B_n)$. Множество $\varphi(\cup_{n=1}^{\infty} B_n)$, как бесконечное подмножество $\mathbb{N}$, счетно. Следовательно, $\cup_{n=1}^{\infty} A_n = \cup_{n=1}^{\infty} B_n$ — счетное множество.

■

Следствие 1. *Множество целых чисел $\mathbb{Z}$ счетно.*

Доказательство. Действительно, $\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\} \cup \{0\}$, т.е. это объединение двух счетных множеств и конечного множества.

■

Следствие 2. *Множество пар $\mathbb{Z}_n = \{(k, n) : k \in \mathbb{Z}\}$ счетно, где $n \in \mathbb{N}$.*

Доказательство. Каждое из этих множеств равномощно с $\mathbb{Z}$, так как n фиксировано.

■

Следствие 3. *Множество рациональных чисел $\mathbb{Q}$ счетно.*

Доказательство. Любое рациональное число можно представить в виде упорядоченной пары (k, n) , где $k \in \mathbb{Z}$, $n \in \mathbb{N}$. Тогда $\mathbb{Q} = \cup_{n=1}^{\infty} \mathbb{Z}_n$ и множество $\mathbb{Q}$ является счетным объединением счетных множеств.

■

Следствие 4. *Множество точек на плоскости с обеими рациональными координатами, т.е. множество $\mathbb{Q} \times \mathbb{Q}$, счетно.*

Доказательство. $\mathbb{Q} \times \mathbb{Q} = \cup_{r \in \mathbb{Q}} (\mathbb{Q} \times \{r\})$. В этом равенстве справа стоит счетное объединение счетных множеств.

■

Ранее количество элементов в конечных множествах мы обозначали через $|A| = n$, где n — натуральное число или ноль. Для обозначения мощности бесконечных множеств используют бесконечные кардинальные числа. Так, мощность $\mathbb{N}$ равна $\aleph_0$ (алеф-ноль). По аналогии с предыдущими обозначениями будем записывать $|\mathbb{N}| = \aleph_0$. В следующем параграфе выяснится,

что счетные множества не являются единственными представителями класса бесконечных множеств и существуют другие кардинальные числа.

Упражнения

1. Можно ли определение φ в теореме 10.3 заменить определением $\varphi = \cup_{n=1}^{\infty}\varphi_n$?

2. Проверьте, что φ из теоремы 10.3 в первом случае является биекцией, а во второй части доказательства — взаимно однозначным отображением «в».

2.11. Несчетные множества

Биекции между счетными множествами часто задаются с помощью формул. Приведем примеры других способов описаний биекций.

П р и м е р 1. Интервал от 0 до 1 равномощен действительной прямой $\mathbb{R}$ ($(0;1) \sim \mathbb{R}$). Доказать это утверждение можно в два этапа: установить равномощность интервала и дуги окружности (без концевых точек), на рис. 14 это делается с помощью биекции ψ , и равномощность последней с вещественной прямой (биекция φ) доказывается с помощью проектирования из центра этой окружности. Композиция этих биекций будет искомой биекцией.

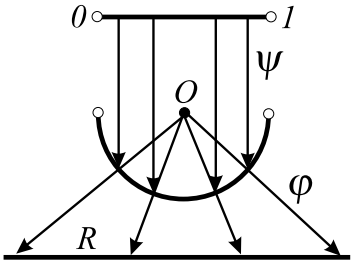

Рис. 14

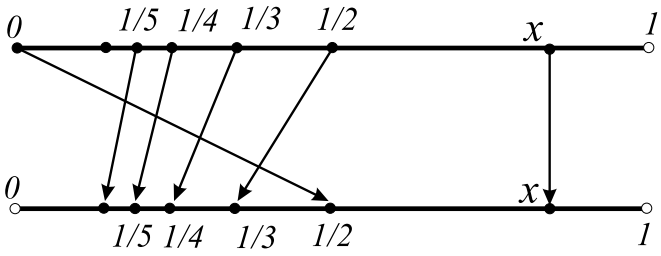

Рис. 15

П р и м е р 2. Сложнее построить биекцию между полуинтервалом $[0;1)$ и интервалом $(0;1)$. Для этого выберем счетное множество интервала, например $A = \{1/n : n \in \mathbb{N}, n \geqslant 2\}$. Заметим, что $A \subseteq (0;1) \subseteq [0;1)$. Зададим биекцию между отрезком и интервалом следующим образом (рис. 15):

$$\varphi(x) = \begin{cases} 1/2, & x = 0, \\ 1/(n+1), & x = 1/n, \\ x, & \text{во всех остальных случаях.} \end{cases}$$

Все свойства биекции легко проверяются, а идея построения используется при доказательстве следующей теоремы.

Лемма 11.1. *В любом бесконечном множестве X существует счетное подмножество.*

Доказательство. Пусть X бесконечно. Будем строить два счетных непересекающихся подмножества A и B по индукции.

Б.И. $n = 1$. Пусть a_1 — произвольный элемент множества X, а b_1 — произвольный элемент из $X\backslash\{a_1\}$.

Ш.И. Предположим, что уже выбраны различные $a_1, \ldots, a_k$, $b_1, \ldots, b_k$. Тогда множество $X\backslash\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ бесконечно и поэтому содержит по крайней мере два различных элемента. Один из них мы обозначим через a_{k+1}, другой — через b_{k+1}.

В результате мы получим два непересекающихся счетных множества: $A = \{a_1, \ldots, a_n, \ldots\}$ и $B = \{b_1, \ldots, b_n, \ldots\}$.

■

Кроме того, что мы нашли счетное подмножество в X (например, A), мы показали, что его можно выбрать так, чтобы $X\backslash A$ продолжало оставаться бесконечным.

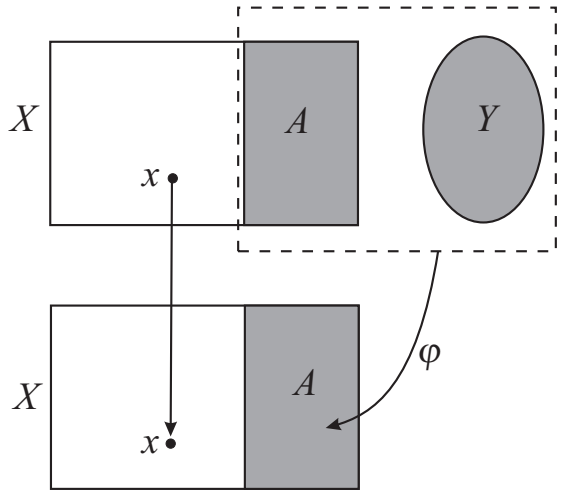

Рис. 16

Теорема 11.2. *Если X бесконечно и Y — конечно или счетно, то справедливо $X \cup Y \sim X$.*

Доказательство. 1. Пусть пересечение $X \cap Y = \varnothing$ (рис. 16). Тогда, пользуясь предыдущей леммой, выделим счетное подмножество $A \subseteq X$. Множество $A \cup Y$ счетно, поэтому существует биекция $\varphi : (A \cup Y) \longrightarrow A$. Теперь опишем биекцию между $X \cup Y$ и X. Пусть

$$\psi(x) = \begin{cases} \varphi(x), & \text{если } x \in (A \cup Y), \\ x, & \text{в остальных случаях.} \end{cases}$$

2. Если $X \cap Y \neq \varnothing$, то заметим, что $X \cup Y = X \cup Y_1$, где $Y_1 = Y\backslash X$. Осталось применить первый случай к Y_1 и X.

■

Определение. *Если существует взаимно однозначное отображение множества X на подмножество из Y, будем писать $|X| \leqslant |Y|$ (мощность X не превосходит мощности Y). Если при этом не существует взаимно однозначного отображения X на все Y, будем писать $|X| < |Y|$ (мощность X*

строго меньше мощности Y*). Если существует биекция между* X *и* Y*, тогда будем использовать обозначение* $|X| = |Y|$ *(мощности множеств* X *и* Y *совпадают).*

Так, если A — счетное множество, то $|A| = |\mathbb{N}| = \aleph_0$. Кроме того, из леммы следует, что для любого бесконечного X выполняется $|\mathbb{N}| \leqslant |X|$.

Каждое ли бесконечное множество является счетным? Оказалось совсем нетрудно получить множество строго большей мощности. Кантор заметил, что операция взятия множества всех подмножеств всегда приводит к образованию множества строго большей мощности. Следующую теорему будем называть *первой теоремой Кантора.*

Теорема 11.3. *Для любого множества* X *выполняется неравенство* $|\mathcal{P}(X)| > |X|$.

Доказательство. Нам необходимо проверить, что существует взаимно однозначное отображение X в $\mathcal{P}(X)$ и при этом между ними не существует биекции.

1. Пусть $\varphi(x) = \{x\}, \quad x \in X$. Тогда φ — взаимно однозначно отображает X на множество $\{\{x\} : x \in X\}$. Последнее содержится в $\mathcal{P}(X)$.

2. Покажем, что любое отображение из X не является отображением на $\mathcal{P}(X)$ (т. е. нет ни одного сюръективного отображения, тем более не существует биекции). Возьмем произвольное отображение $f : X \longrightarrow \mathcal{P}(X)$. Это отображение ставит в соответствие элементам множества X некоторые подмножества X, которые являются элементами $\mathcal{P}(X)$. Найдем множество A, которое не поставлено в соответствие ни одному элементу из X. Определим его так:

$$A^* = \{x \in X : x \notin f(x)\}.$$

Покажем, что оно искомое.

О/п: пусть существует $x^* \in X$, что $f(x^*) = A^* \in \mathcal{P}(X)$. Возможны два случая: $x^* \in A^*$ или $x^* \notin A^*$.

а) пусть $x^* \in A^* \Rightarrow x^* \notin f(x^*) \Rightarrow x^* \notin A^*$. $\lightning$.

б) пусть теперь $x^* \notin A^* \Rightarrow x^* \notin f(x^*) \Rightarrow x^* \in A^*$. $\lightning$.

Итак, отображение f не является отображением «на», поэтому не может быть биекцией.

■

Следствие. $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Определение. $\mathfrak{c} = |\mathcal{P}(\mathbb{N})|$. *Кардинальное число* $\mathfrak{c}$ *называют мощностью континуума.*

Определение. $2^{\aleph_0} = |\{0,1\}^{\mathbb{N}}|$, *т.е. кардинальное число* $2^{\aleph_0}$ *является мощностью множества всех отображений из* $\mathbb{N}$ *в неупорядоченную пару* $\{0,1\}$.

Лемма 11.4. $\mathfrak{c} = 2^{\aleph_0}$.

Доказательство. Достаточно доказать, что множества $\mathcal{P}(\mathbb{N})$ и $\{0,1\}^{\mathbb{N}}$ равномощны. Построим биекцию между ними. Пусть A — произвольное подмножество из $\mathbb{N}$, тогда обозначим через f_A такое отображение:

$$f_A(n) = \begin{cases} 1, & \text{если } n \in A; \\ 0, & \text{если } n \notin A. \end{cases}$$

Тогда искомой биекцией будет $\varphi(A) = f_A$. Соответствие φ всюду определено и взаимно однозначно. Покажем, что оно сюръективно. Для произвольного $f \in \{0,1\}^{\mathbb{N}}$ образуем такое множество $A = \{n \in \mathbb{N} : f(n) = 1\}$. Тогда $f_A = f \Rightarrow \varphi(A) = f$.

■

Следующие две теоремы отвечают на вопрос: какова же мощность $\mathbb{R}$? Теорема 11.5 утверждает, что $\mathbb{R}$ несчетно; метод, который в ней используется, называется *диагональным методом Кантора*. Теорема 11.6 усиливает результат, утверждая, что множества $\mathbb{R}$ и $\mathcal{P}(\mathbb{N})$ равномощны.

Следующую теорему будем называть *второй теоремой Кантора*.

Теорема (Кантор) 11.5. $|\mathbb{R}| > |\mathbb{N}|$.

Доказательство. О/п: предположим, что $\mathbb{R}$ счетно. Тогда и интервал $(0;1)$ счетен, поэтому $(0;1)$ можно представить в виде $\{a_1, a_2, \ldots, a_n, \ldots\}$. Каждое вещественное число a_n запишем в виде бесконечной десятичной дроби $a_n = 0, a_1^n a_2^n \ldots a_n^n \ldots$. Получим следующие представления всех элементов $(0;1)$:

$$\begin{gathered} a_1 = 0, a_1^1 a_2^1 \ldots a_n^1 \ldots \\ a_2 = 0, a_1^2 a_2^2 \ldots a_n^2 \ldots \\ \vdots \\ a_n = 0, a_1^n a_2^n \ldots a_n^n \ldots \\ \vdots \end{gathered}$$

Покажем, что среди выписанных чисел нет по крайней мере одного числа $a^* = 0, a_1^* a_2^* \ldots a_n^* \ldots$ из $(0;1)$. Определим его десятичные знаки следующим образом: $a_1^* \in \{4,5\}\backslash\{a_1^1\}$; $a_2^* \in \{4,5\}\backslash\{a_2^2\}; \ldots$; $a_n^* \in \{4,5\}\backslash\{a_n^n\}; \ldots$ Первая цифра после запятой отличает a^* от a_1, вторая — от a_2, от бесконечной

десятичной дроби a_n число a^* отличается n-й цифрой после запятой, поэтому $a \notin (0;1) = \{a_1, a_2, \ldots, a_n, \ldots\}$. С другой стороны, числа a_i^* выбираются так, что не может получиться 0 и 9 в периоде, поэтому $a^* \in (0;1)$. $\lightning$.

■

Следующую теорему будем называть *третьей теоремой Кантора.*

Теорема 11.6. $|\mathbb{R}| = \mathfrak{c}$.

Доказательство. В начале этого параграфа (примеры 1 и 2) мы показали, что $[0;1) \sim (0;1) \sim \mathbb{R}$. Поэтому достаточно доказать, что $|[0;1)| = \mathfrak{c}$.

Каждому числу $b \in [0;1)$ однозначно можно поставить в соответствие его двоичное представление вида $b = 0, b_1 b_2 \ldots b_n \ldots$, где $b_i \in \{0,1\}$ для любого $i \in \mathbb{N}$ (по определению, в нем не может быть бесконечного периода из единиц, начиная с некоторого места). Каждому такому представлению однозначно соответствует отображение $f_b \in \{0,1\}^{\mathbb{N}}$ такое, что $f_b(n) = b_n$ для каждого $n \in \mathbb{N}$ или, немного подробнее:

$$f_b(n) = \begin{cases} 1, & \text{если } b_n = 1; \\ 0, & \text{если } b_n = 0. \end{cases}$$

Обозначим множество всех отображений, которые соответствуют числам из $[0;1)$, через X, а через Y — множество $\{0,1\}^{\mathbb{N}} \backslash X$. Для каждого $f \in Y$ найдется такое натуральное число $n \in \mathbb{N}$, что $f(i) = 1$ для всех $i \geqslant n$, т. е. отображение f принимает значение 1, начиная с n. Теперь легко доказать счетность множества Y. Действительно, различных отображений, принимающих значение 1, начиная с n, только конечное число (их не более 2^n). Поэтому Y является счетным объединением конечных множеств. Следовательно, Y счетно или конечно. Уже доказано, что $[0;1) \sim X$, теперь же по теореме 11.2 получаем, что

$$|\mathbb{R}| = |[0;1)| = |X| = |X \cup Y| = |\{0,1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}.$$

■

Упражнения

1. Доказать, что соответствия φ и ψ, с помощью которых строилась биекция между интервалом $(0;1)$ и $\mathbb{R}$ в начале этого подраздела, являются биекции.

2. Объединение счетного числа конечных множеств может оказаться конечным множеств. Убедитесь, что множество Y в теореме 11.6 счетно.

2.12. Теорема Кантора–Бернштейна

В предыдущем параграфе было определено отношение $|X| \leqslant |Y|$ (существует биекция множества X на некоторое подмножество из Y). Очевидно, что $|X| \leqslant |X|$. Если $|X| \leqslant |Y|$ (φ — биекция, отображающая X на подмножество из Y) и $|Y| \leqslant |Z|$ (ψ — биекция, отображающая Y на подмножество из Z), то $\psi \circ \varphi$ взаимно однозначно отображает X на некоторое подмножество Z, следовательно, $|X| \leqslant |Z|$.

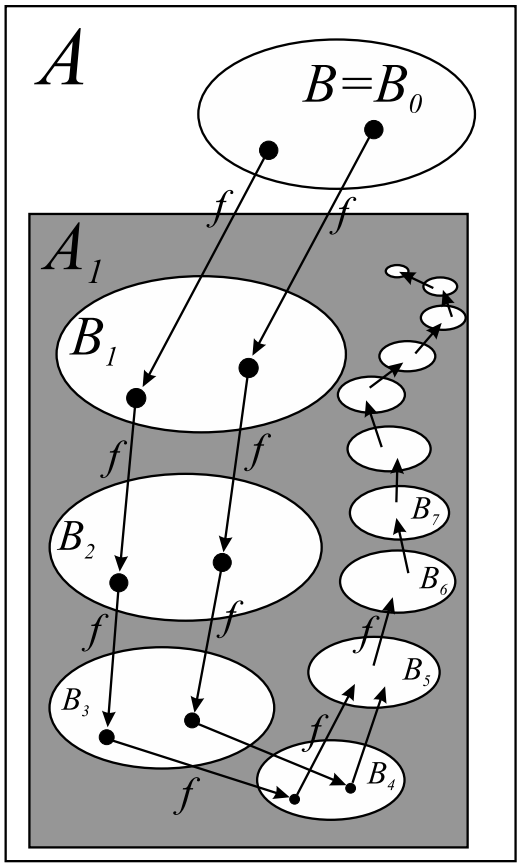

Рис. 17

Предположим теперь, что есть биекция X на подмножество из Y и, наоборот, существует биекция Y на подмножество из X (т.е. $|X| \leqslant |Y|$, и $|X| \leqslant |Y|$), можно ли в этом случае построить биекцию уже между множествами X и Y (т.е. $|X| = |Y|$)?

Утвердительный ответ на этот вопрос, впервые поставленный Г. Кантором, был дан его юным учеником Феликсом Бернштейном[21] зимой 1896–1897 г. Следующая теорема называется *теоремой Кантора–Бернштейна.*

Теорема 12.1. *Если существует взаимно однозначное отображение A в B и, наоборот, из B в A, то между A и B можно построить биекцию (т. е. из $|A| \leqslant |B|$ и $|A| \geqslant |B| \Rightarrow |A| = |B|$).*

Доказательство. Рассмотрим сначала частный случай теоремы.

I. Пусть $B \subseteq (A \backslash A_1)$ и $A \sim A_1$ (рис. 17). Докажем, что $(B \cup A_1) \sim A_1$. Так как $A \sim A_1$, то существует биекция $f : A \to A_1$. Построим биекцию между $(B \cup A_1)$ и A_1. Введем некоторые обозначения. Пусть $B_0 = B$, $B_1 = f(B)$. В общем случае $B_{i+1} = f(B_i)$.

Заметим, что $B \subseteq A \Rightarrow B_1 = f(B) \subseteq f(A) = A_1$. Покажем сначала, что B_i и B_j при разных значениях i и j не пересекаются. Из двух условий $B_0 \subseteq (A \backslash A_1)$ и $B_1 \subseteq A_1$ следует, что $B_0 \cap B_1 = \varnothing$.

[21] Феликс Бернштейн (1878–1956) — немецкий математик, учился у Кантора и Гильберта; основные исследования относятся к теории чисел, теории множеств, теории интегральных уравнений, теории вероятностей; начиная с 20-х годов занимался применением математических методов к задачам генетики и теории наследственности.

Теперь предположим, что для любых $i < j < n$ выполняется $B_i \cap B_j = \varnothing$. Покажем, что $B_j \cap B_n = \varnothing$. По предположению $B_{j-1} \cap B_{n-1} = \varnothing$. По свойству биекции для любых $C \cap D = \varnothing$ следует, что $f(C) \cap f(D) = \varnothing$. Поэтому $f(B_{j-1}) \cap f(B_{n-1}) = \varnothing$. Но $f(B_{j-1}) = B_j$ и $f(B_{n-1}) = B_n$, откуда $B_j \cap B_n = \varnothing$.

Теперь опишем искомую биекцию:

$$\varphi(x) = \begin{cases} f(x), & \text{если } x \in B_i, \text{ для некоторого } i \in \mathbb{N} \cup \{0\}; \\ x, & \text{в остальных случаях.} \end{cases}$$

На рис. 17 темные места множества $B \cup A_1$ соответствуют точкам, которые переходят сами в себя (т. е. остаются неподвижными), светлые множества B_i переходят последовательно друг в друга. Покажем, что φ является биекцией между $B \cup A_1$ и A_1. Очевидно, что φ всюду определено. Так как f, являясь биекцией, отображает множество B_i на множество B_{i+1} и

$$A_1 = (A_1 \setminus \cup_{i=1}^{\infty} B_i) \cup (\cup_{i=1}^{\infty} B_i),$$

то φ сюръективно. Однозначность следует из однозначности f и того факта, что выполняется в точности одно из двух условий: $x \in B_i$ для некоторого $i \in \mathbb{N} \cup \{0\}$ или нет. Немного сложнее проверить инъективность (разным $x, y \in B \cup A_1$ соответствуют разные $\varphi(x), \varphi(y) \in A_1$). Выберем различные $x, y \in B \cup A_1$ и рассмотрим четыре возможных случая:

1) x, y принадлежат темной (неподвижной) части (т.е. $x, y \notin B_i$ для любого $i \in N \cup \{0\}$), тогда $\varphi(x) = x \neq y = \varphi(y)$;

2) один из них, например, x, принадлежит темной части, другой — одному из B_i, тогда $\varphi(y)$ принадлежит следующему светлому множеству — B_{i+1}, а $\varphi(x) = x$, поэтому выполняется $\varphi(x) \neq \varphi(y)$;

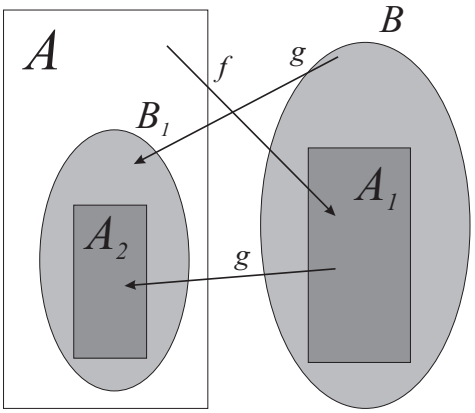

Рис. 18

3) x, y принадлежат различным светлым множествам B_i и B_j, тогда $\varphi(x)$, $\varphi(x)$ также принадлежат различным светлым множествам — B_{i+1} и B_{j+1}, тогда $\varphi(x) \neq \varphi(y)$;

4) x, y принадлежат одному светлому множеству B_i; так как f — биекция, то $\varphi(x) \neq \varphi(y)$.

Все свойства биекции проверены.

II. Докажем теперь, что все промежуточные множества между двумя равномощными множествами им равномощны. Пусть $A_1 \subseteq B \subseteq A$ и $A \sim A_1$. Тогда $B = (B \setminus A_1) \cup A_1$ и по предыдущему случаю $B \sim A_1 \sim A$.

III. Перейдем к доказательству общего случая. Пусть теперь выполняются $A \sim f(A) = A_1 \subseteq B$ и $B \sim g(B) = B_1 \subseteq A$, где f и g — биекции на соответствующие подмножества (рис. 18). Тогда $A \sim A_1 \sim g(A_1) = A_2$ и $A_2 \subseteq B_1$.

Применяя второй случай для множеств A, B_1, A_2, получаем, что существует биекция φ между A и B_1. Следовательно, $g^{-1} \circ \varphi$ — искомое взаимно однозначное отображение A на B.

■

Следствие 1. $(0;1] \sim (0;1)$.

Доказательство. $(0;1] \sim (0;\frac{1}{2}] \subseteq (0;1)$ ($f(x) = \frac{1}{2}x$ — биекция между $(0;1]$ и $(0;\frac{1}{2}]$). С другой стороны, $(0;1) \subseteq (0;1]$, и остается применить предыдущую теорему. Заметим, что каждое B_i состоит только из одной точки: $B_0 = 1$, $B_1 = \frac{1}{2}$, $B_i = \frac{1}{i+1}$. Если строить биекцию между $[0;1]$ и $(0;1)$, то каждое B_i будет состоять из двух точек.

■

Используя проектирование и центральное проектирование (см. пример 1 и пример 2 предыдущего параграфа), можно показать, что круг без границы равномощен полусфере без ограничивающей окружности; последняя, в свою очередь, равномощна плоскости (предлагаем повращать рис. 14 относительно прямой, проходящей через точку O и перпендикулярной к прямой $\mathbb{R}$).

Следствие 2. *Квадрат без границы равномощен кругу без ограничивающей окружности.*

Доказательство. Пусть A — квадрат без границы и B — круг без ограничивающей окружности. Тогда существует круг без границы $B_1 \subseteq A$. Так как $B_1 \sim B \Rightarrow |B| \leqslant |A|$. Аналогично в B содержится некоторый квадрат без границы A_1 (при этом $A_1 \sim A \Rightarrow |A| \leqslant |B|$). По теореме Кантора–Бернштейна получим, что $|A| = |B|$.

■

Следствие 3. *Квадрат без границы* $(0;1) \times (0;1)$ *равномощен интервалу* $(0;1)$.

Доказательство. Очевидно, что $|(0;1)| \leqslant |(0;1) \times (0;1)|$ (так как $(0;1) \sim \sim \left\{\frac{1}{2}\right\} \times (0;1)$).

Построим биекцию $(0;1)\times(0;1)$ на некоторое подмножество интервала $(0;1)$. Пусть $(x,y)\in(0;1)\times(0;1)$. Рассмотрим представление x и y в виде бесконечных десятичных дробей: $x=0,x_1x_2\ldots$ и $y=0,y_1y_2\ldots$ Зададим теперь отображение следующим образом: $f((x,y))=z=0,x_1y_1x_2y_2\ldots$ Это отображение ставит в соответствие число, у которого после запятой на нечетных местах стоят десятичные знаки x, а на четных — десятичные знаки y. Если $(x,y)\neq(x',y')$, то они различаются хотя бы по одной координате, значит, десятичные представления этих координат отличаются в некотором десятичном разряде, следовательно, $z\neq z'$. Итак, f — взаимно однозначное отображение $(0;1)\times(0;1)$ в $(0;1)$.

По теореме Кантора–Бернштейна $(0;1)\times(0;1)\sim(0;1)$.

■

Следующее утверждение также было доказано Кантором.

Следствие 4. $|\mathbb{R}|=|\mathbb{R}\times\mathbb{R}|$.

Доказательство. $\mathbb{R}\sim(0;1)\sim(0;1)\times(0;1)\sim$ (кругу без границы) $\sim$ $\sim$ (полусфере без ограничивающей окружности) $\sim\mathbb{R}\times\mathbb{R}$.

■

Предыдущий результат фактически означает следующее: на прямой и на плоскости одинаковое количество точек.

Упражнения

1. Сравните доказательства того факта, что $[a;b)\sim(a;b)$, приведенные в этом и предыдущем параграфах.

2. Докажите, что любые два круга равномощны.

3. Является ли отображение f, построенное в доказательстве следствия 3, биекцией квадрата без границы на интервал?

4. Докажите, что точек в пространстве столько же, сколько их на прямой.

5. Докажите, что если $X\sim Y$ и X,Y — бесконечные множества, то $X\cup Y\sim X$.

6. Справедлив ли предыдущий результат для пересечения множеств?

7. Докажите, что $\mathbb{R}^n\sim\mathbb{R}$ для любого $n\in\mathbb{N}$.

8. Докажите, что если для любого $n\in\mathbb{N}$ выполняется $X_n\sim Y$ и X,Y — бесконечные множества, то $\cup_{n=1}^{\infty}X_n\sim Y$.

9. Докажите, что $\cup_{n=1}^{\infty}\mathbb{R}^n\sim\mathbb{R}$.

2.13. Отношения порядка и эквивалентности. Лексикографический порядок

Соответствие может устанавливать связи между элементами разных множеств A и B, а может связывать между собой элементы одного и того же множества, т. е. когда $B = A$. В последнем случае такое соответствие принято называть отношением на множестве A.

Определение. *Отношением ρ на множестве A называют произвольное подмножество декартового квадрата $A \times A$ (т.е. $\rho \subseteq A \times A$). Если $(x, y) \in \rho$, будем использовать обозначение $x \ \rho \ y$ (x и y находятся между собой в отношении ρ)*[22].

Так, например, любое отношение на множестве вещественных чисел является подмножеством плоскости $\mathbb{R} \times \mathbb{R}$. Изображение этого подмножества называют *графиком* отношения. Таким образом, отношение на множестве $\mathbb{R}$ и его график означают одно и то же множество плоскости.

Рассмотрим некоторые примеры отношений и их графиков.

Пример 1. $\rho \subseteq P \times P$, где P — множество всех людей. Отношение ρ зададим так: $a \ \rho \ b \Leftrightarrow$ когда дни рождения a и b совпадают.

Пример 2. $\rho \subseteq \mathbb{N} \times \mathbb{N}$. Пусть $n \ \rho \ m \Leftrightarrow$ когда n делит m. Это отношение делимости на множестве $\mathbb{N}$.

Пример 3. $\rho \subseteq \mathbb{N} \times \mathbb{N}$. Пусть $n \ \rho \ m \Leftrightarrow$ когда $n \equiv m \pmod{k}$. Это отношение означает «быть сравнимыми между собой по модулю k», где $k \in \mathbb{N} \backslash \{1\}$.

Пример 4. $\rho \subseteq \mathbb{R} \times \mathbb{R}$. $x \ \rho \ y \Leftrightarrow y = kx + b$. График этого отношения — прямая $y = kx + b$ (рис. 19).

Пример 5. $\rho \subseteq \mathbb{R} \times \mathbb{R}$. $x \ \rho \ y \Leftrightarrow x^2 + (y-4)^2 = 4$. График этого отношения — окружность с центром в $(0, 4)$ и радиусом 2 (рис. 19).

Пример 6. $\rho \subseteq \mathbb{R} \times \mathbb{R}$. $x \ \rho \ y \Leftrightarrow (x+4)^2 + y^2 \leqslant 1$. График этого отношения — круг с центром в $(-4, 0)$ радиуса 1 (рис. 19).

Пример 7. $\rho \subseteq \mathbb{R} \times \mathbb{R}$. Зададим его с помощью некоторой фигуры Φ на плоскости. $x \ \rho \ y \Leftrightarrow (x, y) \in \Phi$. Графиком этого отношения будет в точности эта фигура Φ (рис. 19).

Пример 8. $\rho \subseteq L \times L$, где L — множество всех прямых на плоскости или в пространстве. Пусть $a, b \in L$, $a \ \rho \ b \Leftrightarrow$ когда прямые a и b между собой параллельны. Будем считать по определению, что совпадающие прямые также параллельны.

[22] Греческая буква ρ читается как «ро».

Пример 9. $\rho \subseteq T \times T$. Где T — множество всех треугольников на плоскости. Пусть $\triangle ABC, \triangle DEF \in T$, $\triangle ABC \ \rho \ \triangle DEF \Leftrightarrow$ когда треугольники $\triangle ABC$ и $\triangle DEF$ подобны.

Пример 10. $\rho \subseteq \mathcal{P}(X) \times \mathcal{P}(X)$, где X — некоторое множество. Пусть $A, B \subseteq X$. Тогда $A \rho B \Leftrightarrow A \subseteq B$.

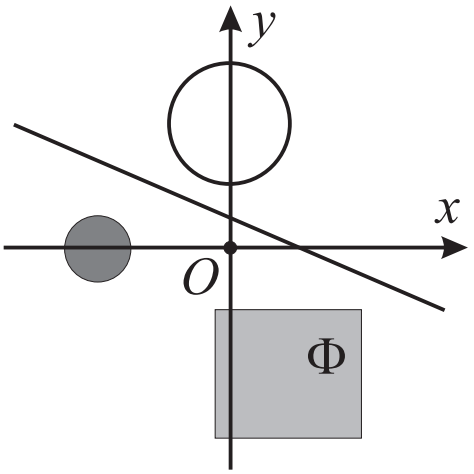

Рис. 19

Среди огромного числа отношений на множестве A мы выделим несколько важных типов:

1) ρ *рефлексивно*, если $a \ \rho \ a$ для любых $a \in A$;

2) ρ *симметрично*, если $a \ \rho \ b \Rightarrow b \ \rho \ a$;

3) ρ *антисимметрично*, если $a \ \rho \ b$ и $b \ \rho \ a \ \Rightarrow a = b$;

4) ρ *транзитивно*, если $a \ \rho \ b$ и $b \ \rho \ c \Rightarrow a \ \rho \ c$;

5) ρ — отношение *порядка*, если оно рефлексивно, антисимметрично и транзитивно;

6) ρ — отношение *эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Примеры 1, 3, 8 и 9 являются примерами отношений эквивалентности. Скажем, в примере 3, если n, m и m, l дают одинаковые остатки при делении на k, то n и l также дают одинаковые остатки при делении на k. Поэтому отношение сравнения по модулю k транзитивно. Также легко проверить остальные свойства для этого и других отношений.

Отношение эквивалентности мы будем обозначать через $\sim$ (отношение равномощности между множествами также является отношением эквивалентности; подобие треугольников — тоже).

Определение. *Пусть $(A, \sim)$ — множество с отношением эквивалентности на нем. Множество $A(a) = \{b \in A : b \sim a\}$ мы будем называть классом эквивалентности по этому отношению $\sim$ (рис 20).*

Определение. *Множество A разбивается на подмножества A_s, $s \in S$, где S — некоторое множество индексов, если $A = \cup_{s \in S} A_s$ и множества A_s и $A_{s'}$ совпадают или не пересекаются.*

Теорема 13.1. *Пусть $(A, \sim)$ — множество с отношением эквивалентности на нем. Тогда отношением $\sim$ это множество разбивается на*

классы эквивалентности. И наоборот, если существует разбиение множества $A = \cup_{s\in S} A_s$, *то существует такое отношение эквивалентности на множестве* A, *что каждое* A_s *будет классом эквивалентности.*

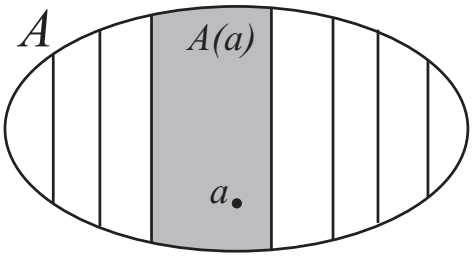

Рис. 20

Доказательство. Пусть $\sim$ — отношение эквивалентности. В силу рефлексивности верно $a \sim a$, поэтому $A = \cup_{a\in A} A(a)$. Покажем, что любые два класса или совпадают, или не пересекаются. Если $c \in A(a) \cap A(b)$, то, используя транзитивность, $a \sim c \sim b \Rightarrow a \sim b$. Следовательно, $A(a) = A(b)$. Получим искомое представление $A = \cup_{a\in A} A(a)$.

Наоборот, если задано некоторое разбиение $A = \cup_{s\in S} A_s$, то введем отношение следующим образом: $a\ \rho\ b$, если $a, b \in A_s$ для некоторого $s \in S$. Легко проверить, что оно искомое.

■

Следующим широко распространенным отношением является отношение порядка. Делимость на множестве натуральных чисел (пример 2) является отношением порядка. Очевидно, что n делит n. Если n делит m и m делит n, то они совпадают. И, наконец, если n делит m и m делит l, то n делит l. Поэтому выполняются соответственно свойства рефлексивности, антисимметричности и транзитивности для данного отношения. Включение множеств (см. пример 10) очевидно обладает свойствами рефлексивности, антисимметричности и транзитивности, поэтому также является отношением порядка.

Отношение порядка будем обозначать с помощью $\leqslant$ или $\preceq$. Множество X с отношением порядка $\leqslant$ на нем обозначается через $(X, \leqslant)$ и называется *частично упорядоченным множеством* (ЧУМ).

Часто к свойствам порядка добавляется четвертое свойство — любые два элемента $a, b \in A$ можно сравнить между собой.

Определение. *Отношение порядка* $\leqslant$ *называется отношением линейного порядка, если для любых* $a, b \in X$ *выполняется* $a \leqslant b$ *или* $b \leqslant a$.

Множество с отношением линейного порядка называется *линейно упорядоченным множеством* (ЛУМ). Порядок в примере 2 не является линейным — уже для 2 и 3 не выполняется ни утверждение «два делит три», ни «три делит два». Примерами линейных порядков являются отношения $\leqslant$ на множествах натуральных, целых, действительных чисел.

Определение. *Пусть* $B \subseteq A$. *Тогда* $a_0 \in B$ *называют наименьшим (соответственно наибольшим) в* B, *если для любых* $b \in B$ *выполняется неравенство* $a_0 \leqslant b$ ($b \leqslant a_0$). *Элемент* $a_0 \in B$ *называют минимальным (соответственно максимальным) в* B, *если для любых* $b \in B, b \leqslant a_0$ ($b \in B, a_0 \leqslant b$) *выполняется* $b = a_0$ ($b = a_0$).

Быть наименьшим или наибольшим элементом — это более сильное свойство, чем быть просто минимальным или максимальным элементом. Так, в двухэлементном множестве $A = \{a, b\}$ (дуплете), с очень бедным порядком $\leqslant = \{(a, a),\ (b, b)\}$ (свойства порядка легко проверяются), a и b являются одновременно максимальными и минимальными элементами по очень простой причине: нет элементов в A больших или меньших их. Но ни один из них не является наибольшим или наименьшим элементом — для этого они должны быть больше или меньше другого, а это не так. Во множествах с линейным порядком, где любые два элемента сравнимы между собой, соответствующие пары терминов означают одно и то же.

Теорема 13.2. *1) пусть* $(X, \leqslant)$ — *ЧУМ,* $A \subseteq X$ *и* $A \neq \varnothing$. *Тогда*
а) если a_0 — *наименьший элемент в* A, *то* a_0 *является минимальным элементом в* A;
б) если a_0 — *наибольший элемент в* A, *то* a_0 *является максимальным элементом в* A.

2) пусть $(X, \leqslant)$ — *ЛУМ,* $A \subseteq X$ *и* $A \neq \varnothing$. *Тогда*
а) a_0 — *наименьший элемент в* $A \Leftrightarrow$ a_0 *является минимальным элементом в* A;
б) a_0 — *наибольший элемент в* $A \Leftrightarrow$ a_0 *является максимальным элементом в* A.

Доказательство. 1) утверждения (а) и (б) сразу следуют из определения.

2) (а) $\Rightarrow$) доказано в (1).

$\Leftarrow$) пусть $a_0 = \min A$ и рассмотрим произвольный элемент $b \in A$. Из линейности порядка $\leqslant$ следует, что выполняется одно из двух условий: $b < a_0$ или $a \leqslant b$. Первое условие противоречит $a_0 = \min A$, поэтому $\forall b \in A \Rightarrow a_0 \leqslant b$. Мы доказали, что a_0 — наименьший элемент в A.

■

Из предыдущего результата следует, что наименьший (или наибольший) элемент в A корректно обозначать $\min A$ (соответственно $\max A$).

Определение. *Отношение линейного порядка* $\leqslant$ *на множестве* X *называ-*

ется отношением полного порядка, если в любом его непустом подмножестве $A \subseteq X$ найдется минимальный элемент. Множество с полным порядком на нем называют вполне упорядоченным множеством (ВУМ).

Так, $(\mathbb{N}, \leqslant)$ является примером вполне упорядоченного множества (см. теоремы о линейности и полноте порядка на $\mathbb{N}$). В любом непустом подмножестве $M \subseteq N$ легко найти минимальный элемент. В то же время $(\mathbb{Z}, \leqslant)$ — ЛУМ, но не ВУМ. В качестве подмножества без минимального элемента можно взять само множество $\mathbb{Z}$. Оказывается, по вполне упорядоченным множествам можно проводить индуктивные доказательства. Такой тип доказательства называют *трансфинитной* индукцией.

Теорема 13.3. *Пусть $(X, \leqslant)$ — вполне упорядоченное множество и a_0 — минимальный элемент в X. Кроме того, $p(a)$ — некоторое утверждение, принимающее для любого $a \in X$ истинное или ложное значение и удовлетворяющее двум свойствам:*
(a) базе, т.е. $p(a_0)$ истинно;
(b) для него доказан шаг, т.е. в предположении, что для любого $a < b$ утверждение $p(a)$ — истинно, доказано, что $p(b)$ также истинно.
Тогда $p(a)$ истинно для любого $a \in X$.

Доказательство. О/п: пусть это не так, т. е. найдется $b_0 \in X$, для которого $p(b_0)$ ложно. Рассмотрим множество $A = \{b \in X : p(b) \text{ — ложно}\}$. Это множество не является пустым, поэтому, в силу полноты порядка, в нем найдется минимальный элемент. Обозначим его через b^* (по базе индукции $b^* \neq a_0$). Тогда для любого $a < b^*$ выполняется $a \notin A \Rightarrow p(a)$ — истинно. Так как шаг доказан, из истинности $p(a)$ для любого $a < b^*$ следует, что $p(b^*)$ — истинно. Но $b^* \in A$. $\lightning$.

■

На декартовых произведениях множеств тоже можно ввести порядок, при условии, что существует порядок на каждом из множителей. Это нам поможет при упорядочивании слагаемых в многочленах от нескольких переменных.

Определение. *Пусть $(X_1, \leqslant_1)$, $(X_2, \leqslant_2), \ldots, (X_n, \leqslant_n)$ — упорядоченные множества. Отношение $\leqslant$ называется лексикографическим порядком на произведении $X = X_1 \times X_2 \times \ldots \times X_n = \prod\limits_{i=1}^{n} X_i$, если оно определяется следующим образом: для любых $x_i, y_i \in X_i$, где $i \in \mathbb{N}_{\leqslant n}$*

$$(x_1, x_2, \ldots, x_n) \leqslant (y_1, y_2, \ldots, y_n) \Leftrightarrow \text{ существует такое}$$

$$i_0 \in \{0,\dots,n\},\ \textit{что}\ x_i = y_i\ \textit{при}\ i \in \{0,\dots,i_0\}\ \textit{и}\ x_{i_0+1} <_{i_0+1} y_{i_0+1}.$$

Например, если лексикографически упорядочить декартову плоскость, то $(1,5) < (2,1)$ (здесь $i_0 = 0$). По похожему принципу упорядочиваются слова в словарях и энциклопедиях: сначала по первой букве, затем внутри слов с одинаковой первой буквой — по второй и т.д. Теперь понятно и происхождение термина. Является ли лексикографический порядок отношением порядка? Следующая теорема, в частности, дает ответ и на этот вопрос.

Теорема 13.4. *Пусть дано семейство упорядоченных множеств* $(X_1,\leqslant_1)$, $(X_2,\leqslant_2),\dots,(X_n,\leqslant_n)$, *отношение* $\leqslant$ *— лексикографический порядок на множестве* $X = \prod\limits_{i=1}^{n} X_i$. *Тогда*

1) $(X,\leqslant)$ *— ЧУМ;*
2) если $(X_i,\leqslant_i)$ *— ЛУМ для каждого* $i \in \mathbb{N}_{\leqslant n}$, *то* $(X,\leqslant)$ *— ЛУМ;*
3) если $(X_i,\leqslant_i)$ *— ВУМ для каждого* $i \in \mathbb{N}_{\leqslant n}$, *то* $(X,\leqslant)$ *— ВУМ.*

Доказательство. В последнем утверждении теоремы необходимо проверить пять свойств. Мы будем доказывать их последовательно, поэтому ограничиваясь первыми тремя (или четырьмя), можно получить справедливость утверждения (1) (или (2)).

3) докажем индукцией по n. В качестве базы рассмотрим случай $n = 2$ (если $n = 1$, доказательство очевидно). Проверим выполнение всех пяти свойств отношения полного порядка.

Рефлексивность. Так как для любого $a \in X_1$ и $b \in X_2 \Leftrightarrow a \leqslant_1 a$ и $b \leqslant_2 b$, то $(a,b) \leqslant (a,b)$. Поэтому «$\leqslant$» удовлетворяет рефлексивности.

Антисимметричность. Предположим, что одновременно $(a,b) \leqslant (a_1,b_1)$ и $(a_1,b_1) \leqslant (a,b)$. Из первого отношения получаем $a <_1 a_1$ или $a = a_1$ и $b \leqslant_2 b_1$. Если $a <_1 a_1$, то второе соотношение ложно, поэтому $a = a_1$. Аналогично $b = b_1$. Получаем, что антисимметричность также выполняется.

Транзитивность. Предположим, что $(a,b) \leqslant (c,d)$ и $(c,d) \leqslant (e,f)$. Покажем, что $(a,b) \leqslant (e,f)$. Исключим из дальнейшего рассмотрения только тривиальный случай совпадения двух или сразу всех пар.

1. $a <_1 c$. Поскольку $c \leqslant_1 e \Rightarrow a <_1 e \Rightarrow (a,b) < (e,f)$.

2. $a = c \Rightarrow b <_2 d$.

   (a) $c <_1 e \Rightarrow a <_1 e \Rightarrow (a,b) < (e,f)$.

(b) $c = e \Rightarrow d <_2 f \Rightarrow b <_2 f \Rightarrow (a,b) < (e,f)$.

Линейность. Рассмотрим две произвольные пары (a,b), $(c,d) \in X$. Так как порядок $\leqslant_1$ линеен, то выполняется одно из трех соотношений: $a <_1 c$, $a >_1 c$ или $a = c$. В первом и во втором случае получаем соответственно $(a,b) < (c,d)$ и $(a,b) > (c,d)$.

Если же $a = c$, то используем линейность порядка $\leqslant_2$: $b >_2 d$ или $b \leqslant_2 d$. Окончательно получаем, что $(a,b) > (c,d)$ или $(a,b) \leqslant (c,d)$.

Существование минимального элемента. Пусть C — произвольное непустое подмножество $X = X_1 \times X_2$. Рассмотрим множество $A = \{a \in X_1 :$ существует такой элемент $b \in X_2$, что $(a,b) \in C\}$ (т.е. $A = Dom\ C$). Так как $(X_1, \leqslant_1)$ является вполне упорядоченным множеством, то в A найдется минимальный элемент. Обозначим его через a^* и рассмотрим множество $B = \{b \in X_2 : (a^*, b) \in C\}$. Это множество не пусто и, в силу полноты порядка $\leqslant_2$, в нем также найдется минимальный элемент — b^*. Покажем, что (a^*, b^*) является минимальным элементом в C. Действительно, для любой пары $(a,b) \in C \Leftrightarrow a^* <_1 a$ или $a^* = a$. В первом случае получаем $(a^*, b^*) < (a,b)$, а во втором — $(a^*, b^*) \leqslant (a,b)$, используя уже минимальность b^* во множестве B.

Ш.И. Предположим, что утверждение истинно, если $n < k$, и докажем его для $n = k$. Для этого первые два сомножителя в декартовом произведении $X = X_1 \times X_2 \times \ldots \times X_k$ обозначим через $Y = X_1 \times X_2$. Последовательно используя базу и предположение индукции, получаем, что лексикографические порядки на Y и на $Y \times X_3 \times \ldots \times X_k$ являются отношениями полного порядка. Осталось только заметить, что лексикографический порядок на $Y \times X_3 \times \ldots \times X_k$ совпадает с лексикографическим порядком на X, что и завершает доказательство.

■

Следствие. *Пусть $X_i = \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ для каждого $i \in \mathbb{N}_{\leqslant n}$. Тогда лексикографический порядок на $X = \prod_{i=1}^{n} X_i$ является отношением полного порядка.*

Доказательство. Очевидно проверяется, что $(\mathbb{Z}^+, \leqslant)$ является вполне упорядоченным множеством. Из предыдущей теоремы сразу получаем нужный результат.

■

Упражнения

1. Рассмотрите отношение эквивалентности «быть сравнимыми между собой по $(\mathrm{mod}\ 7)$» на множестве натуральных чисел. Найти формулу, описывающую все элементы класса, содержащего 4.

2. Пусть $\mathbb{Z} = \{(n,m) : n,m \in \mathbb{N}\}$. Определим отношение на этом множестве следующим образом: $(n,m)\rho(k,l) \Leftrightarrow n+l = m+k$. Докажите, что это отношение является отношением эквивалентности. Пусть $(n,m)+(k,l) = (n+k, m+l)$. Докажите, что эта операция не зависит от выбора представителей, т.е. если $(n,m)\rho(n_1,m_1)$ и $(k,l)\rho(k_1,l_1)$, то выполняется $\Big((n,m)+(k,l)\Big)\,\rho\,\Big((n_1,m_1)+(k_1,l_1)\Big)$.

3. Определите на множестве лучей отношение «быть сонаправленными друг с другом». Докажите, что это отношение является отношением эквивалентности.

4. Сколько существует полных порядков на множестве $\mathbb{N}_{\leqslant n}$? Сколько вообще существует порядков на этом множестве?

2.14. Антиномии. Аксиомы теории множеств

При чтении всего предыдущего материала может возникнуть чувство ясного представления, что такое множество. Поэтому необходимо сделать предупреждение: существует прекрасная возможность утратить это чувство, прочитав этот параграф целиком.

В обсуждении самого понятия множества мы недалеко ушли от того значения, которое используется в обычном языке: объекты, являющиеся элементами множества, могут быть любой природы, и правила $P(x)$, по которым элементы объединяются в множество, также могут быть произвольными. Эту ситуацию нельзя считать окончательной ввиду следующих парадоксов.

Парадокс Рассела. Определим K следующим образом: произвольное множество $X \in K \Leftrightarrow X \notin X$. Предположим, что K — множество, тогда можно попытаться выяснить, $K \in K$ или $K \notin K$? Но если $K \in K$, то по определению $K = \{X : X \notin X\} \Rightarrow K \notin K$. $\lightning$. Если $K \notin K$, то снова воспользуемся определением $K = \{X : X \notin X\}$ и получим $K \in K$. $\lightning$.

Парадокс о брадобрее. Пусть B — брадобрей. По определению будем считать, что он должен брить тех и только тех людей, кто не бреет себя сам. Бреет ли он сам себя? Если да, то он не должен этого делать. А если он не бреет себя сам, то он должен себя брить согласно определению.

Лексический парадокс. Будем определять натуральные числа, используя слова русского языка. Сделаем только одно ограничение: в определении мы

не будем использовать больше тринадцати слов. Слов конечное число (ограничиваясь словарем Даля, будем считать, что их не более 200000). Поэтому и количество чисел, которые можно определить таким образом, конечно. В силу полноты порядка на $\mathbb{N}$ существует минимальное из чисел, которое мы не можем определить. Зададим это число следующим образом: «минимальное из натуральных чисел, которые нельзя определить с помощью не более тринадцати слов». Нетрудно убедиться, что в этом определении в точности тринадцать слов.

Парадокс Бурали–Форти[23]. Это самый первый из появившихся парадоксов. Чтобы его сформулировать, понадобится совокупность, очень похожая на K из парадокса Рассела. Пусть K_1 вместе с каждым множеством содержит каждый его элемент. Пусть теперь K_1 является множеством, тогда по теореме Кантора $|K_1| < |\mathcal{P}(K_1)|$, но по определению K_1 множество $\mathcal{P}(K_1) \subseteq K_1 \Rightarrow |\mathcal{P}(K_1)| \leqslant |K_1|$. $\lightning$.

Чтобы избежать парадоксов, необходимо наложить некоторые ограничения на то, из каких элементов состоит множество и с помощью каких правил оно строится. Было бы логично потребовать, чтобы множество собиралось из элементов, которые уже существуют. Так, например, при построении множества нельзя использовать в качестве его элемента само это множество. Таким образом, мы приходим к очень естественной идее: множество, кроме того, что оно является некоторой совокупностью, является одновременно и неким процессом собирания ранее построенных элементов.

Итак, каждое множество должно строиться на некотором шаге $\mathbf{s}$. Этот шаг должен иметь предшествующие шаги, на которых должны быть построены все элементы этого множества. Каждый шаг имеет последующий, что позволяет образовывать всё новые и новые множества. Более того, каждое множество шагов также имеет последующий, но вся совокупность шагов (которая множеством не является) не имеет последующего, иначе легко было бы получить парадокс, похожий на парадокс Бурали–Форти.

Система аксиом позволяет избежать парадоксов при переходе от одного множества к другому. Фактически она описывает естественные способы получения одних множеств из других и позволяет безопасно путешествовать от одного шага к другому. Так, в частности, все рассмотренные нами ранее

[23] Чезаре Бурали-Форти (1861–1931) — итальянский математик, основные работы относятся к теории векторов; разработал векторное исчисление и применил его к задачам проективной геометрии, дифференциальной геометрии, механики, оптики и гидродинамики; совместно с Пеано работал на основаниями математики.

операции над множествами будут приводить к образованию новых множеств.

Договоримся, что предикатом, или высказывательной функцией, будем называть отображение $P(x)$, которое ставит в соответствие элементам или множествам одно из двух значений — истина или ложь. Если этот предикат задан на некотором множестве, то мы будем говорить, что он ограничен (так, например, предикат $P(x) =$ «$x \leqslant 0$», заданный на множестве $\mathbb{R}$, ограничен; легко видеть, что $P(1) = \text{Л}$ и $P(-1) = \text{И}$).

Следующая аксиоматическая система была впервые предложена Цермело[24] и усовершенствована Френкелем[25] (им добавлена аксиома выделения). Напоминаем, что символы A, B, X, Y мы используем только для обозначения множеств.

Первая аксиома закрепляет то положение, что множество полностью определяется своими элементами.

Аксиома объемности. Если $\forall x(x \in A \Leftrightarrow x \in B)$, то $A = B$.

Следующая аксиома гарантирует, что для двух множеств A, B существует их множество-пара, т. е. множество $\{A, B\}$, единственными элементами которого являются именно эти два множества.

Аксиома пары. $\forall A \forall B \exists X(Y \in X \Leftrightarrow Y = A \vee Y = B)$.

Если элементы множества A сами являются множествами, то можно рассмотреть объединение всех этих элементов. Третья аксиома говорит о том, что это объединение также является множеством.

Аксиома объединения. $\forall A \exists X(Y \in X \Leftrightarrow \exists B \in A : Y \in B)$.

Взятие множества всех подмножеств множества A также приводит к образованию множеств. Об этом следующая аксиома.

Аксиома степени. $\forall A \exists X(Y \in X \Leftrightarrow Y \subseteq A)$.

Если каждое множество, на котором некоторый предикат принимает истинные значения, является элементом некоторого большего множества, то из них можно образовать новую совокупность, которая будет множеством.

Аксиома выделения. Для каждого множества A и предиката $P(a)$ справедливо следующее. Если $(P(a) = \text{И} \Rightarrow a \in A) \Rightarrow \exists X : X = \{a : P(a)\}$.

[24]Эрнст Цермело (1871–1953) — немецкий математик, основные исследования относятся к теории множеств, разработал ее общую аксиоматику и доказал, что всякое множество может быть вполне упорядочено; при доказательстве использовал аксиому выбора (аксиома Цермело).

[25]Абрахам Френкель (1891–1965) — израильский математик, один из авторов аксиоматической теории множеств; первый декан математического факультета, а впоследствии ректор Еврейского университета в Иерусалиме, лауреат Премии Израиля в области точных наук.

Без следующей аксиомы наш мир мог бы состоять только из конечных множеств. Богатство разнообразных по мощности множеств достигается путем введения всего лишь одного бесконечного множества, содержащего $\varnothing$ и вместе с каждым элементом A множество $\{A\}$.

Аксиома бесконечности. $\exists X(Y \in X \Leftrightarrow Y = \varnothing \vee \exists A \in X : Y = \{A\})$.

Если задано некоторое отображение F на множестве A, которое каждому элементу a этого множества ставит в соответствие некоторое множество $Y = F(a)$, то совокупность, состоящая из образов и только из них, также является множеством. Об этом аксиома подстановки.

Аксиома подстановки. Для каждого множества A и отображения F справедливо следующее. $\exists X(Y \in X \Leftrightarrow Y = F(a)$ при некотором $a \in A)$.

При обсуждении понятия множества мы заметили, что его элементы должны строиться на предыдущих шагах. Каждый из этих элементов, сам будучи множеством, строится из элементов, образованных еще на более ранних шагах, и т.д. Чтобы этот процесс не был бесконечным вниз по «лестнице» шагов, вводится следующая и последняя аксиома. Она гарантирует существование минимального элемента. При этом минимальным элементом в непустом множестве A называют такой элемент $B \in A$, что B и A не имеют общих элементов. Это означает, что при построении A не используется ни один из элементов множества B.

Аксиома регулярности. $\forall A(A \neq \varnothing) \Rightarrow (\exists B \in A : \forall X \in B \Rightarrow X \notin A)$.

Довольно часто к системе аксиом Цермело-Френкеля (ZF) добавляют аксиому выбора, которую можно сформулировать следующим образом.

Аксиома выбора. Пусть $\mathcal{F} = \{A_i : i \in I\}$ семейство попарно непересекающихся непустых множеств ($\mathcal{F}$ — это множество, состоящее из множеств). Тогда найдется множество $C = \{x_i : i \in I\}$, содержащее ровно по одному элементу из каждого множества $A_i \in \mathcal{F}$.

Первая строгая формулировка этой аксиомы принадлежит Цермело, хотя ее еще раньше Кантор применял без явного упоминания. Систему аксиом Цермело-Френкеля с добавленной аксиомой выбора принято обозначать ZFC. В 1904 году Цермело в ZFC доказал, что любое множество можно вполне упорядочить (т. е. ввести на нем полный порядок), это позволило вполне упорядочить все кардинальные числа (используемые для обозначения мощности множеств). Кстати, доказательство того, что счетное объединение счетных множеств счетно, также использует аксиому выбора и без нее доказать этот факт невозможно.

2.15. Некоторые проблемы теории множеств

В 1900 году, с 6 по 12 августа, в Париже состоялся Второй Международный конгресс математиков. Главным событием этого Конгресса стал программный доклад Давида Гильберта, сделанный 8 августа. Доклад носил скромное название «Математические проблемы», но в нем Гильберт перечислил важнейшие, по его мнению, проблемы математики. Математический мир принял этот вызов, и в течение века большинство проблем были так или иначе решены. Этот список состоял из 23 проблем (в первоначальной версии — из 24) и первой из них была континуум-гипотеза. Мы уже знаем, что в ZFC (т. е. в системе аксиом теории множеств Цермело-Френкеля с аксиомой выбора) можно вполне упорядочить все кардинальные числа, поэтому существует минимальное кардинальное число (обозначается $\aleph_1$), которое больше $\aleph_0$.

Первая проблема Гильберта, (*континуум-гипотеза*, CH): $\aleph_1 = \mathfrak{c}$.

Предположение о том, что любое бесконечное подмножество $\mathbb{R}$ счетно или континуально (т. е. нет подмножеств промежуточной мощности), выдвинул в 1877 году Георг Кантор.

Интересно, что CH равносильна каждой из следующих проблем:

1) прямая $\mathbb{R}$ может быть раскрашена в счетное количество цветов так, что ни для какой одноцветной четверки чисел $a, b, c, d \in \mathbb{R}$ не выполняется условие $a + b = c + d$.

2) пространство $\mathbb{R}^3$ можно разбить на три множества так, что они пересекаются с любой прямой, параллельной осям Ox, Oy или Oz, лишь в конечном числе точек.

Первые попытки доказать CH в рамках ZFC были неудачны. Решить эту проблему смог П. Коэн[26] только в 1963 году. С помощью разработанного им *метода форсинга* Коэн доказал, что CH не зависит от аксиом ZFC (это означает, что доказать CH или ее отрицание средствами ZFC невозможно).

Следующий список задач по теории множеств возник благодаря Михаилу Патракееву[27]. Решение этих проблем позволит пытливому школьнику существенно расширить свои математические горизонты.

Пусть $\mathbb{N}$ — натуральный ряд и $\mathcal{A}$ — некоторое семейство его подмножеств.

[26]Пол Коэн (1934-2007) — американский математик, лауреат самой престижной математической награды — медали Филдса — за изучение логики (1966).

[27]Михаил Патракеев (р. в 1979) — талантливый выпускник СУНЦ УрГУ (1996), канд.физ.-мат.н., старший научный сотрудник ИММ УрО РАН; основные направления исследований: общая топология, теория множеств, математический анализ, геометрия.

1. Если $\mathcal{A}$ состоит лишь из конечных множеств, то оно не более чем счетно.

2. Найдите не более чем счетное подсемейство $\mathcal{B} \subseteq \mathcal{A}$ такое, что одновременно выполняется: $\bigcup \mathcal{B} = \bigcup \mathcal{A}$ и $\bigcap \mathcal{B} = \bigcap \mathcal{A}$.

3. Мощности попарных пересечений элементов $\mathcal{A}$ ограничены числом 2012. Покажите, что $\mathcal{A}$ не более чем счетно.

4. Семейство называется *почти дизъюнктным* (ПД), если любые два различных его элемента пересекаются по конечному множеству. Покажите, что если $\mathcal{A}$ счетно и ПД, то найдется $D \subseteq \mathbb{N}$, $D \notin \mathcal{A}$ такое, что $\mathcal{A} \cup \{D\}$ — ПД.

5 ***.** Постройте континуальное ПД семейство подмножеств в $\mathbb{N}$.

6 ****.** Найдите континуальное ПД семейство $\mathcal{B}$ подмножеств в $\mathbb{N}$, каждый элемент $D \in \mathcal{B}$ которого имеет верхнюю плотность 1, т. е. для любого $m \in \mathbb{N}$ существует $k > m$, что

$$\frac{|D \cap \{1, \ldots, k\}|}{k} > 1 - \frac{1}{m}.$$

7 ****.** Отыщите несчетное семейство $\mathcal{B}$ подмножеств в $\mathbb{N}$ такое, что для любых различных $X, Y, Z \in \mathcal{B}$ выполняется: $X \cap Y$ бесконечно, а $X \cap Y \cap Z$ конечно.

8 ***.** Придумайте несчетное семейство $\mathcal{B}$ подмножеств в $\mathbb{N}$ такое, что для любых $X, Y \in \mathcal{B}$ или $X \subseteq Y$, или $Y \subseteq X$.

9 ****.** Сконструируйте два семейства $\{A_x\}_{x\in\mathbb{R}}$, $\{B_x\}_{x\in\mathbb{R}}$ подмножеств в $\mathbb{N}$ такие, что для любых различных $x, y \in \mathbb{R}$ выполняется: $A_x \cap B_x = \varnothing$ и $|A_x \cap B_y| = \aleph_0$.

10. Известно, что $\mathcal{A}$ счетно и ПД, и $\mathcal{B} \subseteq \mathcal{A}$. Постройте такое $D \subseteq \mathbb{N}$, что для каждого $X \in \mathcal{B}$ множество $X \cap D$ конечно и для каждого $Y \in \mathcal{A} \setminus \mathcal{B}$ множество $Y \setminus D$ конечно.

11 *****.** Докажите, что если в задаче 10 условие счетности семейств $\mathcal{A}$ и $\mathcal{B}$ заменить на условие $|\mathcal{A}| = |\mathcal{B} \setminus \mathcal{A}| = \aleph_1$, то такого множества D может не найтись.

Глава 3

Функции. Многочлены одной и нескольких переменных

3.1. Числовые функции

Напомним, что для любого соответствия $\varphi \subseteq A \times B$ (чаще всего будем использовать обозначение $\varphi : A \to B$) определяются три множества: область определения ($D(\varphi) = \{a \in A :$ существует элемент $b \in B$, что $(a, b) \in \varphi\}$), множество значений ($E(\varphi) = \{b \in B :$ существует такой $a \in A$, что $(a, b) \in \varphi\}$) и обратное соответствие ($\varphi^{-1} = \{(b, a) : (a, b) \in \varphi\}$). Кроме того, для двух соответствий $\varphi : A \to B$ и $\psi : B \to C$ задана их композиция ($\chi = \psi \circ \varphi : A \to C$) следующим образом: $\chi = \{(a, c) :$ существует такой элемент $b \in B$, что $(a, b) \in \varphi$ и $(b, c) \in \psi\}$. Отображения, функции и числовые функции являются частными случаями соответствий. Чаще всего для обозначения отображений используют латинские буквы ($f, g, h, \dots$) вместо греческих.

Определение. *Отображением f между множествами A и B называется всюду определенное и однозначное соответствие $f : A \to B$ (т. е. $D(f) = A$, и для любых пар (a, b), $(a, b_1) \in f$ следует, что $b = b_1$).*

Для отображений вместо $(a, b) \in f$ принято записывать $b = f(a)$ (благодаря тому, что второй элемент пары определяется однозначно; для многозначного соответствия φ может выполняться $(a, b), (a, b_1) \in \varphi$ при разных b и b_1, поэтому не ясно, какой из элементов обозначает $\varphi(a)$). Композиция отображений $f : A \to B$ и $g : B \to C$ описывается много проще: для каждого $a \in A$ выполняется $(g \circ f)(a) = g\Big(f(a)\Big)$.

Определение. *Функцией называют отображение $f : A \to \mathbb{R}$ в действительную прямую. Если $A \subseteq \mathbb{R}$, то f называют числовой функцией.*

Договоримся, что в этой главе под термином «функция» будем понимать «числовую функцию» . *Графиком* функции f называется множество $\Gamma(f) = \left\{\Big(x, f(x)\Big) : x \in D(f)\right\} \subseteq \mathbb{R}^2$. С точки зрения теории множеств, функция и ее график — это одно и то же (множество упорядоченных пар). Рассмотрим несколько примеров функций.

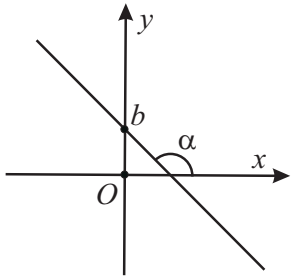

Рис. 21

П р и м е р 1. Линейная функция задается формулой $f(x) = kx + b$, $D(f) = \mathbb{R}$, $\Gamma(f)$ — прямая. Множество значений функции зависит от k : $E(f) = \mathbb{R}$ при $k \neq 0$ и $E(f) = \{b\}$ при $k = 0$. Смысл коэффициентов k и b следующий: $k = \operatorname{tg}\alpha$, где α — угол наклона $\Gamma(f)$ к положительному направлению оси Ox , а b задает смещение $\Gamma(f)$ относительно начала координат вдоль оси Oy (проще говоря, $b = f(0)$). При $k = 0$ прямая $\Gamma(f)$ параллельна оси Ox . На рис. 21 построен график линейной функции при $k < 0$, $b > 0$.

П р и м е р 2. Формула $f(x) = ax^2+bx+c$ при $a \neq 0$ задает квадратичную функцию. $D(f) = \mathbb{R}$, $\Gamma(f)$ — парабола. Знак коэффициента a , как известно, указывает на направление ветвей параболы, $c = f(0)$ — ордината точки пересечения параболы с осью Oy . С осью абсцисс $\Gamma(f)$ пересекается только при условии $D = b^2 - 4ac \geqslant 0$ в точках $x_{1,2} = (-b \pm \sqrt{D})/(2a)$. Вершина параболы имеет координаты (x_0, y_0) , где $x_0 = -b/(2a)$, а $y_0 = -D/(4a)$. Множество значений $f(x)$ зависит от знака a : $E(f) = [y_0; \infty)$ при $a > 0$ и $E(f) = (-\infty; y_0]$ при $a < 0$. На рис. 22 изображен график квадратичной функции при $a > 0$, $c > 0$, $b < 0$.

П р и м е р 3. Областью определения квадратного корня, т. е. функции $f(x) = \sqrt{x}$, является $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geqslant 0\}$, $E(f) = \mathbb{R}^+$, $\Gamma(f)$ может быть получен симметрией относительно прямой $y = x$ из графика функции $y = x^2$, рассмотренной только на множестве $\mathbb{R}^+$. График $f(x) = \sqrt{x}$ изображен на рис. 23.

П р и м е р 4. Функция обратной пропорциональной зависимости задается формулой $f(x) = k/x$, где $k \neq 0$. $D(f) = \{x \in \mathbb{R} : x \neq 0\}$, $E(f) = \{y \in \mathbb{R} : y \neq 0\}$, $\Gamma(f)$ — гипербола, расположенная в первом и третьем координатных углах при $k > 0$, и во втором и четвертом — при $k < 0$. На рис. 24 как раз изображен последний случай.

П р и м е р 5. Функция абсолютной величины, или модуля, определяет-

ся следующим образом: $f(x) = |x| = \begin{cases} x, & \text{если } x \geqslant 0, \\ -x, & \text{если } x < 0. \end{cases}$ Из определения немедленно следует неравенство $|x| \geqslant 0$ при всех $x \in \mathbb{R}$. $D(f) = \mathbb{R}$, $E(f) = \mathbb{R}^+$, график абсолютной величины изображен на рис. 25. Геометрическое свойство модуля: $|x|$ — это расстояние на числовой прямой от x до 0.

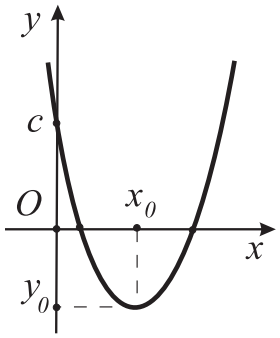

Рис. 22

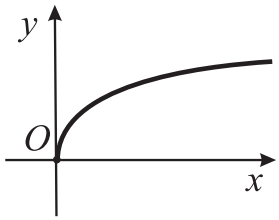

Рис. 23

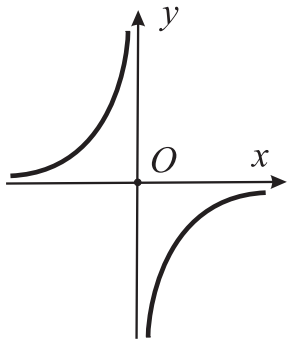

Рис. 24

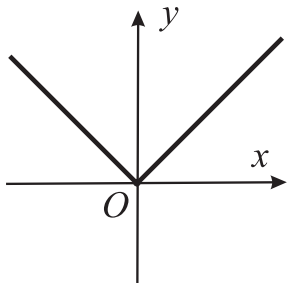

Рис. 25

П р и м е р 6. Функция целой части $f(x) = [x]$ определяется для любого $x \in \mathbb{R}$ как наибольшее целое число, не превосходящее x, т.е. $[x] = k$, $k \in \mathbb{Z} \Leftrightarrow k \leqslant x < k + 1$. Если модуль определяется двумя условиями, то для целой части необходим счетный набор условий. $D(f) = \mathbb{R}$, $E(f) = \mathbb{Z}$, $\Gamma(f)$ изображен на рис. 26.

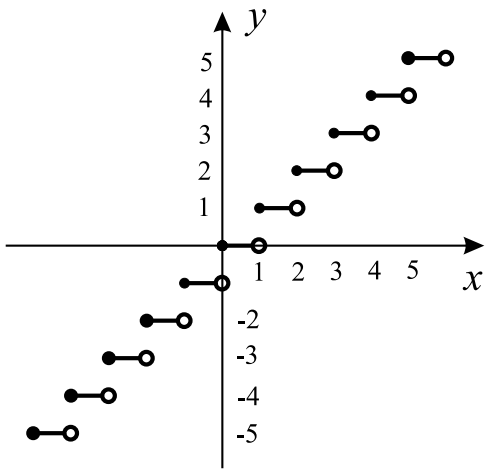

Рис. 26

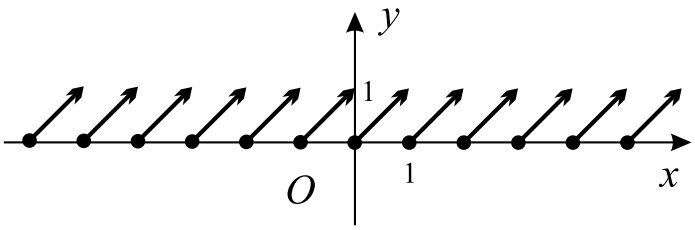

Рис. 27

П р и м е р 7. Функция целой дробной части произвольного действительного числа $f(x) = \{x\}$ определяется формулой $\{x\} = x - [x] = x - k$, где $k \in \mathbb{Z}$, и верно двойное неравенство $k \leqslant x < k + 1$. Например, для $x \in [-2; -1) \Rightarrow \{x\} = x + 2$; для $x \in [-1; 0) \Rightarrow \{x\} = x + 1$; при

$x \in [0;1) \Rightarrow \{x\} = x$ и т. д. Видим, что определение дробной части числа также содержит счетное количество условий. $D(f) = \mathbb{R}$, $E(f) = [0;1)$, $\Gamma(f)$ изображен на рис. 27.

Пример 8. Функция Дирихле $f(x) = \begin{cases} 1, & \text{если } x \in \mathbb{Q}, \\ 0, & \text{если } x \in \mathbb{R}\backslash\mathbb{Q}. \end{cases}$ $D(f) = \mathbb{R}$, $E(f) = \{0,1\}$, $\Gamma(f)$ нам не удалось нарисовать — эта функция разрывна в каждой точке области определения.

Определение. *Пусть заданы функции* $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$. *Суммой (разностью, произведением)* f *и* g *называется такая функция* h, *что* $D(h) = A \cap B$ *и для всех* $x \in D(h)$ *выполняется* $(f+g)(x) = f(x) + g(x)$ ($(f-g)(x) = f(x) - g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$). *Частным* f *и* g *называется такая функция* h, *что* $D(h) = (A \cap B)\backslash\{x \in B : g(x) = 0\}$ *и для всех* $x \in D(h)$ *выполняется* $\dfrac{f}{g}(x) = \dfrac{f(x)}{g(x)}$.

Определение. *Пусть заданы функции* $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$ *и* $E(f) = f(A) \subseteq B$. *Композицией* f *и* g *называется такая функция* $h = g \circ f$, *что* $D(h) = A$ *и для всех* $x \in D(h)$ *выполняется* $(g \circ f)(x) = g\Big(f(x)\Big)$.

Пример 9. Пусть $f(x) = x + 1$ и $g(x) = x^2$ для всех $x \in \mathbb{R}$. Тогда $(g \circ f)(x) = g(x+1) = (x+1)^2$, но $(f \circ g)(x) = f(x^2) = x^2 + 1$. Из этого примера видно, что композиция функций не коммутативна.

Существует несколько способов задания функций.

I. *Формулой.* Задание функции с помощью формулы, т. е. с помощью некоторого алгебраического выражения, является основным способом задания. По умолчанию, областью определения такой функции считают максимальное по включению множество, на котором определены участвующие в этой формуле объекты (такая область определения называется «естественной» областью определения). Так, для функции $f_1(x) = (x-2)/\sqrt{x+1}$ будет выполняться $D(f_1) = (-1;\infty)$, а для $f_2 = \sqrt{x+1}/(x-2)$ — $D(f_2) = [-1;2) \cup (2;\infty)$. Причем область определения может быть разбита на несколько подмножеств, на каждом из которых действует своя формула. Выше приведены примеры именно на такой способ задания функции.

II. *Таблицей.* Если $D(f) = \{x_1, x_2, \ldots, x_n\}$ — некоторое конечное множество, содержащее небольшое количество элементов, то для каждого из них можно указать соответствующее значение y_i и множество пар, задающих f оформить в виде таблицы:

Значение аргумента x:	x_1	x_2	x_3	$\ldots$	x_n
Значение функции $f(x)$:	y_1	y_2	y_3	$\ldots$	y_n

Результаты экспериментов во многих прикладных науках оформляются именно в виде таблиц.

III. *Графиком.* Если числовых данных в ходе эксперимента или наблюдения слишком много, то их представляют не в виде таблицы, а в виде некоторых линий на плоскости или фигур (фигурой называют произвольное подмножество плоскости). Рассмотрим некоторое множество Φ на координатной плоскости $\mathbb{R}^2$. Ясно, что эта фигура всегда задает соответствие между $D(\Phi)$ и $E(\Phi)$, но когда Φ задает функцию?

Теорема 1.1. *Пусть $\Phi \subseteq \mathbb{R}^2$. Φ является графиком некоторой функции тогда и только тогда, когда любая прямая, параллельная оси Oy, пересекает Φ не более, чем в одной точке.*

Доказательство. $\Rightarrow$) о/п: пусть $\Phi = \Gamma(f)$ для некоторой функции f, но на прямой $x = x_0$ нашлись по крайней мере две различные точки (x_0, y_0) и (x_0, y_1), принадлежащие Φ. Тогда $f(x_0) = y_0$ и $f(x_0) = y_1$, что противоречит однозначности f.

$\Leftarrow$) обозначим через $A = \{x_0 \in \mathbb{R} :$ прямая $x = x_0$ пересекается с $\Phi\}$. Для любого x_0 существует единственная точка (x_0, y_0) из пересечения прямой $x = x_0$ с фигурой Φ. По определению будем считать, что $f(x_0) = y_0$. Тогда f всюду определено на A и однозначно, следовательно, является функцией. Нетрудно заметить, что $\Gamma(f) = \Phi$.

■

3.2. Свойства функций

Существует более континуума различных функций. Среди них выделяют классы «хороших» функций. Некоторые из этих классов изучаются в этом параграфе.

I. *Четные и нечетные функции.*

Определение. *Функция $f : A \to \mathbb{R}$ называется четной (соответственно нечетной), если*

а) $\forall x \in A \Rightarrow -x \in A$;

б) $\forall x \in A \Rightarrow f(-x) = f(x)$ $(\, f(-x) = -f(x)\,)$.

Если функция не является ни четной, ни нечетной, то она называется функцией общего вида.

П р и м е р 1. Функции $f_1(x) = |x|$, $f_{2n}(x) = x^{2n}$ при $n \in \mathbb{N}$, функция Дирихле — все являются четными. Функции $f_{2n-1} = x^{2n-1}$ при $n \in \mathbb{N}$, $g(x) = k/x$ нечетны. Целая часть числа является функцией общего вида, поскольку $[1/2] = 0$, а $[-1/2] = -1$.

Теорема 2.1. *Пусть* $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$. *Выполняются следующие свойства:*

1) если f *и* g *— четные функции, то* $f+g$, $f \cdot g$ *и* f/g *четны;*

2) если f *и* g *— нечетные функции, то* $f+g$ *— нечетная, а* $f \cdot g$ *и* f/g *— четные;*

3) если f *— четная функция, а* g *— нечетная функции, то* $f \cdot g$ *и* f/g *— нечетные;*

4) если $f(A) \subseteq B$ *и* f *— четная, то* $g \circ f$ *также четна;*

5) если $f(A) \subseteq B$ *и* f, g *— нечетны, то* $g \circ f$ *также является нечетной функцией;*

6) f *— четная* $\Leftrightarrow$ $\Gamma(f)$ *симметричен относительно оси* Oy;

7) f *— нечетная* $\Leftrightarrow$ $\Gamma(f)$ *симметричен относительно точки* O.

Доказательство. 1) для множества $C = A \cap B$ свойство (а) определения выполняется, поскольку

$$\forall x \in C \Leftrightarrow (x \in A \,\&\, x \in B) \Rightarrow (-x \in A \,\&\, -x \in B) \Rightarrow -x \in C.$$

Теперь используем определение $f+g$ и (б) для f и g:

$$(f+g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f+g)(x).$$

Свойства (а) и (б) проверены, поэтому $f+g$ — четная функция. Аналогично доказывается четность $f \cdot g$ и f/g.

2) свойство (а) проверяется аналогично предыдущему пункту. Нечетность $f+g$ следует из $(f+g)(-x) = f(-x)+g(-x) = -f(x)-g(x) = -(f+g)(x)$.

Четность произведения следует из $(f \cdot g)(-x) = f(-x) \cdot g(-x) = \Big(-f(x)\Big) \cdot \Big(-g(x)\Big) = f(x) \cdot g(x) = (f \cdot g)(x)$. Аналогично доказывается четность f/g.

3) свойство (а) проверяется аналогично предыдущему пункту. Проверим (б). Для любого $x \in A \cap B \Rightarrow f(-x) \cdot g(-x) = f(x) \cdot \Big(-g(x)\Big) = -\Big(f(x) \cdot g(x)\Big)$.

4) из $D(h) = A$ сразу следует выполнение (а). Второе свойство определения следует из $\forall x \in A \Rightarrow (g \circ f)(-x) = g\Big(f(-x)\Big) = g\Big(f(x)\Big) = (g \circ f)(x)$.

5) свойство (а) доказывается аналогично (4), проверим (б): $\forall x \in A \Rightarrow (g \circ f)(-x) = g\Big(f(-x)\Big) = g\Big(-f(x)\Big) = -g\Big(f(x)\Big) = -(g \circ f)(x)$.

6) заметим что при симметрии относительно Oy выполняется равенство $S_{(Oy)}\Big((x_0, y_0)\Big) = (-x_0, y_0)$. Теперь воспользуемся определением:

$$f(x) \text{ — четная } \Leftrightarrow \begin{cases} \forall x \in A \Leftrightarrow -x \in A, \\ \forall x \in A \Rightarrow f(-x) = f(x). \end{cases}$$

Или для любой точки графика выполняется

$$\Big(x, f(x)\Big) \in \Gamma(f) \Leftrightarrow \Big(-x, f(x)\Big) \in \Gamma(f) \Leftrightarrow S_{(Oy)}\Big((x, f(x))\Big) \in \Gamma(f).$$

Это означает, что $\Gamma(f)$ отображается на себя при $S_{(Oy)}$.

7) проверяется аналогично (5) с той лишь разницей, что при центральной симметрии относительно начала координат верно $Z_O\Big((x_0, y_0)\Big) = (-x_0, -y_0)$. ■

II. *Периодические функции.*

Определение. *Пусть $T \in \mathbb{R}$ и $T \neq 0$. Число T называется периодом функции $f : A \to \mathbb{R}$, если*

а) $\forall x \in A \Rightarrow \ x + T,\ x - T \in A$;

б) $\forall x \in A \Rightarrow f(x + T) = f(x)$.

Если у функции есть хотя бы один период, она называется периодической.

П р и м е р 2. Функция дробной части $f(x) = \{x\}$ периодическая с периодом $T = 1$. Для функции Дирихле любое ненулевое рациональное число является ее периодом. Линейная функция $f(x) = kx + b$ является периодической только в случае, когда $k = 0$, и в этом случае ее периодом будет любое ненулевое число.

Теорема 2.2. *Пусть $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$. Выполняются следующие свойства:*

1) если T — общий период f и g, то он является периодом для $f + g$, $f \cdot g$ и f/g;

2) если $f(A) \subseteq B$ и T — период f, то $g \circ f$ также периодическая с периодом T;

3) если T — период f, то $(-T)$ также является периодом f;

4) если T — период f, то для любого $n \in \mathbb{N}$ число $n \cdot T$ также является периодом f;

5) если T *— период* f*, то для любого* $k \in (\mathbb{Z}\backslash\{0\})$ *число* $k \cdot T$ *также является периодом* f*;*

6) f *— периодическая с периодом* $T \Leftrightarrow \Gamma(f)$ *отображается сам на себя при параллельном переносе на вектор* $\overrightarrow{v} = (T, 0)$*.*

Доказательство. 1) выполнение (а) и (б) для $f+g$, $f \cdot g$ и f/g очевидно.

2) так как $D(g \circ f) = A = D(f)$, то выполнение (а) очевидно, проверим только (б):

$$\forall x \in A \Rightarrow (g \circ f)(x+T) = g\Big(f(x+T)\Big) = g\Big(f(x)\Big) = (g \circ f)(x).$$

3) условие (а) можно переписать в виде $x-(-T)$, $x+(-T) \in A$, поэтому $(-T)$ удовлетворяет (а). Используя то, что T — период f, получим

$$\forall x \in A \Rightarrow f(x-T) = f(x-T+T) = f(x),$$

поэтому (б) для числа $(-T)$ также выполняется.

4) докажем индукцией по n. Б.И. При $n = 1$ утверждение очевидно выполняется.

Ш.И. Предположим, что для n утверждение верно и докажем его для $n+1$.

а) по предположению $\forall x \in A \Rightarrow x \pm nT \in A$. Применяя базу, получим $x + nT + T$ и $x - nT - T \in A$, что доказывает (а) для числа $(n+1)T$.

б) рассмотрим произвольный $x \in A$ и последовательно применим базу и предположение индукции:

$$f\Big(x + (n+1)T\Big) = f\Big((x+nT) + T\Big) = f(x+nT) = f(x).$$

Шаг доказан.

5) следует из (4) и (3).

6) обозначим через $\mathfrak{T}_{\overrightarrow{v}}$ параллельный перенос на вектор $\overrightarrow{v} = (T, 0)$ и заметим, что для любой точки (x_0, y_0) координаты ее образа при этом параллельном переносе находятся так: $\mathfrak{T}_{\overrightarrow{v}}\Big((x_0, y_0)\Big) = (x_0+T, y_0)$. А теперь воспользуемся определением периода и получим, что точки $B(x-T, f(x))$, $C(x, f(x))$ и $D(x+T, f(x))$ лежат на графике функции f. Кроме того, $\mathfrak{T}_{\overrightarrow{v}}(B) = C$ и $\mathfrak{T}_{\overrightarrow{v}}(C) = D$. Делаем вывод, что любая точка графика $\Gamma(f)$ переходит в некоторую другую точку графика $\Gamma(f)$ и сама является образом некоторой третьей точки графика $\Gamma(f)$. Отсюда $\mathfrak{T}_{\overrightarrow{v}}(\Gamma(f)) = \Gamma(f)$.

■

Определение. *Если T^* — минимальный из положительных периодов функции $f(x)$, то он называется основным периодом.*

Пример 3. У функции дробной части $f(x) = \{x\}$ число $T = 1$ — основной период. Функция Дирихле, как и $f(x) = b$ при всех $x \in \mathbb{R}$, основного периода не имеют.

III. *Ограниченные функции.*

Определение. *Пусть $f : A \to \mathbb{R}$ и $A_1 \subseteq A$. Функция $f(x)$ называется ограниченной сверху (соответственно снизу) на A_1, если найдется такое число $M \in \mathbb{R}$ ($m \in \mathbb{R}$), что $\forall x \in A_1 \Rightarrow f(x) \leqslant M$ ($m \leqslant f(x)$). При этом число M (m) называется верхней (нижней) границей f. Если f одновременно ограничена и сверху и снизу на A_1, то она называется ограниченной на множестве A_1. Если не уточняют, о каком множестве A_1 идет речь, считают, что $A_1 = A$.*

Пример 4. Функция $f(x) = \sqrt{x}$ ограничена только снизу (например, числом $m = -3$). Дробная часть числа и функция Дирихле являются ограниченными, для них можно выбрать $m = 0$ и $M = 1$. Функция $f(x) = 1/x$ не ограничена ни сверху, ни снизу; но ограничена на отрезке $A_1 = [1; 2070]$.

IV. *Монотонные и строго монотонные функции.*

Определение. *Пусть $f : A \to \mathbb{R}$ и $A_1 \subseteq A$. Функция $f(x)$ называется возрастающей (соответственно строго возрастающей, убывающей, строго убывающей) на A_1 (обозначения: $f \nearrow_{A_1}$, $f \nearrow\!\!\nearrow_{A_1}$, $f \searrow_{A_1}$, $f \searrow\!\!\searrow_{A_1}$), если $\forall x_1, x_2 \in A_1$ и таких, что $x_1 < x_2 \Rightarrow f(x_1) \leqslant f(x_2)$ ($f(x_1) < f(x_2)$, $f(x_1) \geqslant f(x_2)$, $f(x_1) > f(x_2)$). Если $f \nearrow_{A_1}$ или $f \searrow_{A_1}$, то f называют монотонной на A_1; если же $f \nearrow\!\!\nearrow_{A_1}$ или $f \searrow\!\!\searrow_{A_1}$, то f называют строго монотонной на A_1. Если не уточняют, о каком множестве A_1 идет речь, считают, что $A_1 = A$.*

Пример 5. Функция $f(x) = 1/x$ не является строго монотонной, хотя строго убывает на каждом из промежутков: $(-\infty; 0)$, $(0; \infty)$. Будьте осторожны: на каждом из этих промежутков определение строго убывающей функции выполняется, а на их объединении $(-\infty; 0) \cup (0; \infty)$ — нет.

Теорема 2.3. *Пусть $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$. Выполняются следующие свойства:*

1) если f и g монотонны с одинаковым характером монотонности, то $f+g$ имеет тот же характер монотонности; если при этом хотя бы одна

из функций (f или g) строго монотонна, то $f+g$ — строго монотонная функция;

2) если f и g положительны на $A\cap B$ и возрастают (строго возрастают), то и $f\cdot g$ возрастает (строго возрастает);

3) пусть $f(A)\subseteq B$, $h=g\circ f$ и f и g монотонны (строго монотонны) с одинаковым характером монотонности, то h является возрастающей (строго возрастающей);

4) пусть $f(A)\subseteq B$, $h=g\circ f$ и f и g монотонны (строго монотонны) с разным характером монотонности, то h является убывающей (строго убывающей).

Доказательство. 1) выберем произвольные $x_1, x_2 \in A\cap B = C$ (только на пересечении задана сумма функций) и будем считать, что $x_1 < x_2$. Если $f\nearrow\!\!\!\nearrow_C$ и $g\nearrow_C$, то имеем по определению два неравенства $f(x_1) < f(x_2)$ и $g(x_1)\leqslant g(x_2)$, сложив которые, получим $f(x_1)+g(x_1) < f(x_2)+g(x_2)$. Остальные случаи доказываются аналогично.

2) выберем произвольные $x_1, x_2 \in A\cap B = C$ и будем считать, что $x_1 < x_2$. Если $f\nearrow\!\!\!\nearrow_C$ и $g\nearrow\!\!\!\nearrow_C$, то имеем по определению два двойных неравенства $0 < f(x_1) < f(x_2)$ и $0 < g(x_1) < g(x_2)$. Первое из неравенств умножим с сохранением знака на положительное число $g(x_1)$, а второе — на положительное число $f(x_2)$ и получим $f(x_1)\cdot g(x_1) < f(x_2)\cdot g(x_1)$ и $f(x_2)\cdot g(x_1) < f(x_2)\cdot g(x_2)$. Из транзитивности получается нужное неравенство $f(x_1)\cdot g(x_1) < f(x_2)\cdot g(x_2)$. Остальные случаи доказываются аналогично.

3) пусть $f\nearrow\!\!\!\nearrow$, $g\nearrow\!\!\!\nearrow$, $x_1, x_2 \in A$ и $x_1 < x_2$. Первое условие дает нам $f(x_1) < f(x_2)$, а второе — $g\Big(f(x_1)\Big) < g\Big(f(x_2)\Big)$. Если же $f\searrow\!\!\!\searrow$, $g\searrow\!\!\!\searrow$, то сначала получим $f(x_1) > f(x_2)$, а затем — $g\Big(f(x_1)\Big) < g\Big(f(x_2)\Big)$. В результате, $h\nearrow\!\!\!\nearrow$. Остальные случаи доказываются аналогично.

4) пусть $f\nearrow\!\!\!\nearrow$, $g\searrow\!\!\!\searrow$, $x_1, x_2 \in A$ и $x_1 < x_2$. Первое условие дает нам $f(x_1) < f(x_2)$, а второе — $g\Big(f(x_1)\Big) > g\Big(f(x_2)\Big)$. В результате, $h\searrow\!\!\!\searrow$. Остальные случаи доказываются аналогично.

■

Определение. *Пусть $f : A\to\mathbb{R}$ и $f(A)=B$. Функция $g : B\to\mathbb{R}$ называется обратной к f, если $\forall x\in A \Rightarrow g\Big(f(x)\Big) = x$. Если для f существует обратная, то f называется обратимой функцией, а функция g обозначается через f^{-1}.*

Сразу выясним, как понятие обратной функции связано с понятием об-

ратного соответствия, которое было определено ранее (напомним, что для $\varphi : A \to B$ обратное $\varphi^{-1} : B \to A$ и $(a,b) \in \varphi \Leftrightarrow (b,a) \in \varphi^{-1}$). Применяя определение композиции соответствий к φ и φ^{-1}, получим, что $(a,a) \in \varphi^{-1} \circ \varphi$ для каждого $a \in A$. Таким образом, обратная функция согласуется с понятием обратного соответствия и отличается лишь тем, что соответствие g должно быть функцией.

Пример 6. Для функции $f(x) = x$ обратной функцией будет она же сама (не надо путать алгебраическое возведение в степень -1 и переход к обратной функции). Пусть теперь $f(x) = x^2$ при $x \geqslant 0$. Докажем, что $g(x) = \sqrt{x}$ является обратной к f. Ясно, что $E(f) = [0;\infty) = D(g)$. Теперь для любого $x \in D(f)$ найдем $g\Big(f(x)\Big) = g\left(x^2\right) = \sqrt{x^2} = |x| = x$ (в последнем переходе мы использовали условие $x \geqslant 0$).

Замечание. Если функция $y = f(x)$ задается формулой, то для поиска обратной функции к f достаточно в этой формуле заменить переменную x на y, а y — на x (т. е. $x = f(y)$) и выразить из получившегося уравнения y через x.

Пример 7. Найдем обратную функцию к $y = -5x + 3$. Воспользуемся предыдущим замечанием и из уравнения $x = -5y + 3$ получим $y = -\frac{1}{5}x + \frac{3}{5}$. Композиция этих двух функций приведет к

$$g\Big(f(x)\Big) = -\frac{1}{5}(-5x+3) + \frac{3}{5} = x \quad \text{для всех} \quad x \in \mathbb{R}.$$

В следующей теореме установим простой критерий обратимости функции.

Теорема 2.4. *Функция $f : A \to \mathbb{R}$ обратима $\Leftrightarrow$ f является инъективным отображением.*

Доказательство. $\Rightarrow$) о/п: предположим, что существует $g = f^{-1}$, но f не инъективно. Тогда найдутся такие различные $x_1, x_2 \in A$, что $f(x_1) = f(x_2) = y^*$. Но тогда по определению обратной функции, должно выполняться одновременно: $g(y^*) = g\Big(f(x_1)\Big) = x_1$ и $g(y^*) = g\Big(f(x_2)\Big) = x_2$. В результате, g не однозначно, поэтому не является функцией. $\lightning$.

$\Leftarrow$) если f — инъективное отображение, то $f : A \to B$ является биекцией между A и $B = f(A)$. Тогда $g = f^{-1} : B \to A$ также является биекцией и тем более — отображением. Из выше приведенных рассуждений получим, что g является обратной функцией к f.

■

Эта теорема объясняет, почему все строго монотонные функции обратимы.

Теорема 2.5. *Пусть* $f : A \to \mathbb{R}$ *строго монотонна и* $B = f(A)$ *. Тогда*

1) f *обратима, т. е. существует* $g : B \to \mathbb{R}$ *, обратная к* f *;*

2) g *строго монотонна и имеет тот же характер монотонности, что и функция* f *;*

3) графики $\Gamma(f)$ *и* $\Gamma(g)$ *симметричны относительно прямой* $y = x$ *.*

Доказательство. Рассуждения для $f\nearrow\!\!\!\nearrow$ и $f\searrow\!\!\!\searrow$ схожи, поэтому б.о.о. будем считать, что $f\nearrow\!\!\!\nearrow$.

1) рассмотри произвольные различные $x_1, x_2 \in A$. Тогда $x_1 < x_2$ или $x_1 > x_2$. Условие $f\nearrow\!\!\!\nearrow$ дает, что $f(x_1) < f(x_2)$ или $f(x_1) > f(x_2)$. В любом случае, получаем инъективность f и по предыдущей теореме найдется $g : B \to \mathbb{R}$ — обратная функция к f.

2) докажем, что $g\nearrow\!\!\!\nearrow$. О/п: нашлись такие $y_1, y_2 \in B$, что $y_1 < y_2$, но $g(y_1) = x_1 \geqslant x_2 = g(y_2)$. Используя $f\nearrow\!\!\!\nearrow$, получим $f(x_1) \geqslant f(x_2) \Rightarrow f\Big(g(y_1)\Big) \geqslant f\Big(g(y_2)\Big) \Rightarrow y_1 \geqslant y_2$. $\not\nearrow\!\!\!\nearrow$.

3) обозначим симметрию относительно прямой $y = x$ через $S_{y=x}$. Нетрудно заметить, что для любой точки $(x_0, y_0) \in \mathbb{R}^2$ на координатной плоскости выполняется $S\Big((x_0, y_0)\Big) = (y_0, x_0)$. По определению обратного отображения (или обратного соответствия), имеем:

$$\Gamma(f) = \Big\{\Big(x, f(x)\Big) : x \in A\Big\} \quad \text{и} \quad \Gamma(g) = \Big\{\Big(f(x), x\Big) : f(x) \in B\Big\}.$$

Сделанное выше замечание об осевой симметрии дает $S_{y=x}\Big(\Gamma(f)\Big) = \Gamma(g)$.

■

П р и м е р 8. Не надо думать, что строгая монотонность является необходимым условием для обратимости. Функция $f(x) = 1/x$ не монотонна, но обратима и обратной к ней функцией будет $g(x) = 1/x$.

V. *Точки максимума и точки минимума.*

Определение. *Пусть* x_0, $\varepsilon \in \mathbb{R}$ *и* $\varepsilon > 0$. *Тогда* ε*-окрестностью точки* x_0 *называется множество* $O_\varepsilon(x_0) = \{x \in \mathbb{R} : |x - x_0| < \varepsilon\}$.

Нетрудно заметить, что $O_\varepsilon(x_0) = (x_0 - \varepsilon; x_0 + \varepsilon)$ — интервал длины 2ε с центром в точке x_0.

Определение. *Пусть* $f : A \to \mathbb{R}$. *Точка* x_0 *называется точкой максимума (соответственно точкой минимума) функции* $f(x)$ *если найдется такая* ε*-окрестность* $O_\varepsilon(x_0)$*, для которой выполняются условия:* $O_\varepsilon(x_0) \subseteq A$ *и*

$\forall x \in O_\varepsilon(x_0) \Rightarrow f(x) \leqslant f(x_0)$ ($f(x_0) \leqslant f(x)$). *Если* x_0 *является точкой максимума или точкой минимума, то она называется точкой экстремума функции* $f(x)$.

П р и м е р 9. Для квадратичной функции $f(x) = ax^2 + bx + c$ есть единственная точка экстремума — $x_0 = -b/(2a)$. Она будет точкой максимума при $a < 0$ и минимума — при $a > 0$. Функция дробной части $f(x) = \{x\}$ имеет счетное число точек минимума ($\mathbb{Z}$) и ни одной точки максимума. У функции Дирихле все точки являются точками экстремума. Ее минимумы расположены в иррациональных числах, а максимумы — в рациональных. На рис. 28 изображена функция с двумя точками минимума (x_1 и x_3) и одной точкой максимума (x_2).

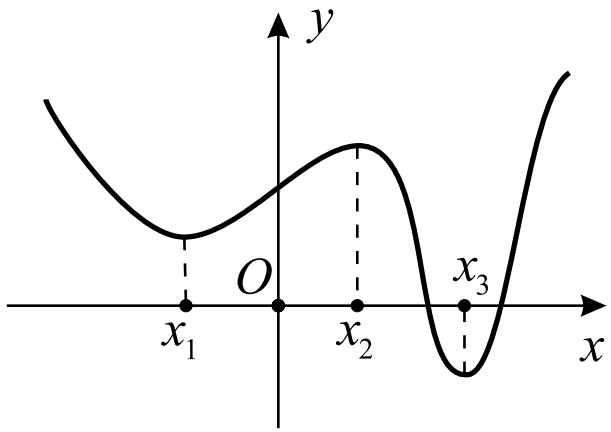

Рис. 28

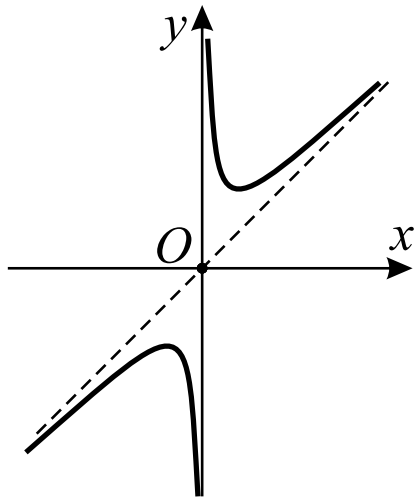

Рис. 29

VI. *Асимптоты.* Строгое определение того, что некоторое число a является пределом функции $f(x)$ при x , стремящемся к x_0 (обозначение $\lim\limits_{x\to x_0} f(x) = a$), будет дано в одиннадцатом классе. Для определения асимптот графика нам будет достаточно интуитивного представления о пределе: $\lim\limits_{x\to x_0} f(x) = a$, если при приближении аргумента x к x_0 , значения $f(x)$ приближаются к a . В качестве x_0 или a могут быть использованы $\pm\infty$.

Определение. *Прямая* $y = kx + b$ *называется асимптотой функции* $f(x)$ *при* $x \to \infty$ *(соответственно* $x \to -\infty$ *), если* $\lim\limits_{x\to\infty}(f(x) - kx - b) = 0$ ($\lim\limits_{x\to-\infty}(f(x) - kx - b) = 0$).

Определение. *Прямая* $x = x_0$ *называется вертикальной асимптотой функции* $f(x)$ *если* $\lim\limits_{x\to x_0} |f(x)| = \infty$.

П р и м е р 10. На рис. 29 изображен график $f(x) = x + 1/x$. У этой функции есть одна вертикальная асимптота — прямая $x = 0$ (поскольку $\lim\limits_{x\to 0}|x + 1/x| = \infty$). Кроме того, прямая $y = x$ одновременно является асимптотой $f(x)$ и при $x \to \infty$, и при $x \to -\infty$ (поскольку верны два предельных равенства: $\lim\limits_{x\to\infty} 1/x = 0 = \lim\limits_{x\to-\infty} 1/x$).

При исследовании свойств какой-либо функции мы будем придерживаться следующей схемы.

Схема исследования функции $f(x)$

I. Найти $D(f)$.

II. Найти $E(f)$.

III. Выяснить, является ли $f(x)$ четной, нечетной или общего вида.

IV. Определить, является ли $f(x)$ периодической, имеет ли она основной период.

V. Найти точки пересечения с осями координат. С осью Oy — это возможная точка $\Big(0, f(0)\Big)$; с осью Ox — это точки вида $(x_0, 0)$, для любых $x_0 \in \{x \in \mathbb{R} : f(x) = 0\}$.

VI. Определить промежутки знакопостоянства (для которых $f(x)$ принимает значения только одного знака).

VII. Найти промежутки монотонности.

VIII. Найти все точки максимума и минимума, определить значения функции в этих точках.

IX. Определить все асимптоты для $f(x)$.

X. Построить $\Gamma(f)$ с учетом всех предыдущих свойств.

3.3. Кольцо многочленов одной переменной

Определение. *Одночленом от x называется выражение ax^n, где $a \in \mathbb{R}$ (коэффициент одночлена), $n \in \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$. Степенью ax^n называется число* $\deg(ax^n) = \begin{cases} n, & \text{если } a \neq 0, \\ 0, & \text{если } a = 0. \end{cases}$

Определение. *Суммой одночленов* ax^n *и* bx^m *называется* $ax^n + bx^m$ *при* $n \neq m$, *или* $(a+b)x^n$, *если* $n = m$ *(в последнем случае это называется правилом приведения подобных). Произведением этих одночленов называется* abx^{n+m}.

Определение. *Многочленом от* x *называется сумма конечного числа одночленов от* x. *Многочлены будем обозначать через* f, g, h *и т. д.;* $\mathbb{R}[x]$ — *множество всех многочленов с действительными коэффициентами. Степенью* $f \in \mathbb{R}[x]$ *называется наибольшее число* $n \in \mathbb{Z}^+$ *(обозначаемое через* $\deg(f)$*) обладающее двумя свойствами: в* f *есть слагаемые степени* n *и не равна нулю сумма всех слагаемых многочлена* f, *которые имеют степень* n.

Пример 1. Если $f = x^3 - x^2 + 2x + 2x^2 - x^3 - 7 - x^2$, то $\deg(f) = 1$.

Определение. *1)* $ax^0 = a$;

2) $0x^n = 0$;

3) пусть $a \neq 0$, *тогда* $ax^n = bx^m$, *если* $a = b$ *и* $n = m$;

4) пусть $f, g \in \mathbb{R}[x]$. *Тогда* $f = g$, *если выполняются условия:*

а) $\deg(f) = \deg(g) = n$;

б) $\forall i \in \{0, 1, \ldots, n\}$ *сумма всех коэффициентов у одночленов степени* i, *которые входят в* f, *совпадает с аналогичной суммой для многочлена* g.

Если для многочлена $f \in \mathbb{R}[x]$ выполняется $f = 0$, то он называется *нулевым* многочленом. Например, $f = 5x^2 - 3x^2 - 2x^2$ — нулевой многочлен.

Определение. *Пусть* $f \in \mathbb{R}[x]$ *и* $\deg(f) = n \in \mathbb{Z}^+$. *Каноническим представлением ненулевого многочлена* f *называется запись его в следующем виде* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *причем* $a_n \neq 0$, a_n *называется старшим коэффициентом* f, *а одночлен* $a_n x^n$ — *старшим слагаемым* f. *Если* f — *нулевой многочлен, то* $f = 0$ — *его каноническое представление.*

Теорема 3.1. *Любой* $f \in \mathbb{R}[x]$ *можно представить в каноническом виде, причем только единственным образом.*

Доказательство. I. *Существование.* Докажем индукцией по $n = \deg(f)$.

Б.И. $n = 0$. Из определения степени многочлена и равенства двух многочленов, существует такое $a_0 \in \mathbb{R}$, что $f = a_0$. Это искомое представление.

Ш.И. Предположим, что для многочленов степени меньше n каноническое представление существует. Пусть теперь $\deg(f) = n$. Предварительно заметим, что из определения равенства двух многочленов следует, что $ax^n + h = h + ax^n$ для любого многочлена h. Это позволяет записать многочлен f в виде $f = b_1 x^n + b_2 x^n + \ldots + b_k x^n + g$, где многочлен g не содержит

слагаемых степени n. Положим $a_n = \sum_{i=1}^{k} b_i$. Из определения степени многочлена получаем, что $a_n \neq 0$. Многочлен f теперь представляется в виде $f = a_n x^n + g$, где $\deg(g) \leqslant (n-1)$. По предположению индукции g можно записать в виде $g = a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ (если $\deg(g) < (n-1)$, несколько первых его коэффициентов могут быть нулевыми). В результате $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ представлен в каноническом виде.

II. *Единственность.* Если $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ и $f = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$ — два канонических представления одного и того же многочлена, то из определения равенства двух многочленов следует, что $n = k$ и $a_i = b_i$ при всех $i \in \{0, 1, \ldots, n\}$. Значит, эти канонические представления одинаковы.

■

Канонический вид многочленов позволяет переписать предыдущие определения в более простом виде. Об этом — в следующих замечаниях.

Замечания. 1) далее многочлены записываем только в каноническом виде.

2) для $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ и $g = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$ — двух многочленов, записанных в каноническом виде, справедливо:

а) $f = g \Leftrightarrow n = m \ \ \& \ \ a_i = b_i$ при всех $i \in \{0, 1, \ldots, n\}$;

б) $$f+g = \begin{cases} (a_n + b_n)x^n + \ldots + (a_i + b_i)x^i + \ldots + (a_0 + b_0), & \text{если } n = m, \\ a_n x^n + \ldots + (a_m + b_m)x^m + \ldots + (a_0 + b_0), & \text{если } n > m, \\ b_m x^m + \ldots + (a_n + b_n)x^n + \ldots + (a_0 + b_0), & \text{если } n < m; \end{cases}$$

в) $f \cdot g =$

$$= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \ldots + \left(\sum_{i+j=k} a_i b_j \right) x^k + \ldots + a_0 b_0 .$$

Теорема 3.2. *Пусть $f, g \in \mathbb{R}[x]$. Тогда*

1) $\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\}$;

2) если $f, g \neq 0$, то $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Доказательство. 1) 1-й случай: $\deg(f) \neq \deg(g)$. Из замечания 2б следует, что $\deg(f+g) = \max\{\deg(f), \deg(g)\}$.

2-й случай: $\deg(f) = \deg(g) = n$. Если $a_n + b_n \neq 0$, то из замечания 2б следует, что $\deg(f+g) = n = \max\{\deg(f), \deg(g)\}$. Если $a_n + b_n = 0$, то из замечания 2б следует, что $\deg(f+g) \leqslant (n-1) < n = \max\{\deg(f), \deg(g)\}$.

2) пусть $a_n x^n$ и $b_m x^m$ — старшие слагаемые f и g соответственно. Тогда из замечания 2в следует, что $a_n b_m x^{n+m}$ — единственное слагаемое, имеющее

степень $n+m$, а остальные слагаемые, входящие в $f \cdot g$, строго меньшей степени. Учитывая, что $a_n \cdot b_m \neq 0$ из определения степени многочлена получаем, что $\deg(f \cdot g) = n + m = \deg(f) + \deg(g)$.

■

Теорема 3.3. *Для любых $f, g, h \in \mathbb{R}[x]$ выполняются следующие свойства:*

1) $f + g = g + f$;
2) $(f + g) + h = f + (g + h)$;
3) $f + 0 = 0 + f = f$;
4) $\exists f_1 \in \mathbb{R}[x] : f + f_1 = f_1 + f = 0$;
5) $(f + g)h = f \cdot h + g \cdot h$;
6) $h(f + g) = h \cdot f + h \cdot g$;
7) $(f \cdot g)h = f(g \cdot h)$;
8) $f \cdot g = g \cdot f$;
9) $1 \cdot f = f \cdot 1 = f$;
10) $f \cdot g = 0 \Leftrightarrow f = 0$ *или* $g = 0$.

Доказательство. Обозначим через a_i, b_j, c_t (соответственно) коэффициенты многочленов f, g, h при x^i, x^j и x^t. Кроме того (б.о.о.) можно считать, что $\deg(f) \geqslant \deg(g) \geqslant \deg(h)$, и для удобства доказательства можно добавить к g и h слагаемые вида $0x^p$ так, чтобы во всех трех многочленах было по одинаковому количеству слагаемых (по $\deg(f) + 1$ — именно столько слагаемых в многочлене f).

Используя замечание 2а, для доказательства свойств 1–10 достаточно проверить, что коэффициент при x^k в левой части равен коэффициенту при x^k в правой части.

1) верно, так как $a_k + b_k = b_k + a_k$.

2) верно, так как $(a_k + b_k) + c_k = a_k + (b_k + c_k)$.

3) верно, так как $a_k + 0 = 0 + a_k = a_k$.

4) если $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, то определим многочлен f_1 так: $f_1 = (-a_n)x^n + (-a_{n-1})x^{n-1} + \ldots + (-a_0)$. Тогда f_1 — искомый, поскольку $f + f_1 = f_1 + f = 0$.

5) преобразуем коэффициент при x^k в левой части:

$$\sum_{i+j=k} (a_i + b_i)c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j.$$

Получили коэффициент при x^k в правой части.

6) доказывается аналогично (5).

7) преобразуем коэффициент при x^k в левой части:

$$\sum_{l+t=k}\left(\sum_{i+j=l} a_i b_j\right) c_t = \sum_{i+j+t=k} a_i b_j c_t = \sum_{i+m=k} a_i \left(\sum_{j+t=m} b_j c_t\right).$$

Получили коэффициент при x^k в правой части.

8) верно, так как $\sum\limits_{i+j=k} a_i b_j = \sum\limits_{j+i=k} b_j a_i$.

9) верно, так как $a_k \cdot 1 = 1 \cdot a_k = a_k$.

10) $\Leftarrow$) очевидно следует из определения умножения многочленов.

$\Rightarrow$) о/п: $f \cdot g = 0$, но $f, g \neq 0$.

Если $\deg(f) = \deg(g) = 0$, то $f = a_0 \neq 0$, $g = b_0 \neq 0$ и произведение этих одночленов $f \cdot g = a_0 \cdot b_0 \neq 0$. $\lightning$.

Пусть теперь $\deg(f) \geqslant 1$ или $\deg(g) \geqslant 1$, тогда по предыдущей теореме имеем $\deg(f \cdot g) = \deg(f) + \deg(g) \geqslant 1$. Отсюда $f \cdot g \neq 0$. $\lightning$.

■

Определение. *Операцией $*$ на множестве G называется отображение $* : G \times G \to G$. Множество с операцией обозначается через $(G, *)$. Множество с двумя операциями, например $+$ и $\cdot$, обозначается $(G, +, \cdot)$.*

Определение. *Если $(K, +)$ удовлетворяет свойствам 2, 3 и 4 из последней теоремы, то $(K, +)$ называется группой[1] по сложению. Если $(K, +)$ удовлетворяет свойствам 1, 2, 3 и 4, то $(K, +)$ называется коммутативной (или абелевой[2]) группой по сложению. Если $(K, +, \cdot)$ удовлетворяет свойствам 1–6, то $(K, +, \cdot)$ называется кольцом. Если $(K, +, \cdot)$ удовлетворяет свойствам 1–7, то $(K, +, \cdot)$ называется ассоциативным кольцом. Если $(K, +, \cdot)$ удовлетворяет свойствам 1–6 и 8, то $(K, +, \cdot)$ называется коммутативным кольцом. Если $(K, +, \cdot)$ удовлетворяет свойствам 1–6 и 9, то $(K, +, \cdot)$ называется кольцом с единицей. Если $(K, +, \cdot)$ удовлетворяет свойствам 1–6 и 10, то $(K, +, \cdot)$ называется кольцом целостности (или без делителей нуля).*

[1]Эварист Галуа (1811–1832) — французский математик, основоположник современной алгебры; участвовал в революционном движении, был заключен в тюрьму и исключен из Высшей Нормальной школы (Париж), был убит на дуэли; в 17 лет получил важные результаты в теории алгебраических уравнений о невозможности решения в радикалах произвольного уравнения степени выше четвертой; пользуясь понятиями «группа», «подгруппа», «нормальный делитель», «поле» создал совершенно новую алгебраическую теорию, развившуюся в теорию групп.

[2]Нильс Хенрик Абель (1802–1829) — норвежский математик, работы посвящены алгебре, теории функций и математическому анализу; доказал неразрешимость в радикалах общего уравнения пятой степени, выделил типы абелевых уравнений, разрешимых в радикалах, заложил основы теории абелевых групп; развил теорию сходимости степенных рядов и впервые (1826) полностью исследовал проблему сходимости общего биномиального ряда; создал теорию эллиптических функций.

Следствие. $(\mathbb{R}[x], +, \cdot)$ *является коммутативно ассоциативным кольцом целостности с единицей.*

Доказательство. Очевидно следует из предыдущей теоремы.

■

3.4. Деление многочленов. Деление с остатком. Алгоритм Евклида

Определение. *Пусть* $f, g \in \mathbb{R}[x]$, $g \neq 0$. *Тогда* f *делится на* g, *если найдется такой многочлен* $h \in \mathbb{R}[x]$, *что* $f = g \cdot h$.

Обозначается делимость многочленов так же, как и для целых чисел: $f \vdots g$ или $g \mid f$ (последнее обозначение читается «g делит f»). Очевидно, что нулевой многочлен делится на любой другой, поэтому в следующей теореме он не рассматривается.

Теорема 4.1. *Пусть* $f, g, h, q \in (\mathbb{R}[x]\backslash\{0\})$, *тогда выполняются следующие свойства:*

1) $f \vdots f$ *(рефлексивность);*

2) если одновременно $f \vdots g$ *и* $g \vdots f$, *то найдется такая константа* $c \in \mathbb{R}$, *что* $f = c \cdot g$;

3) если одновременно $f \vdots g$ *и* $g \vdots h$, *то* $f \vdots h$ *(транзитивность);*

4) если $f + g = h$ *и два многочлена из трех* $\{f, g, h\}$ *делятся на* q, *то и третий многочлен делится на* q *(линейность).*

Доказательство. 1) очевидно, так как $f = f \cdot 1$.

2) по определению найдутся такие $h, h_1 \in \mathbb{R}[x]$, что $f = g \cdot h$ и $g = f \cdot h_1$, откуда $f = f \cdot (h \cdot h_1)$. Поскольку многочлены ненулевые, по теореме 3.2 имеем $\deg(f) = \deg(f) + \deg(h) + \deg(h_1)$, откуда $\deg(h) = \deg h_1 = 0$. Поэтому найдутся такие две ненулевые константы $c, c_1 \in \mathbb{R}[x]$, что $h = c$ и $h_1 = c_1$. В результате получим требуемое: $f = c \cdot g$, для некоторого $c \in \mathbb{R}$.

3) по определению найдутся такие $q_1, q_2 \in \mathbb{R}[x]$, что $f = g \cdot q_1$ и $g = h \cdot q_2$, откуда $f = h \cdot (q_1 \cdot q_2)$ или $f \vdots h$.

4) доказательства всех трех случаев между собой похожи, поэтому (б.о.о.) считаем, что $f, h \vdots q$. Находим такие $f_1, h_1 \in \mathbb{R}[x]$, что $f = q \cdot f_1$ и $h = q \cdot h_1$. Теперь равенство $f + g = h$ можно переписать (учитывая существование обратных по сложению в $\mathbb{R}[x]$ и дистрибутивность) в виде

$$g = h_1 q - f_1 q = (h_1 - f_1) q.$$

Последнее означает, что $g \vdots q$.

■

Определение. *Пусть* $f, g \in \mathbb{R}[x]$, $\deg(g) \geqslant 1$. *Многочлен* f *можно разделить с остатком на* g, *если найдется такая пара* $q, r \in \mathbb{R}[x]$, *что выполняется равенство* $f = gq + r$ *и* $\deg(r) < \deg(g)$.

Теорема 4.2. *Для любых* $f, g \in \mathbb{R}[x]$, $\deg(g) \geqslant 1$ *многочлен* f *можно разделить с остатком на* g, *причем единственным образом.*

Доказательство. I. Докажем сначала существование пары многочленов $q, r \in \mathbb{R}[x]$, удовлетворяющей определению. Представим многочлены в каноническом виде: $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ и $g = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0$.

Доказывать существование частного и остатка будем индукцией по $n = \deg(f) \in \mathbb{Z}^+$.

Б.И. $n = 0$. Тогда $f = g \cdot 0 + f$ — искомое представление, поскольку $\deg(f) < \deg(g)$.

Ш.И. Предположим, что все могочлены, чья степень меньше n, можно разделить с остатком на g. Докажем теперь, что многочлен f, имеющий степень n, также можно разделить с остатком на g. Если $\deg(f) < \deg(g)$, то искомым представлением будет $f = g \cdot 0 + f$. Осталось разобрать случай $n = \deg(f) \geqslant \deg(g) = k$. Пусть $q_0 = \frac{a_n}{b_k} x^{n-k}$ (в нашем случае $n - k \in \mathbb{Z}^+$) и рассмотрим многочлен $f^* = g \cdot q_0$. Ясно, что старший коэффициент f^* равен $\frac{a_n}{b_k} \cdot b_k = a_n$ и $\deg(f^*) = k + (n - k) = n = \deg(f)$. Обозначим через f_1 разность $f - f^*$. Из-за сокращения старших слагаемых получим, что $\deg(f_1) < n$. Теперь по предположению индукции найдем пару $q_1, r \in \mathbb{R}[x]$, что выполняется равенство $f_1 = gq_1 + r$ и $\deg(r) < \deg(g)$, отсюда

$$f - f^* = gq_1 + r \Leftrightarrow f = gq_0 + gq_1 + r \Leftrightarrow f = g(q_0 + q_1) + r \Leftrightarrow f = gq + r,$$

где $q = q_0 + q_1$ и $\deg(r) < \deg(g)$.

II. Докажем, что такое представление единственно. О/п: нашлось другое представление $f = gq^* + r^*$ и $\deg(r^*) < \deg(g)$. Если $r = r^*$, то, из равенства $gq = gq^*$ получим $g(q - q^*) = 0$, а отсутствие делителей нуля (так как $(\mathbb{R}[x], +, \cdot)$ является кольцом целостности) дает $q = q^*$, что противоречит предположению. Осталось рассмотреть случай $r \neq r^*$. Из равенства двух представлений $gq + r = gq^* + r^*$ имеем $r - r^* = g(q^* - q)$. Тогда по теореме 3.2 получим, что $\deg(r - r^*) = \deg(g) + \deg(q^* - q) \geqslant \deg(g)$, но по той же теореме $\deg(r - r^*) \leqslant \max\{\deg(r), \deg(r^*)\} < \deg(g)$. ↯.

■

Определение. *Для произвольных ненулевых* $f, g \in \mathbb{R}[x]$ *их наибольшим общим делителем называется многочлен* $h \in \mathbb{R}[x]$ *(обозначение:* $h = НОД\,(f, g)$ *или* $h = (f, g)$ *), для которого одновременно:*

1) $f \vdots h$ *и* $g \vdots h$ *;*

2) h *имеет максимальную степень среди многочленов, удовлетворяющих свойству (1).*

Пример 1. Для многочленов $g = x^4 - 1$ и $f = x^6 - 1$ наибольшими общими делителями будут каждый из следующих многочленов: $h_1 = x^2 - 1$, $h_2 = -3x^2 + 3$, $h_3 = \sqrt{\pi}x^2 - \sqrt{\pi}$.

Предыдущий пример показывает, что НОД двух многочленов определен неоднозначно. Если для ненулевых $f, g \in \mathbb{R}[x]$ только константы удовлетворяют свойствам (1) и (2) последнего определения, то многочлены f и g называются *взаимно простыми* и используют обозначение $(f, g) = 1$.

Лемма 4.3. *Пусть* $f, g, h^* \in \mathbb{R}[x]$ *и многочлен* h^* *удовлетворяет двум условиям:*

1) $f \vdots h^*$ *и* $g \vdots h^*$,

2) для любого $h \in \mathbb{R}[x]$, *для которого* $f \vdots h$ *и* $g \vdots h$, *выполняется* $h^* \vdots h$. *Тогда* $h^* = (f, g)$.

Доказательство. О/п: предположим, что $h_0 = (f, g)$ и выполняется строгое неравенство $\deg(h_0) > \deg(h^*)$. Поскольку $f, g \vdots h_0$, свойство (2) гарантирует, что $h^* \vdots h_0$, т. е. $h^* = h_0 \cdot q$, где $q \in (\mathbb{R}\backslash\{0\})$, откуда следует $\deg(h^*) = \deg(h_0) + \deg(q) \geqslant \deg(h_0)$. $\lightning$.

■

Еще один вариант *алгоритма Евклида*, изложенный в следующей теореме, позволяет найти $НОД\,(f, g)$.

Теорема 4.4. *Пусть* $f, g \in \mathbb{R}[x]$ *и* $\deg(f) \geqslant \deg(g) \geqslant 1$. *Последовательно делим один многочлен на другой с остатком до тех пор, пока остаток не станет нулевым многочленом:*

1) $f = gq + r$, $\deg(r) < \deg(g)$, $q, r \in \mathbb{R}[x]$, $r \neq 0$ *;*

2) $g = rq_1 + r_1$, $\deg(r_1) < \deg(r)$, $q_1, r_1 \in \mathbb{R}[x]$, $r_1 \neq 0$ *;*

3) $r = r_1q_2 + r_2$, $\deg(r_2) < \deg(r_1)$, $q_2, r_2 \in \mathbb{R}[x]$, $r_2 \neq 0$ *;*

и т.д.....

$n+1)$ $r_{n-2} = r_{n-1}q_n + r_n$, $\deg(r_n) < \deg(r_{n-1})$, $q_n, r_n \in \mathbb{R}[x]$, $r_n \neq 0$ *;*

$n+2)$ $r_{n-1} = r_nq_{n+1} + 0$, $q_{n+1} \in \mathbb{R}[x]$.

Тогда $r_n = (f, g)$.

Доказательство. Сразу заметим, что процесс деления с остатком будет конечным, поскольку $\deg(g) > \deg(r) > \deg(r_1) > \deg(r_2) > \ldots$, и последний ненулевой остаток будет получен не более чем за $\deg(g)$ шагов (считаем, что один шаг — это одно деление с остатком). Поэтому r_n определен корректно.

1) докажем, что $f, g \vdots r_n$. Рассуждать будем, начиная с последнего уравнения, поднимаясь вверх (*метод подъема*). Из последнего уравнения сразу следует, что $r_n \mid r_{n-1}$. Учитывая, что $r_n \mid r_n$, $r_n \mid r_{n-1}$, предпоследнее уравнение и свойство линейности нам дают $r_n \mid r_{n-2}$. Аналогично рассуждая, приходим к $r_n \mid r_1, r \Rightarrow r_n \mid g$, и, наконец, из первого уравнения и условий $r_n \mid r$, $r_n \mid g$ получим, что $r_n \mid f$.

2) теперь рассмотрим произвольный многочлен $h \in \mathbb{R}[x]$, для которого $f \vdots h$ и $g \vdots h$. На этот раз начнем рассуждать с первого уравнения, двигаясь вниз (*метод спуска*). Из первого уравнения и свойства линейности получим, что $r \vdots h$. Далее, второе уравнение и условия $g \vdots h$ и $r \vdots h$ дают нам, что $r_1 \vdots h$. Повторив такие рассуждения еще $n-1$ раз, получим $r_n \vdots h$.

Поскольку r_n удовлетворяет свойствам (1) и (2) предыдущей леммы, заключаем, что $r_n = (f, g)$.

■

П р и м е р 2. Применим алгоритм Евклида для многочленов $f = x^6 - 1$ и $g = x^4 - 1$. Последовательно делим многочлены с остатком:

$$x^6 - 1 = (x^4 - 1)x^2 + (x^2 - 1), \quad x^4 - 1 = (x^2 - 1)(x^2 + 1) + 0.$$

За два шага мы получили, что $x^2 - 1 = (f, g)$.

3.5. Теорема Безу. Схема Горнера

Определение. *Пусть* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{R}[x]$. *Функцией, задаваемой многочленом* f *называется* $f(x) : \mathbb{R} \to \mathbb{R}$, *которая каждому* $x \in \mathbb{R}$ *ставит в соответствие число* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. *Число* $x_0 \in \mathbb{R}$ *называется корнем многочлена* f, *если* $f(x_0) = 0$.

Следующая теорема называется *теоремой Безу*[3].

Теорема 5.1. *Пусть* $f \in \mathbb{R}[x]$. *Тогда остаток от деления многочлена* f *на двучлен* $x - x_0$ *равен* $f(x_0)$ *— значению многочлена в* x_0.

[3]Этьен Безу (1730–1783) — французский математик, работал в училище гардемаринов и в Королевском артиллерийском корпусе; работы посвящены алгебре, разработал общие методы решения систем алгебраических уравнений любых степеней; автор «Курса математики» в шести томах, впоследствии неоднократно переиздававшегося.

Доказательство. По теореме 4.2 найдутся такие многочлены $q, r \in \mathbb{R}[x]$, что $f = (x-x_0)q+r$, причем $\deg(r) < \deg(x-x_0) = 1$. Последнее означает, что $\deg(r) = 0$, т. е. r является константой и от x не зависит. Равенство многочленов дает равенство функций, которые ими задаются, поэтому для всех $x \in \mathbb{R}$ выполняется $f(x) = (x-x_0)q(x)+r$. Подставляя в это равенство x_0, получим $f(x_0) = (x_0 - x_0)q(x_0) + r$ или $f(x_0) = r$.

■

П р и м е р 1. Найдем остаток от деления многочлена $f = x^{2021}+7x+9$ на $x+1$. Переписав $x+1$ в виде $x-(-1)$, получим, что $x_0 = -1$. Применяя теорему Безу, имеем $r = f(-1) = -1-7+9 = 1$.

Следствие. *Пусть $f \in \mathbb{R}[x]$. Тогда x_0 является корнем $f \Leftrightarrow f \vdots (x-x_0)$.*

Доказательство. $\Rightarrow$) по теореме Безу, если $r = f(x_0) = 0$, то $f = (x-x_0)q$ для некоторого $q \in \mathbb{R}[x]$. Последнее означает, что $f \vdots (x-x_0)$.

$\Leftarrow$) пусть теперь $f \vdots (x-x_0)$. Найдем такой многочлен $q \in \mathbb{R}[x]$, что $f = (x-x_0)q$. Поэтому для всех $x \in \mathbb{R}$ выполняется $f(x) = (x-x_0)q(x)$. Подставляя в это равенство x_0, получим $f(x_0) = (x_0 - x_0)q(x_0) = 0$.

■

Теорема 5.2. *Пусть $f \in \mathbb{R}[x]$, $f \neq 0$, $\deg(f) = n \in \mathbb{Z}^+$. Тогда f может иметь не более n корней.*

Доказательство. Индукция по n. Б.И. При $n = 0$ имеем $f = a_0 \neq 0$ и f не имеет корней. При $n = 1$ рассмотрим многочлен $f = a_1x+a_0$, $a_1 \neq 0$. Тогда $a_1x + a_0 = 0 \Leftrightarrow x_0 = -a_0/a_1$ — единственный корень многочлена f.

Ш.И. Предположим, что любой ненулевой многочлен степени $k < n$ имеет не более k корней. Рассмотрим $f \in \mathbb{R}[x]$, для которого $\deg(f) = n > 1$. Если f не имеет корней, то утверждение доказано. Пусть теперь x_0 — корень f. По предыдущему следствию представим f в виде $f = (x-x_0)g(x)$. Из равенства $\deg(f) = 1 + \deg(g)$ получим, что $\deg(g) = n-1$, поэтому g, по предположению индукции, имеет не более $n-1$ корня. Любой корень g является корнем f (если $g(x_1) = 0$, то $f(x_1) = (x_1-x_0)g(x_1) = 0$). Осталось показать, что других корней, кроме x_0 и корней многочлена g, у f нет. Если $x^* \neq x_0$ и $g(x^*) \neq 0$, то (поскольку в кольце целостности $(\mathbb{R}, +, \cdot)$ нет делителей нуля) выполняется $f(x^*) = (x^* - x_0)g(x^*) \neq 0$. Таким образом, f имеет не более n корней и шаг индукции доказан.

■

Следствие 1. *Пусть $f, g \in \mathbb{R}[x]$, $f \neq 0$, $\deg(f), \deg(g) \leqslant n \in \mathbb{Z}^+$. Если*

найдутся такие попарно различные x_1, $x_2, \ldots,$ $x_{n+1} \in \mathbb{R}$, *для которых* $f(x_i) = g(x_i)$ *при всех* $i \in \{1, 2, \ldots, n+1\}$, *то* $f = g$.

Доказательство. О/п: $f \neq g$. Рассмотрим многочлен $h = f - g$. Тогда $\deg(h) \leqslant n$ и $h(x_i) = f(x_i) - g(x_i) = 0$. Таким образом, ненулевой многочлен степени не выше n имеет по крайней мере $n+1$ корень, что противоречит предыдущей теореме.

■

Напомним, что две функции $f : A \to \mathbb{R}$ и $g : B \to \mathbb{R}$ равны, если $A = B$ и $\forall x \in A \Rightarrow f(x) = g(x)$. Кроме того, у нас еще определено равенство многочленов. Логично ожидать, что эти два равенства приводят к одинаковым результатам.

Следствие 2. *Пусть* $f, g \in \mathbb{R}[x]$. *Тогда* $f = g \Leftrightarrow \Big(\forall x \in \mathbb{R} \Rightarrow f(x) = g(x)\Big)$.

Доказательство. $\Rightarrow$) равенство многочленов дает равенство функций, которые ими задаются, поэтому для всех $x \in \mathbb{R}$ выполняется $f(x) = g(x)$.

$\Leftarrow$) найдем такое число $n \in \mathbb{Z}^+$, что $n + 1 > \deg(f), \deg(g)$ (достаточно положить $n = \max\{\deg(f), \deg(g)\}$). Выберем попарно различные x_1, $x_2, \ldots,$ $x_{n+1} \in \mathbb{R}$, для них выполняется $f(x_i) = g(x_i)$. По предыдущему следствию имеем $f = g$.

■

Формулы следующей теоремы называются *схемой Горнера или схемой Руффини*[4]*-Горнера*[5].

Теорема 5.3. *Пусть* $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{R}[x]$, $n = \deg(f) \in \mathbb{N}$, $c \in \mathbb{R}$. *Если* $f(x) = (x - c)g(x) + r$, *то* $\deg(g) = n - 1$ *и коэффициенты многочлена* $g(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots + b_1 x + b_0$ *и остаток* r *находятся по следующим формулам:*

$b_{n-1} = a_n$;
$b_{n-2} = b_{n-1} \cdot c + a_{n-1}$;
$\vdots$
$b_i = b_{i+1} \cdot c + a_{i+1}$;
$\vdots$
$b_0 = b_1 \cdot c + a_1$;
$r = b_0 \cdot c + a_0$.

[4]Паоло Руффини (1765–1822) — итальянский математик и медик; преподавать начал еще будучи студентом; первым доказал (1798) невозможность решения в радикалах всех уравнений степени выше четвертой; прежде Э. Галуа и Н. Х. Абеля установил значение теории групп для учения об алгебраических уравнениях.

[5]Уильям Горнер (1786–1837) — английский математик; исследования относятся к теории алгебраических уравнений, разработал способ приближенного решения уравнений любой степени.

Доказательство. Из $f(x) = (x-c)g(x) + r$ сразу получаем уравнение $\deg(f) = 1 + \deg(g)$ или $\deg(g) = n-1$ (остаток r имеет нулевую степень, поэтому мы его не учитываем в уравнении для степеней). Равенство двух многочленов

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_{i+1}x^{i+1} + a_i x^i + \ldots + a_1 x + a_0 =$$

$$= (x-c)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_{i+1}x^{i+1} + b_i x^i + \ldots + b_1 x + b_0) + r$$

позволяет нам приравнять соответствующие коэффициенты при одинаковых степенях. При x^n: $a_n = b_{n-1}$. При x^{n-1}: $a_{n-1} = b_{n-2} - b_{n-1}\cdot c$ или $b_{n-2} = b_{n-1}\cdot c + a_{n-1}$. При x^{i+1}: $a_{i+1} = b_i - b_{i+1}\cdot c$ или $b_i = b_{i+1}\cdot c + a_{i+1}$. При x^1: $a_1 = b_0 - b_1 \cdot c$ или $b_0 = b_1 \cdot c + a_1$. Наконец, при x^0: $a_0 = r - b_0 \cdot c$ или $r = b_0 \cdot c + a_0$.

■

Замечание. Схему Горнера обычно записывают в виде следующей таблицы.

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
c	a_n	$b_{n-1}\cdot c + a_{n-1}$	$b_{n-2}\cdot c + a_{n-2}$	$\ldots$	$b_1\cdot c + a_1$	$b_0\cdot c + a_0$
	$\shortparallel$	$\shortparallel$	$\shortparallel$	$\ldots$	$\shortparallel$	$\shortparallel$
	b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	r

П р и м е р 2. Разделим с остатком многочлен $f(x) = x^5 + x^4 - 2x^2 + 25$ на $x+2$. Сначала перепишем $x+2$ в виде $\Big(x-(-2)\Big)$ и поймем, что $c = -2$. Далее в схеме Горнера дополним все недостающие коэффициенты нулями и составим таблицу:

	1	1	0	-2	0	25
-2	1	-1	2	-6	12	1

Таким образом, получим разложение $f = (x+2)(x^4 - x^3 + 2x^2 - 6x + 12) + 1$.

Следствие 1. *Пусть* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{R}[x]$, $c \in \mathbb{R}$, $n = \deg(f) \in \mathbb{N}$. *Если* $f(x) = (x-c)g(x) + r$, *то* $\deg(g) = n-1$ *и старший коэффициент* g *совпадает со старшим коэффициентом многочлена* f.

Доказательство. Равенство $b_{n-1} = a_n$ дает первая формула схемы Горнера.

■

Следствие 2. *Пусть* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{R}[x]$, $c \in \mathbb{R}$, $n = \deg(f) \in \mathbb{N}$. *Если* $f(x) = (x-c)g(x) + r$ *и все коэффициенты* f *и число* c *являются целыми, то все коэффициенты* g *и остаток* r *также являются целыми числами.*

Доказательство. Из предыдущего следствия имеем $b_{n-1} = a_n \in \mathbb{Z}$. По второй формуле получим, что $b_{n-2} = b_{n-1} \cdot c + a_{n-1} \in \mathbb{Z}$. Если уже доказано, что $b_{i+1} \in \mathbb{Z}$, то $b_i = b_{i+1} \cdot c + a_{i+1} \in \mathbb{Z}$. Поэтому все коэффициенты многочлена g являются целыми. Последняя формула схемы Горнера дает $r = b_0 \cdot c + a_0 \in \mathbb{Z}$.

■

3.6. Рациональные корни многочленов с целыми коэффициентами

Напомним стандартные обозначения для множеств натуральных и целых чисел: $\mathbb{N} = \{1, 2, \ldots, n, \ldots\}$ и $\mathbb{Z} = \{0, \pm1, \pm2, \ldots, \pm n, \ldots\}$. Число вида n/l, где $n, l \in \mathbb{Z}$ и $l \neq 0$ называется *рациональным*, $\mathbb{Q}$ — это множество всех рациональных чисел. Также будем считать, что $i \in \{0, 1, 2, \ldots, n\}$ и $i = \overline{0, n}$ обозначают одно и то же. Сразу из определения суммы и произведения многочленов следует, что множества

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 : \, n \in \mathbb{Z}^+, a_i \in \mathbb{Z}, \, i = \overline{0, n}\},$$

$$\mathbb{Q}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 : \, n \in \mathbb{Z}^+, a_i \in \mathbb{Q}, \, i = \overline{0, n}\}$$

с операциями сложения и умножения являются кольцами (точнее, ассоциативно-коммутативными кольцами целостности с единицей). Множество $\mathbb{Z}[x]$ — это множество всех многочленов, имеющих только целые коэффициенты, а $\mathbb{Q}[x]$ — множество всех многочленов, все коэффициенты которых рациональны.

Дробь $p/q \in \mathbb{Q}$ называется *несократимой*, если выполнено равенство $(|p|, |q|) = 1$, т. е. $|p|$ и $|q|$ — взаимно простые числа. Нетрудно заметить, что если $(|p|, |q|) = 1$, то и для любой пары натуральных чисел k, n верно $(|p^k|, |q^n|) = 1$. Иначе бы $|p^k|$ и $|q^n|$ имели бы общий простой делитель $r \in P$. Но тогда из свойств делимости следует, что $|p| \vdots r$ и $|q| \vdots r$, что дает $(|p|, |q|) \geqslant r$. $\not\subset$.

Следующее простое утверждение показывает, что задача поиска корней многочлена с рациональными коэффициентами быстро сводится к нахождению корней многочлена с целыми коэффициентами.

Лемма 6.1. *1) для любого* $f \in \mathbb{Q}[x]$ *найдется такой многочлен* $g \in \mathbb{Z}[x]$, *что* $f(x) = 0 \Leftrightarrow g(x) = 0$.

2) пусть $\frac{p}{q}, \frac{p_1}{q_1} \in \mathbb{Q}$ *и* $q, q_1 \in \mathbb{N}$. *Если дробь* p/q *несократимая и выполняется равенство* $p/q = p_1/q_1$, *то* $q \leqslant q_1$.

3) если дробь p/q *несократимая и* $q \in \mathbb{N}$, *то для любого целого* k *дробь* $\dfrac{p - k \cdot q}{q}$ *также будет несократимой.*

Доказательство. 1) пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ и $a_i = k_i/l_i \in \mathbb{Q}$ для всех $i = \overline{0, n}$. Обозначим через $L = l_0 \cdot l_1 \cdot \ldots \cdot l_n = \prod\limits_{i=0}^{n} l_i$ (если $a_i = 0$, будем считать, что $l_i = 1$). Тогда $L \neq 0$ и многочлен $g(x) = L \cdot f(x)$ будет с целыми коэффициентами. Поскольку $L \neq 0$, равенство $f(x) = 0$ равносильно $L \cdot f(x) = 0$, т. е. $f(x) = 0 \Leftrightarrow g(x) = 0$.

2) из равенства двух дробей сразу получаем $p \cdot q_1 = p_1 \cdot q \vdots q$, откуда (в силу $(|p|, |q|) = 1$) выполняется $q_1 \vdots q$, что для натуральных дает $q_1 \geqslant q$.

3) рассуждая от противного, имеем $\dfrac{p - k \cdot q}{q} = \dfrac{p_1}{q_1}$, причем $q, q_1 \in \mathbb{N}$ и $q > q_1$. Отсюда

$$\frac{p}{q} - k = \frac{p_1}{q_1} \quad \text{или} \quad \frac{p}{q} = \frac{p_1 + k \cdot q_1}{q_1},$$

что противоречит предыдущему утверждению.

■

Следующая теорема называется *первой теоремой о рациональных корнях многочлена с целыми коэффициентами.*

Теорема 6.2. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Если несократимая дробь* $p/q \in \mathbb{Q}$ *является корнем многочлена* $f(x)$, *то* p *делит свободный член (т.е.* $a_0 \vdots p$*), а* q *делит старший коэффициент (т.е.* $a_n \vdots q$*).*

Доказательство. Пусть $f(p/q) = 0$. Значит $a_n \cdot \dfrac{p^n}{q^n} + a_{n-1} \cdot \dfrac{p^{n-1}}{q^{n-1}} + \ldots + a_1 \cdot \dfrac{p}{q} + a_0 = 0$ или, после умножения на q^n,

$$a_n \cdot p^n + a_{n-1} \cdot p^{n-1} \cdot q + \ldots + a_1 \cdot p \cdot q^{n-1} + a_0 \cdot q^n = 0. \qquad (1)$$

Отсюда $a_0 \cdot q^n = -(a_n \cdot p^n + a_{n-1} \cdot p^{n-1} \cdot q + \ldots + a_1 \cdot p \cdot q^{n-1})$. Правая часть этого равенства делится на p, поэтому $a_0 \cdot q^n \vdots p$. Учитывая, что $(|p|, |q^n|) = 1$, получим $a_0 \vdots p$.

Из (1) также следует $a_n \cdot p^n = -(a_{n-1} \cdot p^{n-1} \cdot q + \ldots + a_1 \cdot p \cdot q^{n-1} + a_0 \cdot q^n)$. Аналогично приходим к $a_n \cdot p^n \vdots q$ и $a_n \vdots q$.

■

Очевидно, что предыдущая теорема не может быть обратима. В противном случае уравнение $30x^3 - 13x^2 - 5x + 2 = 0$ имело бы две дюжины корней! Видно, что если старший и свободный коэффициенты имеют большое число делителей, то список рациональных чисел, которые потенциально могут быть корнями этого многочлена, велик. Сократить его поможет следующая теорема (она называется *второй теоремой о рациональных корнях многочлена с целыми коэффициентами*).

Теорема 6.3. *Пусть* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Если несократимая дробь* $p/q \in \mathbb{Q}$ *является корнем многочлена* $f(x)$, *то для любого целого числа* k, *для которого* $p - k \cdot q \neq 0$, *выполняется соотношение* $f(k) \vdots (p - k \cdot q)$.

Доказательство. Домножим многочлен $f(x)$ на q^n и сделаем замену $y = qx$:

$$q^n f(x) = a_n (qx)^n + a_{n-1} q (qx)^{n-1} + \ldots + a_1 q^{n-1} (qx) + a_0 q^n =$$

$$= a_n y^n + a_{n-1} q y^{n-1} + \ldots + a_1 q^{n-1} y + a_0 q^n = g(y). \qquad (2)$$

Очевидно, что $g(y)$ — это многочлен с целыми коэффициентами, то есть $g(y) \in \mathbb{Z}[y]$. Обозначим через $x_0 = p/q$ и $y_0 = q x_0 = p$. Теперь из равенства (2) имеем $g(y_0) = q^n f(x_0) = 0$, отсюда $y = p$ — корень многочлена $g(y)$, поэтому, по теореме Безу, $g(y) = (y - p) h(y)$. По второму следствию из схемы Горнера получаем, что все коэффициенты $h(y)$ являются целыми числами (так как $g(y) \in \mathbb{Z}[y]$ и $p \in \mathbb{Z}$). Последнее означает, что $h(k \cdot q)$ является целым числом для любого $k \in \mathbb{Z}$. Таким образом из (2) при $x = k$ и $y = k \cdot q$ получаем

$$q^n f(k) = g(k \cdot q) = (k \cdot q - p) h(k \cdot q) \vdots (p - k \cdot q).$$

Учитывая, что $(|q^n|, |p - k \cdot q|) = 1$ (это следует из третьего утверждения леммы), окончательно получим $f(k) \vdots (p - k \cdot q)$.

■

Покажем на следующем примере как работают в связке обе теоремы о рациональных корнях многочлена с целыми коэффициентами.

П р и м е р 1. Найдем все рациональные корни многочлена, который нам уже встречался: $f(x) = 30x^3 - 13x^2 - 5x + 2$. По первой теореме $2 \vdots p$ и

$30 \vdots q$. Договоримся знак дроби относить к числителю, потому $p \in \{\pm 1, \pm 2\}$ и $q \in \{1, 2, 3, 5, 6, 10, 15, 30\}$. Тогда список несократимых дробей, которые потенциально могут быть корнями этого многочлена выглядит следующим образом (целые числа также запишем в виде дробей, чтобы позже было удобно пользоваться второй теоремой):

$$\pm\frac{1}{1}, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{5}, \pm\frac{1}{6}, \pm\frac{1}{10}, \pm\frac{1}{15}, \pm\frac{1}{30},$$
$$\pm\frac{2}{1}, \pm\frac{2}{3}, \pm\frac{2}{5}, \pm\frac{2}{15}.$$

Быстро находим $f(1) = 14$. Не расстраиваемся, что $x = 1$ не является корнем нашего многочлена, поскольку при $k = 1$ вторая теорема о рациональных корнях нам дает очень полезную информацию:

$$14 = f(1) \vdots (p - q). \tag{3}$$

Из этого соотношения делаем вывод, что $-1/2$ не может быть корнем нашего многочлена, так как 14 не делится на $p - q = -1 - 2 = -3$. Аналогично рассуждая, отсеиваем дроби: $-1/3$, $\pm 1/5$, $1/6$, $\pm 1/10$, $-1/15$, $\pm 1/30$, $-2/1$, $-2/3$, $2/5$, $\pm 2/15$. Из первоначального списка остались дроби (список сократили в три раза!):

$$-\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, -\frac{1}{6}, \frac{1}{15}, \frac{2}{1}, \frac{2}{3}, -\frac{2}{5}.$$

Дальше найдем $f(-1) = -36$. И снова применим вторую теорему, но уже при $k = -1$:

$$-36 = f(-1) \vdots (p + q). \tag{4}$$

Дробь $-1/6$ не удовлетворяет последнему соотношению, поскольку -36 не делится на $-1 + 6 = 5$. Также (4) позволяет отбросить $1/15$ и $2/3$. Остаются дроби (число $-1 = -1/1$ исключили непосредственной подстановкой): $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{1}$, $-\frac{2}{5}$. Теперь, подставляя по схеме Горнера, обнаруживаем, что $f(1/2) = f(1/3) = f(-2/5) = 0$. Больше трех у многочлена третьей степени корней быть не может.

3.7. Кратные корни многочленов. Обобщенная теорема Виета

Определение. *Число x_0 называется корнем многочлена $f(x) \in \mathbb{R}[x]$ кратности k ($k \in \mathbb{N}$), если $f(x) = (x - x_0)^k g(x)$ и $g(x_0) \neq 0$.*

Так, например, у многочлена $f(x) = -2(x+1)^3(x-2)(x-5)^2$ корни -1, 2 и 5 имеют (соответственно) третью, первую и вторую кратности.

Лемма 7.1. *1) пусть $f(x) = f_1(x) \cdot f_2(x)$ и x_0 является корнем $f_i(x)$ кратности k_i $(i \in \{1,2\})$, тогда x_0 является корнем $f(x)$ кратности $k_1 + k_2$.*

2) пусть $x_0 \neq x_1$, а натуральные числа k, l — кратности (соответственно) корней x_0 и x_1 у многочлена $f(x)$. Если $f(x) = (x - x_0)^k g(x)$, то выполняются следующие два утверждения:

a) старшие коэффициенты многочленов f и g одинаковы;

b) кратность корня x_1 у многочлена $g(x)$ также равна l.

Доказательство. 1) по определению $f_i(x) = (x - x_0)^{k_i} g_i(x)$ и $g_i(x_0) \neq 0$ $(i \in \{1,2\})$. Отсюда $f(x) = (x - x_0)^{k_1+k_2} g(x)$, где $g(x) = g_1(x) \cdot g_2(x)$ и $g(x_0) = g_1(x_0) \cdot g_2(x_0) \neq 0$, тогда x_0 является корнем $f(x)$ кратности $k_1 + k_2$.

2) первое утверждение следует из схемы Горнера — старший коэффициент наследуется частным при делении на двучлен $x - x_0$. При доказательстве второго утверждения воспользуемся определением и представим $f(x) = (x-x_0)^k g(x) = (x-x_1)^l h(x)$. Поскольку $0 = f(x_1) = (x_1-x_0)^k g(x_1)$, число x_1 также является корнем многочлена $g(x)$ (по условию, $x_1 - x_0 \neq 0$). Обозначим через m кратность x_1 в многочлене $g(x)$. Из первого утверждения леммы следует, что m не может быть больше l. Осталось доказать, что m не может быть меньше l. Предположим противное, $m < l$. Тогда $f(x) = (x-x_0)^k (x-x_1)^m g_1(x) = (x-x_1)^m (x-x_1)^{l-m} h(x)$ и $g_1(x_1) \neq 0$. Из теоремы о делении с остатком следует, что частное от деления (в нашем случае — на $(x-x_1)^m$) и остаток (в нашем случае — нулевой остаток) находятся однозначно, поэтому $(x - x_0)^k g_1(x) = (x - x_1)^{l-m} h(x)$. Правая часть этого равенства при $x = x_1$ обращается в ноль, в то время как $(x_1 - x_0)^k g_1(x_1) \neq 0$. $\nleftrightarrow$.

■

Теорема 7.2. *Пусть $\deg f = n \in \mathbb{N}$ и a_n — старший коэффициент $f(x)$. Числа $x_1, x_2, \ldots, x_n$ (выписанные столько раз, какова их кратность) являются корнями $f(x)$ тогда и только тогда, когда*

$$f(x) = a_n(x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n).$$

Доказательство. $\Rightarrow$) докажем индукцией по n. База индукции при $n = 1$ очевидна. Проверим шаг. Пусть x_1 — корень $f(x)$ кратности k. Можно считать, что $x_1 = x_2 = \ldots = x_k$. По лемме $f(x) = (x - x_1)^k g(x)$, причем $x_{k+1}, \ldots, x_n$ являются корнями $g(x)$ той же кратности, причем старшие коэффициенты f и g равны. Это позволяет воспользоваться предположением

индукции и представить $g(x) = a_n(x - x_{k+1}) \cdot \ldots \cdot (x - x_n)$, что после подстановки в равенство $f(x) = (x - x_1)^k g(x)$ завершает доказательство шага.

$\Leftarrow$) очевидно, поскольку каждое из чисел x_1, x_2, $\ldots$, x_n является корнем многочлена $f(x)$.

■

Следующая теорема называется *обобщенной теоремой Виета*[6].

Теорема 7.3. *Пусть* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$. *Числа* x_1, x_2, $\ldots$, x_n *(выписанные столько раз, какова их кратность) являются корнями* $f(x)$ *тогда и только тогда, когда они удовлетворяют следующей системе*

$$\begin{cases} x_1 + x_2 + \ldots + x_n = -\dfrac{a_{n-1}}{a_n}, \\ x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \dfrac{a_{n-2}}{a_n}, \\ \qquad\qquad \vdots \\ \displaystyle\sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1}x_{i_2} \cdot \ldots \cdot x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}, \\ \qquad\qquad \vdots \\ x_1x_2 \cdot \ldots \cdot x_n = (-1)^n \dfrac{a_0}{a_n}. \end{cases} \tag{5}$$

Доказательство. По предыдущей теореме числа x_1, x_2, $\ldots$, x_n (выписанные столько раз, какова их кратность) являются корнями $f(x)$ тогда и только тогда, когда

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-1} + \ldots + a_k x^k + \ldots + a_1 x + a_0 =$$

$$= a_n(x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n) =$$

$$= a_n x^n - a_n(x_1 + x_2 + x_3 + \ldots + x_n)x^{n-1} + a_n(x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n)x^{n-2} + \ldots$$

$$+ (-1)^k a_n \left(\sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1}x_{i_2} \cdot \ldots \cdot x_{i_k} \right) x^{n-k} + \ldots + (-1)^n a_n x_1x_2 \cdot \ldots \cdot x_n.$$

[6]Франсуа Виет (1540–1603) — французский математик, по профессии юрист; впервые ввел символические обозначения не только для неизвестных, но и для коэффициентов уравнений; нашел первое точное выражение для π в виде бесконечного произведения; предложил ряд способов решения сферических треугольников; Виет, по поручению Генриха IV, сумел расшифровать переписку испанских агентов во Франции, за что был даже обвинен испанским королем Филиппом II в использовании черной магии.

Приравниваем коэффициенты при соответствующих степенях, делим на ненулевое a_n и получаем формулы системы (5).

■

Формулы, доказанные в следующей теореме, называются *формулами сокращенного умножения.*

Теорема 7.4. *1) для любого натурального n и любых $x, a \in \mathbb{R}$ выполняется*

$$x^n - a^n = (x-a)\left(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \ldots + x \cdot a^{n-2} + a^{n-1}\right).$$

2) для любого нечетного натурального n и любых $x, a \in \mathbb{R}$ выполняется

$$x^n + a^n = (x+a)\left(x^{n-1} - x^{n-2}a + x^{n-3}a^2 - \ldots - x \cdot a^{n-2} + a^{n-1}\right).$$

Доказательство. 1) индукция по n.

Б.И. При $n = 1$ утверждение очевидно.

Ш.И. Предположим, что формула верна для n и докажем ее для $n+1$:

$$x^{n+1} - a^{n+1} = x^{n+1} - a^n x + a^n x - a^{n+1} = x\left(x^n - a^n\right) + a^n(x-a) =$$

$$= x(x-a)\left(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \ldots + x \cdot a^{n-2} + a^{n-1}\right) + a^n(x-a) =$$

$$= (x-a)\left(x^n + x^{n-1}a + x^{n-2}a^2 + \ldots + x \cdot a^{n-1} + a^n\right).$$

2) следует из (1), так как при любом нечетном n справедливо равенство $x^n + a^n = x^n - (-a)^n$.

■

3.8. Многочлены от нескольких переменных

В этом параграфе рассмотрим пример использования трансфинитной индукции при доказательстве одного алгебраического факта. Речь пойдет о представлении произвольного симметрического многочлена в виде многочлена от элементарных симметрических многочленов. Доказательство этой важной теоремы потребует от нас значительного числа вспомогательных понятий и утверждений.

Определение. *Одночленом от переменных x_1, $x_2, \ldots, x_n$ называется выражение f_0 вида $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, где $a \in \mathbb{R}$ и k_i являются неотрицательными целыми числами для всех $i \in \mathbb{N}_{\leqslant n}$. Сумма $\sum_{i=1}^{n} k_i$ называется степенью*

f_0, *если* $a \neq 0$ *(обозначается через* $\deg(f_0)$*). Если коэффициент* a *равен нулю, то одночлен называется нулевым и его степень равна нулю. При* $a \neq 0$ *упорядоченный* n*-набор* $(k_1, k_2, \ldots, k_n)$ *называется показательным кодом одночлена (обозначается через* $ПК(f_0)$*). При* $a = 0$ *считаем, что* $ПК(f_0) = (0, 0, \ldots, 0)$.

Определение. *1)* $0x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} = 0$ *— нулевой одночлен;*
2) $ax_1^{k_1}\ldots x_{i-1}^{k_{i-1}}x_i^0x_{i+1}^{k_{i+1}}\ldots x_n^{k_n} = ax_1^{k_1}\ldots x_{i-1}^{k_{i-1}}x_{i+1}^{k_{i+1}}\ldots x_n^{k_n}$ *;*
3) при $a \neq 0$ *выполняется* $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} = bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$*, если* $(a, k_1, k_2, \ldots, k_n) = (b, l_1, l_2, \ldots, l_n)$.

Определение. *Ненулевые одночлены* $f_0 = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ *и* $g_0 = bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ *называются подобными, если* $ПК(f_0) = ПК(g_0)$ *. При этом их суммой называется одночлен* $(a+b)x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ *(правило приведения подобных). Если же эти одночлены не подобны между собой, их суммой называется выражение* $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} + bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$.

Определение. *Многочленом от переменных* x_1 , $x_2, \ldots, x_n$ *называется сумма конечного числа одночленов от этих переменных. Через* $\mathbb{R}[x_1, x_2, \ldots, x_n]$ *обозначают множество всех многочленов от переменных* x_1 , $x_2, \ldots, x_n$.

В силу двух последних определений можно считать, что многочлен не содержит подобных слагаемых. В этом случае его степенью мы будем называть максимальную из степеней входящих в него слагаемых. Так, например, степень многочлена от трех переменных $f(x, y, z) = x^4y + x^4 + x^2y^3 + z^5$ равна пяти. Заметим, что $f(x, y, z)$ содержит три слагаемых пятой степени. Порядок, в котором выписаны эти слагаемые, называется *лексикографическим*.

Определение. *Многочлен записан в лексикографическом порядке, если его слагаемые упорядочены по убыванию их показательных кодов. Старшим слагаемым многочлена называется слагаемое с максимальным показательным кодом.*

Записанные в лексикографическом порядке многочлены не содержат подобных слагаемых. Пусть $f, g \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ записаны в лексикографическом порядке. Тогда $f = g$, если для каждого слагаемого, входящего в f, найдется равное ему слагаемое входящее в g, и, наоборот, для каждого одночлена, входящего в g, найдется равный ему одночлен, входящий в f.

Суммой двух многочленов $f, g \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ называется многочлен $f + g$, полученный суммой слагаемых f и g и применением правила приведения подобных.

Произведением одночленов $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ и $bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ называется одночлен $abx_1^{k_1+l_1}x_2^{k_2+l_2}\dots x_n^{k_n+l_n}$. Теперь, чтобы получить произведение $f\cdot g$ двух многочленов $f(x_1,\dots,x_n)$ и $g(x_1,\dots,x_n)$, достаточно сложить все попарные произведения одночленов f на одночлены g и применить правило приведения подобных.

На множестве $\mathbb{R}[x_1,x_2,\dots,x_n]$ мы определили операции сложения и умножения. Ожидаемо, что $(\mathbb{R}[x_1,x_2,\dots,x_n],+,\cdot)$ будет коммутативно ассоциативным кольцом целостности с единицей (или *абелево кольцо с единицей*). Доказательство этого утверждения ведется индукцией по числу переменных n. Б.И. Случай $n=1$ разобран в теореме 3.3. Ш.И. Предположив, что $(\mathbb{R}[x_1,x_2,\dots,x_n],+,\cdot)$ — абелево кольцо с единицей, будем рассматривать множество многочленов $(\mathbb{R}[x_1,x_2,\dots,x_n,x_{n+1}],+,\cdot)$ как многочлены только от одной переменной x_{n+1} с коэффициентами из $(\mathbb{R}[x_1,x_2,\dots,x_n],+,\cdot)$. Но тогда по базе индукции это множество также будет абелевым кольцом с единицей. Шаг индукции проверен.

Лемма 8.1. *Пусть $f,g\in\mathbb{R}[x_1,x_2,\dots,x_n]$. Старшим слагаемым произведения $f\cdot g$ будет являться произведение старшего слагаемого f на старшее слагаемое g.*

Доказательство. Запишем f и g в лексикографическом порядке:

$$f=ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}+\dots+cx_1^{m_1}x_2^{m_2}\dots x_n^{m_n}+\dots,$$

$$g=bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}+\dots+dx_1^{t_1}x_2^{t_2}\dots x_n^{t_n}+\dots.$$

По условию $(k_1,k_2,\dots,k_n)>(m_1,m_2,\dots,m_n)$, поэтому

$$(k_1+l_1,k_2+l_2,\dots,k_n+l_n)>(m_1+l_1,m_2+l_2,\dots,m_n+l_n). \qquad (*)$$

Также, сравнивая ПК старшего и ПК любого другого слагаемого для второго многочлена, получим $(l_1,l_2,\dots,l_n)>(t_1,t_2,\dots,t_n)$, поэтому

$$(m_1+l_1,m_2+l_2,\dots,m_n+l_n)>(m_1+t_1,m_2+t_2,\dots,m_n+t_n). \qquad (**)$$

Из $(*)$ и $(**)$, а также из транзитивности лексикографического порядка следует, что ПК произведения двух старших слагаемых больше ПК любых других попарных произведений.

■

Среди многочленов от n переменных особое место занимают симметрические многочлены и элементарные симметрические многочлены.

Определение. *Многочлен* $f(x_1, \ldots, x_n)$ *называется симметрическим многочленом, если для любых* $i, j \in \mathbb{N}_{\leqslant n}$ *и* $i < j$ *выполняется*

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Это означает, что многочлен f *не изменяется при одновременной замене во всех его одночленах переменной* x_i *на* x_j *и переменной* x_j *на* x_i .

П р и м е р 1. Так, например, многочлены $x^3y + y^3x$ и $x^2 - xy + y^2$ являются симметрическими от двух переменных. Многочлен относительно трех переменных $f(x, y, z) = x^2+y^2+xyz$ не является симметрическим, поскольку после замены $x \leftrightarrow z$ получится другой многочлен $g(x, y, z) = z^2 + y^2 + xyz$.

Легко проверяется, что сумма и произведение симметрических многочленов от одних и тех же переменных также является симметрическим многочленом от этих переменных. Кроме того, старшее слагаемое любого симметрического многочлена обладает следующим свойством.

Лемма 8.2. *Пусть* $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ *— старшее слагаемое симметрического многочлена* $f(x_1, \ldots, x_n)$. *Тогда* $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$.

Доказательство. О/п: предположим, что существует такое наименьшее $i < n$, что $k_i < k_{i+1}$. Так как f является симметрическим многочленом, то в него также входит одночлен $ax_1^{k_1}\ldots x_{i+1}^{k_i}x_i^{k_{i+1}}\ldots x_n^{k_n}$. Легко заметить, что $(k_1, \ldots, k_{i+1}, k_i, \ldots, k_n) > (k_1, \ldots, k_i, k_{i+1}, \ldots, k_n)$, т. е. многочлен содержит слагаемое с большим показательным кодом, а это противоречит тому, что $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ — старшее слагаемое многочлена.

■

Определение. *Элементарными симметрическими многочленами от переменных* $x_1, \ldots, x_n$ *называются следующие многочлены:*

$$\begin{aligned}
&\sigma_1(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_n,\\
&\sigma_2(x_1, \ldots, x_n) = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \sum_{i<j\leqslant n} x_ix_j,\\
&\vdots\\
&\sigma_k(x_1, \ldots, x_n) = \sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n} x_{i_1}x_{i_2}\ldots x_{i_k},\\
&\vdots\\
&\sigma_n(x_1, \ldots, x_n) = x_1x_2\ldots x_n.
\end{aligned}$$

П р и м е р 2. Представим симметрические многочлены $f(x, y) = x^3y+y^3x$ и $g(x, y) = x^2-xy+y^2$ в виде многочленов от элементарных симметрических:

$\sigma_1(x,y) = x + y$ и $\sigma_2(x,y) = xy$. После несложных преобразований

$$f(x,y) = xy\Big((x+y)^2 - 2xy\Big) = \sigma_2({\sigma_1}^2 - 2\sigma_2) = f_1(\sigma_1,\sigma_2),$$

$$g(x,y) = (x+y)^2 - 3xy = {\sigma_1}^2 - 3\sigma_2 = g_1(\sigma_1,\sigma_2).$$

Теорема 8.3. *Любой симметрический многочлен $f(x_1,\ldots,x_n)$ может быть представлен в виде многочлена от элементарных симметрических многочленов от переменных $x_1,\ldots,x_n$.*

Доказательство. Воспользуемся следствием теоремы 13.4 из второй главы: множество $X = (\mathbb{Z}^+)^n$ с лексикографическим порядком будет вполне упорядоченным множеством. Кроме того, из леммы 8.2 нам известно, что показатели степеней у старшего слагаемого многочлена f убывают. Поэтому во множестве X рассмотрим подмножество

$$A = \{(k_1,k_2,\ldots,k_n) \in X : k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n\}.$$

Если между элементами множества A рассматривать тот же порядок, что был между ними на множестве X (т.е. рассмотреть пересечение лексикографического порядка с множеством $A \times A$), то полученный порядок также будет полным. Далее применим трансфинитную индукцию в доказательстве следующего утверждения: $T(k_1,k_2,\ldots,k_n) =$ «любой симметрический многочлен со старшим слагаемым $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, где $(k_1,k_2,\ldots,k_n) \in A$, может быть представлен в виде многочлена от $\sigma_1,\sigma_2,\ldots,\sigma_n$».

Б.И. Докажем $T(0,0,\ldots,0)$. Поскольку $ax_1^0x_2^0\ldots x_n^0$ является старшим слагаемым f (и, к тому же, единственным, поскольку слагаемых с меньшим ПК не существует), то $f = a\sigma_1^0\sigma_2^0\ldots\sigma_n^0$, что и завершает доказательство базы.

Ш.И. Предположим теперь, что $T(l_1,l_2,\ldots,l_n)$ истинно для любого упорядоченного набора $(l_1,l_2,\ldots,l_n) < (k_1,k_2,\ldots,k_n)$ (т.е. любой многочлен со старшим слагаемым $ax_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$, где $(l_1,l_2,\ldots,l_n) < (k_1,k_2,\ldots,k_n)$, представим в виде $f_1(\sigma_1,\sigma_2,\ldots,\sigma_n)$). Докажем, что $T(k_1,k_2,\ldots,k_n)$ также истинно. Для этого рассмотрим вспомогательный одночлен

$$g_0(\sigma_1,\sigma_2,\ldots,\sigma_n) = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\ldots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}.$$

Заметим, что при замене $\sigma_1,\sigma_2,\ldots,\sigma_n$ на их значения от $x_1,x_2,\ldots,x_n$ получится некоторый многочлен от переменных $x_1,x_2,\ldots,x_n$. Легко определяется его старшее слагаемое. Действительно, оно равно произведению старших

слагаемых $\sigma_1(x_1,\ldots,x_n)$, $\sigma_2(x_1,\ldots,x_n),\ldots,$ $\sigma_n(x_1,\ldots,x_n)$, т.е.

$$a(x_1)^{k_1-k_2}\cdot(x_1x_2)^{k_2-k_3}\cdot\ldots\cdot(x_1x_2\ldots x_{n-1})^{k_{n-1}-k_n}\cdot(x_1x_2\ldots x_n)^{k_n}=$$

$$=ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}.$$

В результате старшее слагаемое f равно старшему слагаемому g_0. Таким образом, многочлен $g=f-g_0$ имеет своим старшим слагаемым слагаемое, которое строго младше $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$. Применяя к g предположение индукции, имеем $g(x_1,\ldots,x_n)=g_1(\sigma_1,\ldots,\sigma_n)$, откуда

$$f=g+g_0=g_1(\sigma_1,\ldots,\sigma_n)+g_0(\sigma_1,\ldots,\sigma_n)=h(\sigma_1,\ldots,\sigma_n).$$

■

На практике использовать предыдущую теорему технически сложно, поэтому для представления симметрического многочлена от элементарных симметрических применяют *метод неопределенных коэффициентов.*

Алгоритм. Пусть f — симметрический многочлен от x_1, $x_2,\ldots,$ x_n. Для представления f в виде многочлена $g(\sigma_1,\ldots,\sigma_n)$ от элементарных симметрических достаточно:

1) f представить в виде суммы симметрических однородных многочленов $f_1+f_2+\ldots+f_s$ (многочлен, у которого все слагаемые имеют одинаковую степень называется *однородным*);

2) пусть каждое слагаемое многочлена f_i имеет степень m, тогда представить f_i в виде суммы всех таких одночленов от $\sigma_1,\ldots,\sigma_n$ с неопределенными коффициентами, которые также имеют степень m относительно x_1, $x_2,\ldots,$ x_n (здесь надо учесть, что σ_i — это однородный многочлен степени i от x_1, $x_2,\ldots,$ x_n);

3) неопределенные коэффициенты у слагаемых многочлена f_i определить подстановкой конкретных значений вместо x_1, $x_2,\ldots,$ x_n и σ_1, $\sigma_2,\ldots,$ σ_n.

П р и м е р 3. Представим $f(x,y,z)=(xyz)^5+x^3+x^2+y^3+y^2+z^3+z^2$ в виде многочлена от σ_1, σ_2, σ_3, где $\sigma_1=x+y+z$, $\sigma_2=xy+xz+yz$, $\sigma_3=$ $=xyz$. Для этого сначала запишем $f=f_1+f_2+f_3$, где $f_1=(xyz)^5=(\sigma_3)^5$, $f_2=x^2+y^2+z^2=(x+y+z)^2-2xy-2xz-2yz=\sigma_1^2-2\sigma_2$ и $f_3=x^3+y^3+z^3$. Остается применить метод неопределенных коэффициентов для f_3. Все его слагаемые имеют степень 3, поэтому будем подбирать одночлены от σ_1, σ_2 и σ_3, которые также имеют степень 3 относительно x, y, z:

$$f_3(x,y,z)=A\sigma_1^3+B\sigma_1\sigma_2+C\sigma_3=g_3(\sigma_1,\sigma_2\sigma_3).$$

Заметим, что в этой сумме нет слагаемых вида $D\sigma_1^2$, $E\sigma_1\sigma_3$, $F\sigma_2^3$, поскольку они имеют от переменных x, y, z соответственно степени 2, 4 и 6 (и даже если они появятся в правой части равенства, то коэффициенты при этих одночленах будут нулевыми). Теперь определим три коэффициента A, B и C подстановкой конкретных значений вместо x, y, z и σ_1, σ_2, σ_3. Это удобно делать с помощью следующей таблицы (мы приравниваем значения из четвертого и восьмого столбцов таблицы).

x	y	z	$f_3(x,y,z)$	σ_1	σ_2	σ_3	$g_3(\sigma_1,\sigma_2\sigma_3)$	$f_3=g_3$
1	0	0	1	1	0	0	A	$A=1$
1	1	0	2	2	1	0	$8A+2B$	$B=-3$
1	1	-2	-6	0	-3	-2	$-2C$	$C=3$

Таким образом, $f_3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$, что дает

$$f(x,y,z)=(\sigma_3)^5+\sigma_1^2-2\sigma_2+\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3.$$

3.9. Комплексные числа, основная теорема алгебры

В этом параграфе используются свойства действительной прямой, которая будет построена в одиннадцатом классе, и несколько тригонометрических формул, доказанных в следующей главе, поэтому к изучению комплексных чисел можно вернуться позже.

Впервые комплексные числа появились в работах Кардано[7](1545) и Бомбелли[8] (1572). Обозначение i для мнимой единицы было предложено Л. Эйлером. Основная причина появления комплексных чисел — в разрешимости уравнений степени выше первой. Любое уравнение вида $ax+b=c$ при $a,b,c\in\mathbb{Q}$ и $a\neq 0$ разрешимо в $\mathbb{Q}$, т. е. найдется число $x_0\in\mathbb{Q}$, которое будет корнем этого уравнения (нетрудно заметить, что $(c-b)/a$ рационально). При $a,b,c\in\mathbb{R}$ и $a\neq 0$ та же формула даст действительный корень уравнения $ax+b=c$, т. е. линейные уравнения разрешимы и в $\mathbb{R}$. Уравнения

[7]Джироламо Кардано (1502–1576) — итальянский математик и механик, врач; в 1545 издал труд «Великое искусство», в котором привел решение уравнений третьей и четвертой степени (о решении уравнений третьей степени ему сообщил Н. Тарталья, о четвертой — Л. Феррари, ученик Кардано); вывел общие правила передачи движения применительно к зубчатым механизмам; опубликовал устройство карданного вала (механизм был известен еще Леонардо да Винчи); был изобретателем масляной лампы с автоматической подачей масла и кодового замка.

[8]Рафаэль Бомбелли (1526–1572) — итальянский математик, инженер-гидравлик; перевел и опубликовал «Арифметику» Диофанта, благодаря этому событию начинается теория чисел в Европе; доказал, что решение древних задач о трисекции угла и удвоении куба можно свести к решению кубического уравнения; придумал первые математические скобки, они имели вид перевернутой буквы L.

второй и большей степени уже могут не быть разрешимыми в $\mathbb{R}$. Так, например, уравнение $x^2+1=0$ (с действительными коэффициентами) не имеет действительных корней. Попробуем расширить множество действительных чисел до некоторого поля так, чтобы это уравнение уже имело корень.

Прежде обсудим несколько алгебраических понятий.

Определение. *Множество G с операцией $*$ называется группой, если выполняются три свойства:*

1) $\forall a,b,c\in G \Rightarrow (a*b)*c=a*(b*c)$ (ассоциативность);

2) $\exists e\in G : e*a=a*e$ для всех $a\in G$ (существование нейтрального элемента e);

3) $\forall a\in G\ \exists b\in G : a*b=b*a=e$ (существование b — обратного элемента к a).

Если к этим свойствам добавляется (4) $\forall a,b\in G \Rightarrow a*b=b*a$ (коммутативность), то $(G,*)$ называется коммутативной или абелевой группой.

Нейтральный элемент по сложению традиционно обозначается через 0, по умножению — через 1. Обратный элемент к a по сложению обозначается $-a$, по умножению — через a^{-1}. Полем $(\mathbb{P},+,\cdot)$ называется множество с двумя операциями, причем $(\mathbb{P},+)$ и $(\mathbb{P}\backslash\{0\},\cdot)$ — абелевы группы и выполняется дистрибутивность: $\forall a,b,c\in\mathbb{P}\Rightarrow(a+b)\cdot c=a\cdot c+b\cdot c$. В любом поле нет делителей нуля, поскольку равенство $a\cdot b=0$ при ненулевом a можно домножить на a^{-1} и получить $(a^{-1}\cdot a)\cdot b=a^{-1}\cdot 0$, что дает $b=0$. Таким образом, любое поле является абелевым кольцом (т. е. коммутативно ассоциативным кольцом целостности) с единицей и обратными по умножению к каждому ненулевому элементу. Примерами полей будут $(\mathbb{Q},+,\cdot)$ и $(\mathbb{R},+,\cdot)$, но $(\mathbb{Z},+,\cdot)$ — только абелево кольцо, в нем нет обратных по умножению ко многим элементам.

Напомним, что биекцией f между множествами X и Y называется всюду определенное и однозначное соответствие (т.е. каждому элементу $x\in X$ ставится в соответствие единственный $y=f(x)$), которое к тому же сюръективно (т.е. $f(X)=Y$) и инъективно (т.е. $f(x_1)\neq f(x_2)$ для любых $x_1\neq x_2$). Пусть теперь на множествах X и Y заданы некоторые операции $*$ и $\star$ (речь идет о бинарных операциях, т.е. отображениях $*: X\times X\to X$ и $\star: Y\times Y\to Y$). Если биекция $f: X\to Y$ сохраняет результат операции (т.е. для любой пары $x_1,x_2\in X$ выполняется $f(x_1*x_2)=f(x_1)\star f(x_2)$), то f называется *изоморфизмом*, а множества $(X,*)$ и $(Y,\star)$ называются *изоморфными* (что обозначают через $X\cong Y$ или $(X,*)\cong(Y,\star)$). С точки зрения алгебры изоморфные множества считаются одинаковыми. Когда

говорят об изоморфизмах колец (множеств с двумя операциями), требуют, чтобы биекция сохраняла результат каждой из операций.

Определение. *Множеством комплексных чисел называется множество* $\mathbb{C}$ *с двумя операциями* $+, \cdot$, *удовлетворяющее следующим свойствам:*

1) $(\mathbb{C}, +, \cdot)$ *— поле;*

2) $\mathbb{C}$ *содержит*[9] $\mathbb{R}$, *причем операции сложения и умножения на* $\mathbb{C}$ *продолжают операции, определенные на* $\mathbb{R}$;

3) существует такой элемент в $\mathbb{C}$, *квадрат которого равен* -1 *(т.е. найдется* $i \in \mathbb{C}$, *что* $i^2 = -1$*);*

4) $\mathbb{C}$ *— минимальное*[10] *поле со свойствами 1–3.*

Условие (4) предыдущего определения заменим более простым в проверке условием из следующей теоремы. Опять, равенства и включения множеств надо понимать с точностью до изоморфизма.

Теорема 9.1. *Пусть* $(K, +, \cdot)$ *— поле, удовлетворяющее свойствам (1)–(3) предыдущего определения,* $j \in K$, $j^2 = -1$. *Если для каждого элемента* $z \in K$ *найдутся такая пара действительных чисел* a, b, *что* $z = a + b \cdot j$, *тогда* $K = \mathbb{C}$.

Доказательство. Из (4) свойства сразу следует, что $\mathbb{C} \subseteq K$, поэтому достаточно проверить только обратное включение. Обозначим через $i \in \mathbb{C}$ тот элемент, что $i^2 = -1 = j^2$. Так как K — поле, то из последнего равенства получаем $j^2 = i^2$ или $(j-i)(j+i) = 0$. Учитывая, что в поле нет делителей нуля, получим $j = i \in \mathbb{C}$ или $j = -i \in \mathbb{C}$. Поэтому для любого $z \in K$ будет выполняться $z = a + b \cdot j = a + b \cdot i \in \mathbb{C}$ или $z = a - b \cdot i \in \mathbb{C}$ (так как $a, b, \pm i \in \mathbb{C}$). Отсюда $K \subseteq \mathbb{C}$.

■

Построение множества комплексных чисел. Рассмотрим простой путь построения множества комплексных чисел, считая, что свойства поля $(\mathbb{R}, +, \cdot)$ нам уже известны. Пусть[11] $C = \{(a, b) : a, b \in \mathbb{R}\}$. Для краткости элементы C будем обозначать z, z', z_1, z_2 и т. д. Пусть $z_1 = (a, b) \in C$ и $z_2 = (c, d) \in C$. Определим операции на C следующим образом:

$$z_1 + z_2 = (a + c, b + d) \quad (1), \qquad z_1 \cdot z_2 = (ac - bd, ad + bc) \quad (2).$$

[9] точнее, содержит изоморфную копию, т.е. такое $\widetilde{\mathbb{R}} \subseteq \mathbb{C}$, что $(\widetilde{\mathbb{R}}, +, \cdot) \cong (\mathbb{R}, +, \cdot)$.

[10] по включению, но опять, с точностью до изоморфизма.

[11] Эта стандартная модель была описана Гамильтоном в 1835 году в работе «Теория алгебраических пар». Уильям Гамильтон (1805–1865) — ирландский математик, механик-теоретик; один из лучших математиков XIX века; изобрел кватернионы, заложил основы векторного анализа и вариационного исчисления; автор вариационного принципа наименьшего действия, применяемого во многих разделах физики.

Теорема 9.2. $(C,+,\cdot)$ — *поле.*

Доказательство. 1) проверка того, что $(C,+)$ — коммутативная группа не составляет труда. Заметим только, что $\tilde{0}=(0,0)$ является нейтральным элементом по сложению, а обратным по сложению для $z=(a,b)$ будет $z'=$ $=(-a,-b)$.

2) докажем, что $(C\backslash\{\tilde{0}\},\cdot)$ — коммутативная группа. Коммутативность и ассоциативность умножения легко следуют из (1), (2) и аналогичных свойств сложения и умножения действительных чисел. Нейтральным элементом по умножению будет $\tilde{1}=(1,0)$. Действительно, из (2) имеем

$$(a,b)\cdot(1,0)=(a\cdot 1-b\cdot 0,a\cdot 0+b\cdot 1)=(a,b).$$

Осталось показать, что любой элемент $z=(a,b)\neq\tilde{0}$ имеет обратный по умножению. Условие $(a,b)\cdot(x,y)=(1,0)$ равносильно системе линейных уравнений: $ax-by=1$, $bx+ay=0$. Равносильно преобразуем к системе: $(a^2+b^2)x=a$, $bx+ay=0$. Откуда $x=\dfrac{a}{a^2+b^2}$, $y=-\dfrac{b}{a^2+b^2}$ (для равносильного перехода здесь мы использовали $a^2+b^2\neq 0$). Таким образом, обратным по умножению к $z=(a,b)$ будет элемент (сразу договоримся его обозначать через z^{-1})

$$z^{-1}=\left(\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\right).$$

3) проверим, что выполняется дистрибутивность. Для произвольной тройки $z_1=(a,b)$, $z_2=(c,d)$, $z_3=(e,f)$ имеем:

$$z_1(z_2+z_3)=(a,b)\cdot(c+e,d+f)=(ac+ae-bd-bf,ad+af+bc+be),$$

$$z_1z_2+z_1z_3=(ac-bd,ad+bc)+(ae-bf,af+be)=$$
$$=(ac+ae-bd-bf,ad+af+bc+be).$$

■

Теорема 9.3. *Существует такое* $\tilde{\mathbb{R}}\subseteq C$, *что* $(\tilde{\mathbb{R}},+,\cdot)\cong(\mathbb{R},+,\cdot)$.

Доказательство. Пусть $\tilde{a}=(a,0)$ и $\tilde{\mathbb{R}}=\{\tilde{a}:a\in\mathbb{R}\}$. Очевидно, что отображение $f:\tilde{\mathbb{R}}\to\mathbb{R}$, действующее по правилу $f(\tilde{a})=a$ является биекцией и надо только проверить сохранения сложения и умножения этим отображением. Только в этой теореме операции сложения и умножения на $\tilde{\mathbb{R}}$ будем обозначать через $\oplus$ и $\bullet$. Рассмотрим теперь произвольные два элемента $\tilde{a}=(a,0)$ и $\tilde{b}=(b,0)$

Сохранение сложения: $f(\tilde{a}\oplus\tilde{b}) = f\Big((a,0)\oplus(b,0)\Big) = f\Big((a+b,0)\Big) = a+b = f(\tilde{a}) + f(\tilde{b})$.

Сохранение результата умножения: $f(\tilde{a}\bullet\tilde{b}) = f\Big((a,0)\bullet(b,0)\Big) = f\Big((a\cdot b+0\cdot 0, 0\cdot a+b\cdot 0)\Big) = f\Big((ab,0)\Big) = a\cdot b = f(\tilde{a})\cdot f(\tilde{b})$.

■

После установленного изоморфизма $(\tilde{\mathbb{R}},+,\cdot) \cong (\mathbb{R},+,\cdot)$ можно считать, что a означает то же самое, что и $\tilde{a}$ при всех $a\in\mathbb{R}$.

Теорема 9.4. *В C существует такой элемент i, квадрат которого равен -1. Для каждого элемента $z\in C$ найдется такая пара действительных чисел a,b, что $z = a+b\cdot i$.*

Доказательство. Пусть $i = (0,1)$. Из определения умножения на C имеем $i^2 = (0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1,0) = -1$.

Нетрудно проверить, что $(0,b) = (b,0)\cdot(0,1)$. Тогда для произвольного $z=(a,b)\in C$ выполняется:

$$z = (a,b) = (a,0) + (0,b) = (a,0) + (b,0)\cdot(0,1) = a + b\cdot i.$$

■

Следствие. *Множество $(C,+,\cdot)$ является множеством комплексных чисел.*

Доказательство. Непосредственно следует из теорем 9.1–9.4.

■

Алгебраическая форма комплексных чисел. Сопряженные числа. Представление комплексного числа в виде $z = a+b\cdot i$, где $a,b\in\mathbb{R}$ и $i^2=-1$ называется *алгебраической формой записи* z, при этом коэффициент $a = \Re(z) = \operatorname{Re} z$ называется *действительной (или вещественной)* частью z, а $b = \Im(z) = \operatorname{Im} z$ называется *мнимой* частью z. При $a=0$ число $z = b\cdot i$ называется *чисто мнимым*. Нетрудно заметить, что представление комплексного числа в алгебраической форме единственно. Действительно, из равенства $z = a+b\cdot i = c+d\cdot i$ сразу получаем $a-c = (d-b)i$ (используем существование обратных по сложению и дистрибутивность). При $d=b$ сразу имеем $a=c$. Если же $d-b\neq 0$, используем существование обратных по умножению в поле для выражения $i = (a-c)/(d-b)\in\mathbb{R}$, что противоречит условию $i\notin\mathbb{R}$.

Определение. *Сопряженным к числу $z = a+b\cdot i$ называется $\bar{z} = a-b\cdot i$.*

Теорема 9.5. *1)* $z = \bar{z} \Leftrightarrow z \in \mathbb{R}$ *;*

2) $z + \bar{z}$ *и* $z \cdot \bar{z}$ *являются действительными числами;*

3) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$, $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$ *;*

4) если $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ *— многочлен с действительными коэффициентами (т.е.* $f \in \mathbb{R}[z]$ *) и комплексное число* $z_0 \in \mathbb{C}\backslash\mathbb{R}$ *является его корнем, тогда и* $\bar{z}_0$ *также является корнем* $f(z)$ *;*

5) если $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ *— многочлен с действительными коэффициентами и комплексное число* z_0 *является корнем кратности* l *этого многочлена, тогда и* $\bar{z}_0$ *также является корнем* $f(z)$ *кратности* l *.*

Доказательство. 1) очевидно, так как равенство $b = -b$ возможно только при $b = 0$.

2) проверим только для $z \cdot \bar{z} = (a^2 + b^2) + (ba - ab) \cdot i = a^2 + b^2 \in \mathbb{R}$.

3) пусть $z_1 = a + b \cdot i$, $z_2 = c + d \cdot i$. Снова, проверим только результат о произведении:

$$\overline{z_1 \cdot z_2} = \overline{(ac - bd) + (ad + bc) \cdot i} = (ac - bd) - (ad + bc) \cdot i,$$

$$\bar{z}_1 \cdot \bar{z}_2 = (a - b \cdot i)(c - d \cdot i) = (ac - bd) - (ad + bc) \cdot i.$$

4) пусть z_0 является корнем $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 \in \mathbb{R}[z]$. Тогда, используя свойства (1) и (3), получим

$$\bar{0} = \overline{f(z_0)} = \overline{a_n z_0^n} + \overline{a_{n-1} z_0^{n-1}} + \ldots + \overline{a_1 z_0} + \overline{a_0} = \bar{a}_n \bar{z}_0{}^n + \bar{a}_{n-1} \bar{z}_0{}^{n-1} + \ldots + \bar{a}_1 \bar{z}_0 + \bar{a}_0 =$$

$$= a_n \bar{z}_0{}^n + a_{n-1} \bar{z}_0{}^{n-1} + \ldots + a_1 \bar{z}_0 + a_0 = f(\bar{z}_0).$$

5) из (4) получаем, что многочлен $f(z)$ делится на квадратный трехчлен $g(z) = (z - z_0)(z - \bar{z}_0) = z^2 - (z_0 + \bar{z}_0) z + z_0 \cdot \bar{z}_0$ (из условия $z_0 \in \mathbb{C}\backslash\mathbb{R}$ следует, что $z_0 \neq \bar{z}_0$). Но из (2) следует, что $g(z) \in \mathbb{R}[z]$. Теперь предположим, что $\bar{z}_0$ является корнем $f(z)$ кратности k и $k \neq l$. Пусть, например (б.о.о.), $k < l$. Тогда $g^k(z) \in \mathbb{R}[z]$, $f(z) = g^k(z) \cdot h(z)$. Отсюда $h(z)$ — многочлен с действительными коэффициентами, имеющий корень z_0 , но $h(\bar{z}_0) \neq 0$, что противоречит (4).

■

Сопряженные числа очень полезны при нахождении отношений комплексных чисел.

П р и м е р 1. Найдем z_1/z_2 , где $z_1 = a + b \cdot i$, $z_2 = c + d \cdot i \neq 0$.

$$\frac{a + b \cdot i}{c + d \cdot i} = \frac{(a + b \cdot i)(c - d \cdot i)}{(c + d \cdot i)(c - d \cdot i)} = \frac{ac + bd + (bc - ad) \cdot i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} \cdot i.$$

Следующую теорему об алгебраической замкнутости поля комплексных чисел часто называют *основной теоремой теории многочленов* или даже *основной теоремой алгебры.*

Теорема 9.6. *Всякий многочлен с действительными или комплексными коэффициентами, степень которого не меньше единицы, имеет хотя бы один корень, в общем случае, комплексный.*

После Гаусса[12], впервые доказавшего эту теорему в конце XVIII века, было найдено много ее доказательств. Но все они опираются на непрерывность многочленов на множестве действительных или комплексных чисел, т. е. используют топологические свойства $\mathbb{R}$ и $\mathbb{C}$, поэтому доказательство будет приведено только в университетском курсе математического анализа. Мы сформулируем только несколько важных следствий этой теоремы.

Следствие 1. *Любой многочлен степени $n \geqslant 1$ с действительными или комплексными коэффициентами имеет точно n корней (с учетом их кратности).*

Следствие 2. *Любой многочлен $f(z)$ степени $n \geqslant 1$ с действительными или комплексными коэффициентами разложим в произведение линейных множителей $f(z) = a_n(z - z_1)(z - z_2) \cdot \ldots \cdot (z - z_n)$, где a_n — старший коэффициент $f(z)$.*

Эти два следствия легко доказываются по индукции.

Следствие 3. *Любой многочлен $f(z)$ степени $n \geqslant 1$ с действительными коэффициентами разложим в произведение линейных множителей и, может быть, квадратичных трехчленов с отрицательным дискриминантом (линейные множители и квадратные трехчлены в разложении имеют действительные коэффициенты).*

Последнее утверждение сразу следует из основной теоремы алгебры и свойства (4) теоремы 9.5. Надо только заметить, что квадратный трехчлен $g(z) = (z - z_0)(z - \bar{z}_0) = z^2 - (z_0 + \bar{z}_0)z + z_0 \cdot \bar{z}_0$ с действительными коэффициентами и имеет отрицательный дискриминант.

Таким образом, во множестве всех многочленов с действительными коэффициентами, неприводимыми над $\mathbb{R}$ (т. е. неразложимыми на неконстантные множители меньшей степени с коэффициентами из $\mathbb{R}$) являются только

[12]Иоганн Карл Фридрих Гаусс (1777–1855) — немецкий математик, механик, физик, астроном и геодезист. Считается одним из величайших математиков всех времен, «королем математиков». Лауреат медали Копли (1838), иностранный член Шведской (1821) и Российской (1824) Академий наук, английского Королевского общества.

многочлены первой степени и квадратные трехчлены с отрицательным дискриминантом.

Геометрическое и тригонометрическое представления комплексных чисел. Мы уже знаем, что комплексное число можно считать точкой $z = (a, b)$ на координатной плоскости xOy (рис. 30). Такое представление комплексных чисел называют *геометрическим*[13]. При этом представлении действительные числа являются точками оси (Ox), ось (Oy) состоит из чисто мнимых чисел. Начало координат соответствует комплексному числу ноль. Расстояние от $z = (a, b)$ до начала координат называется *модулем* комплексного числа z, и обозначается $|z|$ (очевидно, что $|z| = \sqrt{a^2 + b^2}$).

Пусть $z = (a, b)$ и $z_1 = (c, d)$. Из формул $z + z_1 = (a + c, b + d)$ и $z - z_1 = (a - c, b - d)$ становится ясно, что сумма и разность комплексных чисел соответствует сумме и разности радиус-векторов на координатной плоскости, построенных для точек z и z_1 (напомним, что радиус-вектор точки z — это вектор с началом в точке O и концом в z, он обозначается через $\overrightarrow{Oz}$). Сложение векторов по правилу параллелограмма и неравенство треугольника сразу дают $|z + z_1| \leqslant |z| + |z_1|$. А разность векторов сразу указывает на геометрический смысл неотрицательного действительного числа $|z - z_1|$ — это расстояние между точками z и z_1 на координатной плоскости.

П р и м е р 2. Пусть $r \in \mathbb{R}$, $r > 0$, $z_1, z_2 \in \mathbb{C}$. Что задают на комплексной плоскости следующие уравнения и неравенство: а) $|z - z_1| = r$; б) $|z + z_2| \leqslant r$; в) $|z - z_1| = |z + z_2|$?

Ответы на эти вопросы сразу следуют из геометрического смысла $|z - z_1|$ и наблюдения, что $|z + z_2| = |z - (-z_2)|$.

а) окружность с центром в точке z_1 радиусом r.

б) круг с центром в точке $(-z_2)$ радиусом r.

в) серединный перпендикуляр к отрезку с концами в точках z_1 и $(-z_2)$.

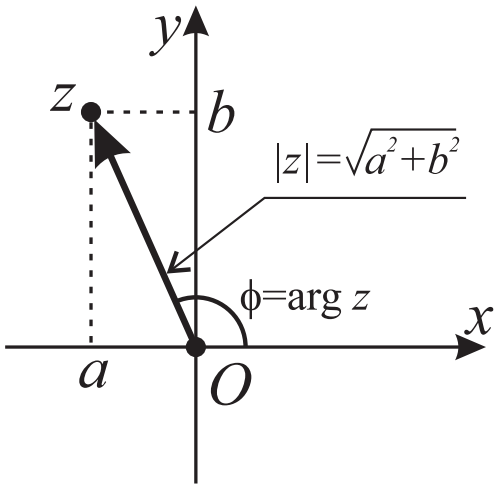

Рис. 30

Аргументом комплексного числа $z \neq 0$ (обозначение: $\arg z$) называется величина угла наклона вектора $\overrightarrow{Oz}$ к положительному направлению оси Ox (рис. 30). Аргумент у комплексного числа определен с точностью

[13]Приоритет геометрической интерпретации комплексных чисел принадлежит К. Весселю. Каспар Вессель (1745–1818) — датско-норвежский математик, землемер по профессии; в работе «Об аналитическом представлении направлений» (1799) дал геометрическое представление комплексных чисел.

до $2\pi k$, где $k \in \mathbb{Z}$ (т.е. φ и $\varphi + 2\pi k$ являются аргументами z при $k \in \mathbb{Z}$). Аргументом нуля принято считать любое число. Нетрудно заметить (рис. 30), что для ненулевого комплексного числа справедливы равенства: $\cos\varphi = a/(\sqrt{a^2+b^2})$, $\sin\varphi = b/(\sqrt{a^2+b^2})$. Отсюда

$$z = a + b\cdot i = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}\cdot i\right) = |z|(\cos\varphi + i\cdot\sin\varphi).$$

Определение. *Тригонометрическим представлением комплексного числа* z *называется запись его в виде* $z = r(\cos\varphi + i\cdot\sin\varphi)$, *где* $r = |z| \geqslant 0$ *и* $\varphi = \arg z$.

Выше было установлено как связаны между собой алгебраическое, геометрическое и тригонометрические представления комплексных чисел. Отметим только, что для $z = 0$ при любом φ справедливо $0 = 0(\cos\varphi + i\cdot\sin\varphi)$ (это тригонометрическая форма записи нуля). Для ненулевых чисел их тригонометрические представления единственны (если считать, что аргумент у комплексного числа определен с точностью до $2\pi k$, где $k \in \mathbb{Z}$). Действительно, приравнивая отдельно действительные части и мнимые части двух представлений

$$z = r\cos\varphi + i\cdot r\sin\varphi = r_1\cos\psi + i\cdot r_1\sin\psi,$$

получим систему: $r\cos\varphi = r_1\cos\psi$, $r\sin\varphi = r_1\sin\psi$. Возводя уравнения в квадрат и складывая соответственно левые и правые части, получим $r^2 = r_1^2$. Отсюда, учитывая $r, r_1 \geqslant 0$, имеем $r = r_1$. Упрощая систему, получим: $\cos\varphi = \cos\psi$, $\sin\varphi = \sin\psi$. Таким образом, углы φ и ψ отличаются на $2\pi k$, где $k \in \mathbb{Z}$.

Тригонометрические представления комплексных чисел позволяют легко находить их произведения, частные, натуральные степени.

Теорема 9.7. *1) пусть* $z = z_1\cdot z_2$. *Тогда верны равенства:* $|z| = |z_1|\cdot|z_2|$ *и* $\arg z = \arg z_1 + \arg z_2$.

2) пусть $z_2 \neq 0$ *и* $z = z_1/z_2$. *Тогда верны равенства:* $|z| = |z_1|/|z_2|$ *и* $\arg z = \arg z_1 - \arg z_2$.

Доказательство. 1) при $z_1 = 0$ или $z_2 = 0$ доказательство очевидно. Пусть $z_1, z_2 \neq 0$ и $z_1 = r_1(\cos\varphi_1 + i\cdot\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\cdot\sin\varphi_2)$ — их тригонометрические представления. Тогда

$$z = z_1\cdot z_2 = r_1r_2\Big((\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i\cdot(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\Big) =$$

$$= r_1 r_2 \Big(\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2) \Big).$$

Откуда и следует требуемое.

2) достаточно уравнение $z = z_1/z_2$ преобразовать к виду $z \cdot z_2 = z_1$ и воспользоваться (1).

■

Из свойства (1) предыдущей теоремы почти сразу получаем формулу Муавра[14] для возведения комплексного числа в натуральную степень.

Следствие 1. *Пусть $z = r(\cos\varphi + i \cdot \sin\varphi)$ — тригонометрическое представление комплексного числа z. Тогда для любого $n \in \mathbb{N}$ выполняется*

$$z^n = r^n(\cos n\varphi + i \cdot \sin n\varphi) \quad (\textbf{\textit{первая формула Муавра}}).$$

Пример 3. Пусть $z = i \cdot \sqrt{3} - 1$. Найти z^{12}. Начнем с тригонометрического представления z. Очевидно, что $|z| = 2$, а аргумент z находится из системы: $\cos\varphi = -1/2$, $\sin\varphi = \sqrt{3}/2$. Отсюда $\varphi = \arg z = 2\pi/3$ и, по формуле Муавра

$$z^{12} = 2^{12}(\cos 8\pi + i \cdot \sin 8\pi) = 2^{12} = 4096.$$

Определение. *Пусть $n \in \mathbb{N}$ и $n \geqslant 2$. Корнем n-ой степени из комплексного числа z называется такое комплексное число w, что $w^n = z$.*

Следствие 2. *Пусть $z = r \in \mathbb{C}$, $z \neq 0$, $z = r(\cos\varphi + i \cdot \sin\varphi)$ — тригонометрическое представление z, $n \in \mathbb{N}\backslash\{1\}$. Существует точно n различных корней n-ой степени из комплексного числа z:*

$$w_k = \sqrt[n]{|z|}\left(\cos\frac{\varphi + 2\pi k}{n} + i \cdot \sin\frac{\varphi + 2\pi k}{n}\right), \quad \textit{где} \quad 0 \leqslant k \leqslant n-1,\ k \in \mathbb{Z}$$

*(**вторая формула Муавра**). Эти числа расположены в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|z|}$ с центром в начале координат.*

Доказательство. Из формулы Муавра сразу получим, что $w_k^n = z$. Проверим, что $w_l \neq w_m$ при $0 \leqslant l < m \leqslant n-1$. Рассуждая от противного, из уравнения $\arg w_m = \arg w_l + 2\pi p$ приходим к $m = l + pn$, что при $p \neq 0$ противоречит неравенству $1 < m < n$.

[14] Абрахам Муавр (1667–1754) — английский математик; француз по происхождению, был в заключении как протестант, после чего эмигрировал в Англию; с 1703 был в дружбе с И. Ньютоном; установил связь между рекуррентными последовательностями и разностными уравнениями.

Докажем теперь, что других корней нет. Пусть $w = r_1(\cos\psi + i\cdot\sin\psi)$ и $w^n = z$. Опять из формулы Муавра получаем $r_1^n = r$ и систему двух тригонометрических уравнений: $\cos n\psi = \cos\varphi$, $\sin n\psi = \sin\varphi$. Из системы получим $n\psi = \varphi + 2\pi s$, $s \in \mathbb{Z}$. Разделим s на n с остатком: $s = nq + k$, где $0 \leqslant k \leqslant n-1$. Тогда $\psi = \dfrac{\varphi + 2\pi k}{n} + 2\pi q$, т.е. $w = w_k$.

Нетрудно заметить, что w_k получается из w_0 поворотом вокруг начала координат на угол $k\cdot\frac{2\pi}{n}$, откуда следует последняя часть утверждения.

■

П р и м е р 4. Найдем все значения $\sqrt{-1}$. Запишем в тригонометрической форме $-1 = 1(\cos\pi + i\cdot\sin\pi)$. Из последнего следствия получаем два возможных значения для $\sqrt{-1}$:

$$\cos\frac{\pi}{2} + i\cdot\sin\frac{\pi}{2} = i,\ \cos\frac{\pi+2\pi}{2} + i\cdot\sin\frac{\pi+2\pi}{2} = -i.$$

П р и м е р 5. Найдем все значения $\sqrt[12]{1}$. Запишем в тригонометрической форме $1 = 1(\cos 0 + i\cdot\sin 0)$. Из последнего следствия получаем двенадцать возможных значений для $\sqrt[12]{1}$, расположенных в вершинах правильного двенадцатиугольника (рис. 31):

$$w_k = \cos\left(k\cdot\frac{\pi}{6}\right) + i\cdot\sin\left(k\cdot\frac{\pi}{6}\right),\ \text{где}\quad 0 \leqslant k \leqslant 11,\ k \in \mathbb{Z}.$$

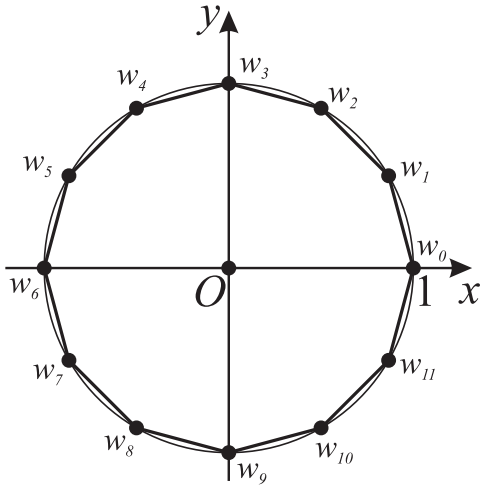

Рис. 31

В заключение параграфа обсудим одно приложение формулы Муавра в тригонометрии. Заметим только, что формула Бинома Ньютона справедлива в любом поле, в том числе, в поле комплексных чисел.

П р и м е р 6. Выведем формулы для $\cos 3\varphi$ и $\sin 3\varphi$, выражающие эти значения через $\cos\varphi$ и $\sin\varphi$. Пусть $z = \cos\varphi + i\cdot\sin\varphi$. Тогда по формулам Муавра и бинома Ньютона, получим (не забудем, что $i^2 = -1$ и $i^3 = -i$, $\sin^2\varphi = 1 - \cos^2\varphi$)

$$\cos 3\varphi + i\cdot\sin 3\varphi = (\cos\varphi + i\cdot\sin\varphi)^3 =$$
$$= \cos^3\varphi + 3i\cdot\cos^2\varphi\sin\varphi - 3\cos\varphi\sin^2\varphi - i\cdot\sin^3\varphi.$$

Приравнивая отдельно действительные и мнимые части, имеем

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi = 4\cos^3\varphi - 3\cos\varphi,$$
$$\sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi = 3\sin\varphi - 4\sin^3\varphi.$$

Глава 4

Тригонометрия

4.1. Определение тригонометрических функций

Из курса геометрии вспомним некоторые понятия и обозначения. В любой плоскости α можно выбрать пару таких векторов $\overrightarrow{i}$ и $\overrightarrow{j}$, что $\overrightarrow{i} \perp \overrightarrow{j}$ и $|\overrightarrow{i}| = |\overrightarrow{j}| = 1$ (пара векторов $\overrightarrow{i}$, $\overrightarrow{j}$ называется *ортонормированным базисом* плоскости α или ОНБ). Также выберем некоторую точку $O \in \alpha$ (она будет называться *началом координат*) и отложим от нее векторы $\overrightarrow{i}$ и $\overrightarrow{j}$: $\overrightarrow{OE_1} = \overrightarrow{i}$ и $\overrightarrow{OE_2} = \overrightarrow{j}$ (рис. 32). На прямой OE_1 вводим порядок $\leqslant_{\overrightarrow{i}}$ с помощью $\overrightarrow{i}$: для любых $A, B \in (OE_1)$ считаем $A \leqslant_{\overrightarrow{i}} B \Leftrightarrow \overrightarrow{AB} \uparrow\uparrow \overrightarrow{i}$. Прямая, с введенным на ней порядком, называется *осью*. Прямые OE_1 и OE_2 с порядками, введенными векторами $\overrightarrow{i}$ и $\overrightarrow{j}$ соответственно, называются *осью абсцисс* и *осью ординат* и обозначаются (Ox) и (Oy). Для любой точки $M \in \alpha$ вектор $\overrightarrow{OM}$ называется *радиус-вектором* точки M (рис. 32). Также из курса геометрии известно, что любой вектор плоскости α единственным образом раскладывается по базису $\overrightarrow{i}$, $\overrightarrow{j}$. Поэтому для $\overrightarrow{OM}$ найдется единственная упорядоченная пара чисел $(x, y) \in \mathbb{R}^2$, что $\overrightarrow{OM} = x \cdot \overrightarrow{i} + y \cdot \overrightarrow{j}$. Пару (x, y) называют *координатами вектора* $\overrightarrow{OM}$ и *координатами*[1] *точки* M и используют обозначения: $\overrightarrow{OM} = (x, y)$ и $M(x, y)$. Так вводится на плоскости *декартова система координат*.

Для окружности с центром в точке O и радиусом $r \geqslant 0$ используем обозначение $\omega = \omega(O, r)$. Через ω_1 обозначаем единичную окружность $\omega(O, 1)$ — она называется *тригонометрической* окружностью. Углом $\angle AOB$ будем называть часть плоскости, ограниченную парой лучей с общей вершиной (рис. 33, закрашенное множество). Пусть $A, B \in \omega_1$, тогда *дугой* AB (на которую опирается угол AOB) называют множество $\overset{\smile}{AB} = \angle AOB \cap \omega_1$.

[1] Как обычно, x называется абсциссой точки M, а число y — ее ординатой.

Ломаной называется объединение отрезков: $z = \cup_{i=1}^{n}[A_iA_{i+1}]$. Вершины, звенья и смежные звенья z определяются очевидным образом. Ломаная z называется *простой*, если ее несмежные звенья не пересекаются, а смежные пересекаются только по общей вершине. Ломаная $z = \cup_{i=1}^{n}[A_iA_{i+1}]$ называется вписанной в $\overset{\smile}{AB}$ (рис. 33), если все вершины этой ломаной лежат на $\overset{\smile}{AB}$ и $A = A_1$, $B = A_{n+1}$ (т. е. концы ломаной совпадают с концами дуги).

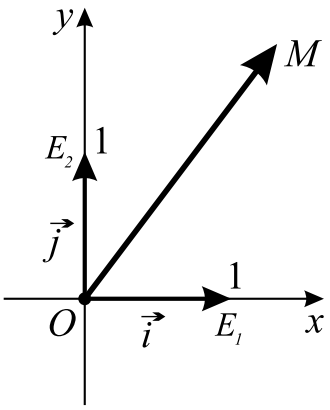

Рис. 32

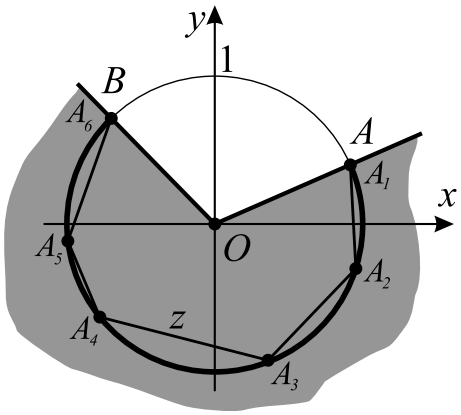

Рис. 33

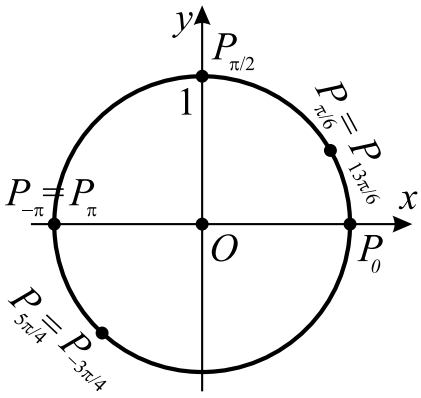

Рис. 34

Определение. *Пусть* $F \subseteq \mathbb{R}$ *и* $F \neq \varnothing$, $a_0 \in \mathbb{R}$. *Число* a_0 *называется верхней границей множества* F , *если* $\forall x \in F \Rightarrow x \leqslant a_0$. *Множество, для которого найдется хотя бы одна верхняя граница, называется ограниченным сверху. Наименьшая из верхних границ* F *называется супремумом этого множества и обозначается* $\sup F$.

П р и м е р 1. Для интервала $F = (1; 2)$ его верхними границами будут 3 , 5 , 7 . Наименьшая из верхних границ равна $\sup F = 2$.

Если во множестве есть наибольший элемент, он будет являться супремумом этого множества. Как видно из предыдущего примера, $\sup F$ не обязан принадлежать F (максимальный и наибольший элементы по определению должны принадлежать этому множеству). В одиннадцатом классе будет доказано, что для любого ограниченного сверху множества найдется супремум и он только один.

Определение. *Длиной дуги* $\overset{\smile}{AB} \subseteq \omega_1$ *называется число* $l(\overset{\smile}{AB}) = \sup\{l(z) :$ z *— простая ломаная, вписанная в дугу* $\overset{\smile}{AB}\}$. *Пусть* $P_0(1, 0)$, $B(-1, 0)$ *и* $\overset{\smile}{P_0B}$ *— дуга* ω_1 , *тогда* $\pi = l(\overset{\smile}{P_0B})$.

Из определения сразу следует, что длина ω_1 равна 2π . Кроме того, отношение длины любой окружности к ее диаметру также равно π . В 1761 году

И. Ламберт[2] доказал иррациональность числа π, а в 1882 году Ф. Линдеман[3] значительно усилил этот результат, доказав трансцендентность[4] π. Первым использовал обозначение π английский математик Уильям Джонс (1675–1749) в 1706, но общепринятым это обозначение стало после работ Л. Эйлера в 1737 году. Будучи иррациональным числом, π является бесконечной непериодической дробью, поэтому практики обречены на использование только приближенных значений этого числа. Архимед, рассматривая правильный 96-угольник, получил два верных знака после запятой. Развитие математического анализа и теории рядов позволили сделать существенный скачок в вычислении π с большой точностью — к концу XIX века были известны уже более пятисот верных знаков после запятой числа π. Современные компьютеры позволяют с помощью нетривиальных математических формул найти $31,4$ триллиона знаков после запятой у числа π. Ниже приведено начало этой грандиозной цепочки:

$$\pi = 3,\,1415926535\,8979323846\,2643383279\,5028841971\,6939937510\ldots$$

Обозначим через $Arc_0 = \{\overset{\smile}{P_0A}\colon A \in \omega_1,\ \overset{\smile}{P_0A} \neq \omega_1\}$ — множество всех дуг с фиксированным концом в точке $P_0 = (1,0)$.

Определение. *Радианным измерением дуг называется такая функция* $g : Arc_0 \to (-2\pi; 2\pi)$, *что для любой дуги* $\overset{\smile}{P_0A} \in Arc_0$ *выполняются два свойства:*

1) $\left|g(\overset{\smile}{P_0A})\right| = l(\overset{\smile}{P_0A})$;

2) $g(\overset{\smile}{P_0A}) \geqslant 0 \Leftrightarrow$ *дуга* $\overset{\smile}{P_0A}$ *отложена от точки* P_0 *в положительном направлении.*

Величиной дуги $\overset{\smile}{P_0A}$ *называется число* $g(\overset{\smile}{P_0A})$ *(или* $g(\overset{\smile}{P_0A})$ *радиан).*

Заметим, что для каждого $x \in (-2\pi; 2\pi)$ найдется единственная точка $P_x \in \omega_1$, что величина дуги $\overset{\smile}{P_0P_x}$ будет равна x радиан (тот факт, что

[2]Иоганн Ламберт (1728–1777) — немецкий математик, физик и астроном; работал над теорией конических сечений; ввел тригонометрические функции синуса и косинуса; составил таблицу первых 1770 простых чисел; занимался теорией перспективы и сферической геометрией; разработал математические основания построения географических карт.

[3]Фердинанд Линдеман (1852–1939) — немецкий математик; основные направления его исследований включали проективную, дифференциальную и алгебраическую геометрии, теорию чисел; был научным руководителем Д. Гильберта; многие годы безуспешно пытался доказать Великую теорему Ферма, обнародовал несколько ошибочных доказательств; доказав трансцендентность числа π, решил одну из трех проблем античности о «квадратуре круга».

[4]Число называется трансцендентным, если оно не является корнем многочлена с целыми коэффициентами. Все трансцендентные числа иррациональны. Число $\sqrt{2}$ является примером иррационального, но не трансцендентного числа.

функция g является биекцией, будет доказан в одиннадцатом классе). Этого уже достаточно для определения тригонометрических функций на интервале $(-2\pi; 2\pi)$, но введем еще одно определение, которое позволит определить синус и косинус на всем множестве $\mathbb{R}$. На рис. 34 отмечены некоторые точки P_x, соответствующие классическим дугам из Arc_0, а также обобщенным дугам.

Определение. *Обобщенной дугой* $\widetilde{P_0A}$ *называется алгебраическое выражение* $k \cdot \psi_0 + \overset{\smile}{P_0A}$, *где* $k \in \mathbb{Z}$, $\overset{\smile}{P_0A} \in Arc_0$ *и* $\psi_0 = \omega_1$ *— полная окружность. Через* $\widetilde{Arc_0}$ *обозначим множество всех обобщенных дуг.*

Смысл целого коэффициента k в предыдущем определении состоит в том, что от точки P_0 мы откладываем $|k|$ раз полную окружность в направлении, которое определено знаком k, а затем откладываем от точки P_0 обычную дугу $\overset{\smile}{P_0A}$.

Замечания. 1) функцию g можно продолжить до функции $\widetilde{g} : \widetilde{Arc_0} \to \mathbb{R}$ следующим образом: на обобщенной дуге $\widetilde{P_0A} = k \cdot \psi_0 + \overset{\smile}{P_0A}$ по определению будем считать, что

$$\widetilde{g}(\widetilde{P_0A}) = 2\pi \cdot k + g(\overset{\smile}{P_0A}).$$

2) для любого $x \in \mathbb{R}$ и $x \geqslant 0$ однозначно найдутся такие два числа $k \in \mathbb{Z}^+$, $x_1 \in [0; 2\pi)$, что $x = 2\pi \cdot k + x_1$ (делим x на 2π с остатком).

3) для любого $x \in \mathbb{R}$ и $x < 0$ однозначно найдутся такие два числа $k \in (\mathbb{Z} \backslash \mathbb{N})$, $x_1 \in (-2\pi; 0]$, что $x = 2\pi \cdot k + x_1$ (для этого меняем знак у x, используем (2) и снова меняем знак).

4) из предыдущих замечаний следует, что для любого $x \in \mathbb{R}$ однозначно найдется такая обобщенная дуга $\widetilde{P_0P_x}$, что $\widetilde{g}(\widetilde{P_0P_x}) = x$. В этом случае будем говорить, что величина $\widetilde{P_0P_x}$ равна x радиан.

Определение. *Для любого* $x \in \mathbb{R}$ *пусть точка* P_x *выбрана на единичной окружности* ω_1 *так, что величина обобщенной дуги* $\widetilde{P_0P_x}$ *равна* x *радиан. Тогда синусом* x *(соответственно косинусом* x*) называется ордината (абсцисса) точки* P_x. *Используем привычные обозначения:* $\sin x$ *и* $\cos x$. *Две оставшиеся основные тригонометрические функции (тангенс и котангенс) определяются так:* $\operatorname{tg} x = \sin x / \cos x$ *и* $\operatorname{ctg} x = \cos x / \sin x$.

4.2. Свойства тригонометрических функций

Применим стандартную схему (см. второй параграф предыдущей главы) для исследования свойств основных тригонометрических функций и построения графиков.

A $f(x) = \sin x$.

I. $D(f) = \mathbb{R}$ — это следует из последнего определения предыдущего параграфа.

II. $E(f) = [-1;1]$, поскольку проекцией ω_1 на ось ординат является отрезок $[-1;1]$.

III. $f(x)$ является нечетной. Свойство (а) $\forall x \in \mathbb{R} \Rightarrow -x \in \mathbb{R}$ очевидно выполняется. Заметим, что при откладывании дуг $\overset{\smile}{P_0P_x}$ и $\overset{\smile}{P_0P_{-x}}$, имеющих одинаковую длину, от одной точки P_0, но в противоположных направлениях, мы получим (рис. 35), что точки P_x и P_{-x} симметричны относительно оси (Ox), поэтому их абсциссы совпадают (т. е. $\cos(-x) = \cos x$), а ординаты отличаются только знаком, что дает $\sin(-x) = -\sin x$.

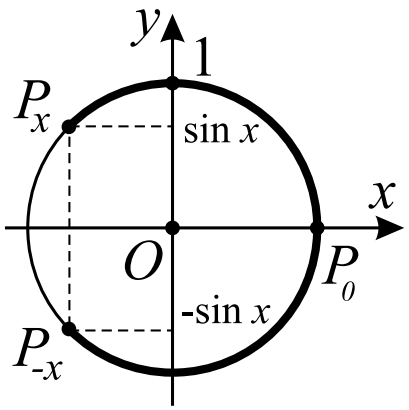

Рис. 35

IV. Функция $f(x)$ является периодической, причем $T = 2\pi$ — ее основной период. Очевидно, что $\forall x \in \mathbb{R} \Rightarrow x \pm 2\pi \in \mathbb{R}$, поэтому свойство (а) определения выполняется. Кроме того, точки P_x и $P_{x+2\pi}$ на единичной окружности совпадают, поэтому имеют одинаковые первые и вторые координаты, что дает $\cos(x+2\pi) = \cos x$ и $\sin(x+2\pi) = \sin x$. Осталось показать, что любое число $T^* \in (0;2\pi)$ периодом $f(x)$ не будет. Заметим, что точка $P_{T^*+\pi/2}$ не совпадает с точкой $P_{\pi/2}$ — единственной точкой ω_1, у которой вторая координата равна 1. Поэтому $\sin(T^*+\pi/2) < 1 = \sin(\pi/2)$. Таким образом, $T^* \in (0;2\pi)$ периодом $f(x)$ не будет.

V. У точки P_0 координаты равны $(1,0)$, поэтому $\cos 0 = 1$ и $\sin 0 = 0$ и точкой пересечения $\Gamma(f)$ с осью (Oy) будет начало координат — точка $O(0,0)$. На ω_1 только точки $P_{\pi\cdot k}$ при $k \in \mathbb{Z}$ имеют нулевую вторую координату, поэтому $\sin x = 0 \Leftrightarrow x = \pi k$ при $k \in \mathbb{Z}$ и точки пересечения $\Gamma(f)$ с осью (Ox) будут иметь вид $(\pi k, 0)$ при $k \in \mathbb{Z}$.

VI. Легко определяется множество точек ω_1 с положительной второй координатой — верхняя открытая (т. е. без концевых точек) полуокружность. С учетом периода получим, что $\sin x > 0 \Leftrightarrow x \in (2\pi k; \pi + 2\pi k)$ при $k \in \mathbb{Z}$. Аналогично $\sin x < 0 \Leftrightarrow x \in (-\pi + 2\pi k; 2\pi k)$ при $k \in \mathbb{Z}$.

VII. Нетрудно заметить, что $\sin x$ строго возрастает на отрезке $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$ и строго убывает на отрезке $[\pi/2; 3\pi/2]$. С учетом периода получим, что
1) $f(x)\nearrow$ на каждом отрезке $[(-\pi/2) + 2\pi k; (\pi/2) + 2\pi k]$ при $k \in \mathbb{Z}$;
2) $f(x)\searrow$ на каждом отрезке $[(\pi/2) + 2\pi k; (3\pi/2) + 2\pi k]$ при $k \in \mathbb{Z}$.

VIII. Точками максимума $f(x)$ будут все точки вида $(\pi/2) + 2\pi k$ при $k \in \mathbb{Z}$; значение функции во всех этих точках равны 1. Точками минимума $f(x)$ будут все точки вида $(-\pi/2) + 2\pi k$ при $k \in \mathbb{Z}$; значение функции во всех этих точках равны -1.

IX. Асимптот у $f(x)$ нет.

X. С учетом основного периода, достаточно построить график функции $f(x) = \sin x$ на отрезке $[0; 2\pi]$.

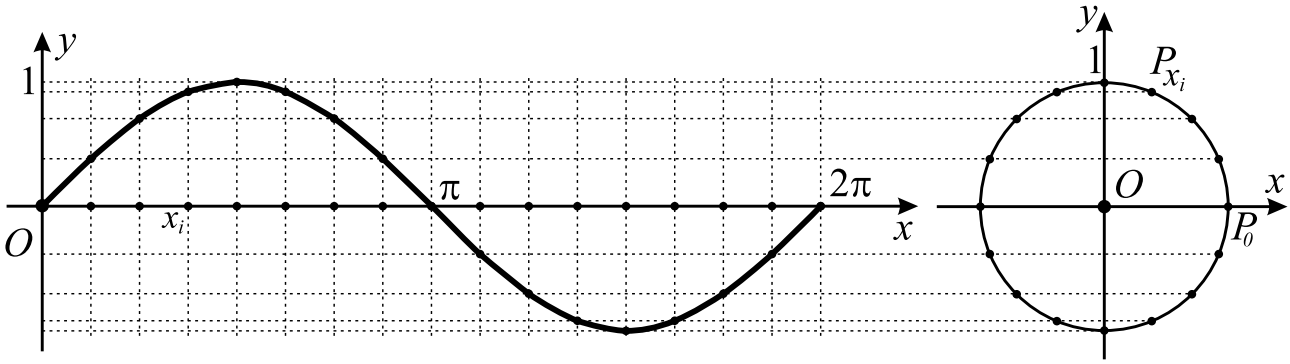

Рис. 36

Разделим отрезок $[0; 2\pi]$ и окружность ω_1 на 2^n равных частей, $n \in \mathbb{N}$. Это легко сделать с помощью циркуля и линейки, строя серединные перпендикуляры или биссектрисы углов (на рис. 36 отрезок и окружность делим на 16 частей, т. е. $n = 4$). Получим числа $0 = x_0 < x_1 < \ldots < x_{2^n} = 2\pi$ и точки $P_0 = P_{x_0}$, $P_{x_1}, \ldots, P_{x_{2^n}}$ на ω_1. Поскольку длина ω_1 равна 2π (что совпадает с длиной отрезка $[0; 2\pi]$), и деление окружности и отрезка происходило на одинаковое количество равных частей, длина дуги $\overset{\smile}{P_0 P_{x_i}}$ будет равна x_i. По определению синуса имеем, что значение $\sin x_i$ будет равно ординате точки P_{x_i}. Проводя горизонтальные и вертикальные прямые, на их пересечении получим 2^n точек, лежащих на графике функции $f(x) = \sin x$. Соединив эти точки кривыми, получи эскиз части $\Gamma(\sin x)$. Увеличивая n,

можно добиться высокой точности построения $\Gamma(\sin x)$. Далее, учитывая период $T = 2\pi$, остается «размножить» построенный участок на всю числовую прямую.

В $g(x) = \cos x$.

Исследование свойств $g(x)$ аналогично исследованию $f(x) = \sin x$, за исключением следующих моментов. Функция $g(x)$ четна (установлено выше). При доказательстве того, что $T = 2\pi$ является основным периодом $g(x)$ вместо точки $P_{\pi/2}$ необходимо выбрать точку P_0 — единственную точку единичной окружности ω_1, у которой первая координата равна 1. В следующем параграфе будет доказана простая формула приведения, связывающая $f(x)$ и $g(x)$: $\forall x \in \mathbb{R} \Rightarrow \cos x = \sin(x + \pi/2)$. Поэтому нули функции $g(x) = \cos x$, точки пересечения $\Gamma(g)$ с (Ox), промежутки монотонности $g(x)$, точки экстремума и график $\Gamma(\cos x)$ получаются сдвигом **влево** на $\pi/2$ из соответствующих объектов функции $f(x) = \sin x$. Точка пересечения $\Gamma(\cos x)$ с осью (Oy) имеет координаты $(0, 1)$, поскольку $\cos 0 = 1$.

Перед разбором свойств тангенса введем понятие *оси тангенсов* и поймем, почему она так называется.

Определение. *Прямая a, задающаяся уравнением $x = 1$, называется осью тангенсов.*

Теорема 2.1. *Пусть a — ось тангенсов и для любого $x \in (-\pi/2; \pi/2)$ точка $P_x \in \omega_1$ выбрана так, что величина дуги $\overset{\smile}{P_0P_x}$ равна x радианам. Если точка T_x является пересечением луча $[OP_x)$ с прямой a, то вторая координата точки T_x равна $\operatorname{tg} x$.*

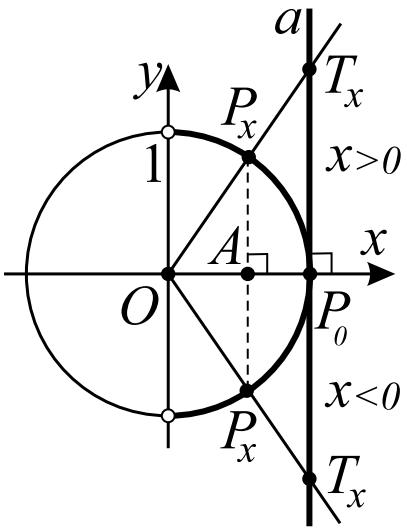

Рис. 37

Доказательство. Если $x = 0$, то $T_0 = P_0$ и ордината точки T_0 равна $0 = \sin 0 / \cos 0$, поэтому далее считаем, что $x \neq 0$.

1-й случай: $x \in (0; \pi/2)$. Пусть $A = \operatorname{Пр}_{(Ox)}(P_x)$ — проекция точки P_x на ось абсцисс (рис. 37). Тогда прямоугольные треугольники OAP_x и OP_0T_x подобны между собой, откуда

$$T_xP_0 = \frac{T_xP_0}{1} = \frac{P_xA}{OA} = \frac{\sin x}{\cos x} = \operatorname{tg} x.$$

2-й случай: $x \in (-\pi/2; 0)$. Прямоугольные треугольники OAP_x и OP_0T_x также подобны между собой, но учтем, что для длин сторон этих треугольников выполняются другие соотношения: $P_xA = -\sin x$ и T_xP_0 — это вторая координата точки T_x, взятая со знаком минус. Отсюда

$$-T_xP_0 = \frac{-T_xP_0}{1} = \frac{-P_xA}{OA} = \frac{\sin x}{\cos x} = \operatorname{tg} x.$$

■

C $h(x) = \operatorname{tg} x$.

I. $D(h) = \mathbb{R}\setminus\left\{\frac{\pi}{2} + \pi k : k \in \mathbb{Z}\right\}$. По определению частного двух функций, необходимо исключить нули знаменателя: $\cos x = 0 \Leftrightarrow x = \frac{\pi}{2} + \pi k$ где $k \in \mathbb{Z}$.

II. $E(h) = \mathbb{R}$. Следует из предыдущей теоремы, поскольку для любого $y \in \mathbb{R}$ на оси тангенсов можно найти точку T, у которой вторая координата равна y. Пересекая луч $[OT)$ с ω_1, найдем P_x, тогда по теореме 2.1 получим $\operatorname{tg} x = y$.

III. Функция $h(x)$ является отношением нечетной и четной функции, поэтому нечетна по теореме 2.1 предыдущей главы.

IV. Докажем, что $T = \pi$ является основным периодом $h(x)$. Из I следует, что $\forall x \in D(h) \Rightarrow x \pm \pi \in D(h)$, поэтому свойство (а) определения периода функции выполняется, проверим (б). Точки P_x и $P_{x+\pi}$ делят ω_1 на две равных дуги, поэтому они симметричны относительно центра этой окружности — начала координат. Таким образом, координаты этих точек равны по модулю и противоположны по знаку, т. е. $\sin(x+\pi) = -\sin x$ и $\cos(x+\pi) = -\cos x$. Отсюда $\operatorname{tg}(x+\pi) = (-\sin x)/(-\cos x) = \operatorname{tg} x$ для всех $x \in D(h)$.

Осталось доказать, что любое число $T^* \in (0; \pi)$ не является периодом $h(x)$. Предположив противное, подставим в функцию $x = 0$:

$$0 = \operatorname{tg}(0) = \operatorname{tg}(0 + T^*) = \operatorname{tg} T^* \neq 0.$$

Последнее неравенство следует из того, что точка P_{T^*} имеет ненулевую ординату. ↯.

V. Поскольку $\operatorname{tg} 0 = 0$, $(0, 0) \in \Gamma(h)$. Уравнение $\operatorname{tg} x = 0$ равносильно уравнению $\sin x = 0$, поэтому $\Gamma(h)$ пересекает ось абсцисс в точках множества $\{\pi k : k \in \mathbb{Z}\}$.

VI. Из теоремы 2.1 и периодичности $h(x)$ следует, что
1) $\operatorname{tg} x > 0 \Leftrightarrow x \in \left(\pi k; \frac{\pi}{2} + \pi k\right)$, где $k \in \mathbb{Z}$;
2) $\operatorname{tg} x < 0 \Leftrightarrow x \in \left(-\frac{\pi}{2} + \pi k; \pi k\right)$, где $k \in \mathbb{Z}$.

VII. Из теоремы 2.1 и периодичности $h(x)$ следует, что $\operatorname{tg} x \nearrow$ на каждом промежутке $\left(-\frac{\pi}{2} + \pi k; \frac{\pi}{2} + \pi k\right)$, где $k \in \mathbb{Z}$.

VIII. Точек экстремума у тангенса нет, поскольку каждая точка области определения попадает в один из интервалов строгой монотонности, поэтому она не может быть ни точкой максимума, ни точкой минимума.

IX. Функция $h(x)$ имеет счетное число вертикальных асимптот, которые задаются формулами $x = \frac{\pi}{2} + \pi k$, где $k \in \mathbb{Z}$ (при приближении аргумента к этим точкам косинус стремится к нулю, а $|\sin x|$ стремится к единице). Других асимптот у тангенса нет.

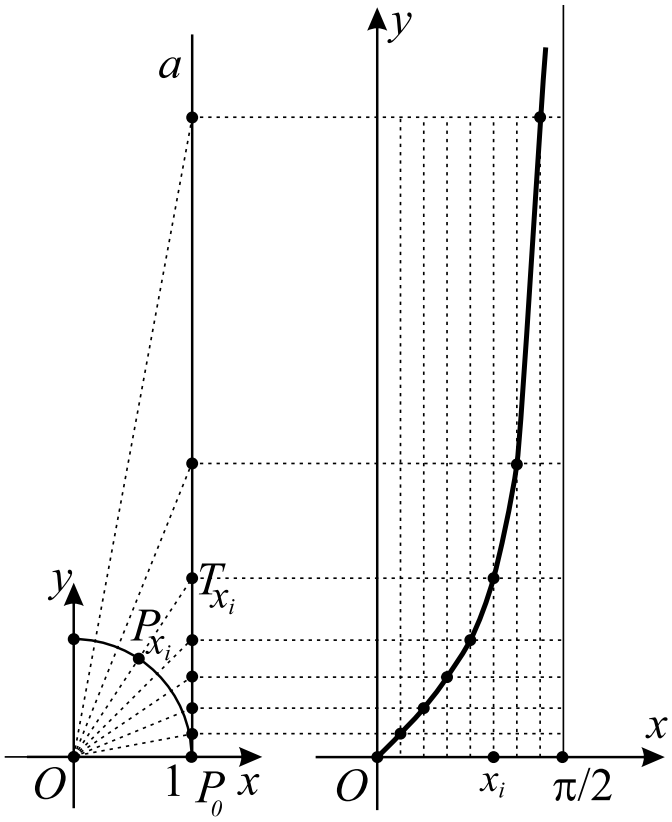

Рис. 38

X. Учитывая, что $T = \pi$ является периодом тангенса, достаточно построить $\Gamma(h)$ на интервале длины π, например, на промежутке $(-\pi/2; \pi/2)$. Воспользуемся еще нечетностью тангенса и построим график $\Gamma(h)$ только на полуинтервале $[0; \pi/2)$. Этого будет достаточно, поскольку останется отобразить построенный кусок относительно начала координат, и, получив график $\Gamma(h)$ на интервале $(-\pi/2; \pi/2)$, размножить его параллельными переносами на всю область определения.

Разделим полуинтервал $[0; \pi/2)$ и первую четверть окружности ω_1 на 2^n равных частей, $n \in \mathbb{N}$ (на рис. 38 полуинтервал и дугу делим на 8 частей, т. е. $n = 3$). Получим числа $0 = x_0 < x_1 < \ldots < x_{2^n} = \pi/2$ и точки $P_0 = P_{x_0}$, $P_{x_1}, \ldots, P_{x_{2^n}}$ на ω_1. Поскольку длина четверти окружности ω_1 равна $\pi/2$

(что совпадает с длиной полуинтервала $[0;\pi/2)$), и деление окружности и отрезка происходило на одинаковое количество равных частей, длина дуги $\overset{\smile}{P_0P_{x_i}}$ будет равна x_i. Далее проведем лучи $[OP_{x_i})$ через все точки, кроме последней и пересечем их с осью тангенсов. Найдем точки T_{x_i}, ординаты которых по теореме 2.1 будут равны $\operatorname{tg} x_i$. Проводя горизонтальные и вертикальные прямые, на их пересечении получим 2^n-1 точек, лежащих на графике функции $h(x)=\operatorname{tg} x$. Соединив эти точки кривыми, получим эскиз достаточной части $\Gamma(\operatorname{tg} x)$.

D $p(x)=\operatorname{ctg} x$**.**

В следующем параграфе будет доказана формула приведения, связывающая $\operatorname{tg} x$ и $\operatorname{ctg} x$: $\forall x\in\mathbb{R}\Rightarrow \operatorname{ctg} x=-\operatorname{tg}(x+\pi/2)$. Поэтому нули функции $p(x)=\operatorname{ctg} x$, точки пересечения $\Gamma(p)$ с (Ox), асимптоты $p(x)$ получаются сдвигом **влево** на $\pi/2$ из соответствующих объектов функции $h(x)=\operatorname{tg} x$. График $\Gamma(\operatorname{ctg} x)$ получается из $\Gamma(\operatorname{tg} x)$ композицией двух движений плоскости: параллельного переноса **влево** на $\pi/2$ и симметрии относительно оси (Ox). Присутствие минуса в формуле приведения также скажется на характере монотонности: $\operatorname{ctg} x\searrow$ на каждом промежутке $(\pi k;\pi+\pi k)$, для произвольного $k\in\mathbb{Z}$.

4.3. Формулы сложения

Тригонометрические формулы обычно имеют вид $f(x)=g(x)$. Мы ясно понимаем, что перед нами не стоит задача нахождения корней этого уравнения, а нам необходимо доказать, что это равенство справедливо на некотором множестве M (часто используют термин тригонометрическое *тождество* или тождество на множестве M и обозначают $f\equiv g$ или $f\overset{M}{\equiv}g$). Применение тригонометрических формул (тождеств) понятно: в уравнении, неравенстве или системе мы заменяем $f(x)$ на $g(x)$. Но во время таких замен нас могут ждать сюрпризы. Поэтому сразу обсудим основные типы формул и возможность их безопасного применения. Будем использовать обозначения: $X=D(f)$ и $Y=D(g)$.

Формулы типа **A**: $X=Y$ и для любых $x\in X\Rightarrow f(x)=g(x)$. Это лучшие из формул, их можно смело использовать в решении задач, переходя к равносильным[5] уравнениям, неравенствам или системам.

[5] Т. е. с тем же самым множеством решений.

Формулы типа **B**: $X = Y \cup Z$, $Y \cap Z = \varnothing$, $Z \neq \varnothing$ и для любых $x \in Y$ следует, что $f(x) = g(x)$. При замене $f(x)$ на $g(x)$ у исходного уравнения (или неравенства) могут быть потеряны корни, если они входят во множество Z. Справиться с этой проблемой несложно: достаточно все числа из множества Z (обычно это одна или несколько серий) подставить в исходное уравнение (или неравенство). При обратной замене — $g(x)$ на $f(x)$ — произойдет расширения ОДЗ как раз на множество Z, за счет него могут появиться посторонние корни. Эта проблема решается еще проще: все серии решений из множества Z необходимо отбросить, поскольку они не входят в ОДЗ исходной задачи.

Формулы типа **C**: неверные формулы. Это тождества, которые не выполняются на множестве $X \cap Y$. Примерами таких формул будет популярная в геометрии формула $\cos x = \sqrt{1 - \sin^2 x}$ или неудачная попытка ее исправить: $\cos x = \pm\sqrt{1 - \sin^2 x}$ (в первом случае почему-то считают, что $\cos x$ всегда неотрицателен, во втором — что он неоднозначен). Внимательный читатель сможет разбить $\mathbb{R}$ на промежутки и написать на каждом из них формулу типа A, связывающую синус и косинус из основного тригонометрического тождества.

Далее будем указывать номер и тип формулы, а в случае формулы типа B — дополнительно указывать область определения левой части (D (л.ч.)) и область определения правой части (D (п.ч.)). Формулы типа C изучаться не будут.

Соотношение, доказанное в следующей теореме, называют *основным тригонометрическим тождеством.*

Теорема 3.1. *Для каждого* $x \in \mathbb{R} \Rightarrow$ $\cos^2 x + \sin^2 x = 1$, *(1),* $\boxed{A}$.

Доказательство. Используем обозначения рис. 37, считая, что $x \in \mathbb{R}$. Из прямоугольного треугольника OAP_x получим:

$$1 = OP_x^2 = OA^2 + AP_x^2 = \cos^2 x + \sin^2 x.$$

■

Следствие. *1)* $1 + \operatorname{tg}^2 x = \dfrac{1}{\cos^2 x}$, *(2),* $\boxed{A}$.

2) $1 + \operatorname{ctg}^2 x = \dfrac{1}{\sin^2 x}$, *(3),* $\boxed{A}$.

Доказательство. 1) $1 + \operatorname{tg}^2 x = \dfrac{\cos^2 x + \sin^2 x}{\cos^2 x} = \dfrac{1}{\cos^2 x}$.

2) аналогично (1).

■

Замечание. Далее вместо переменных x, y используем привычные для тригонометрии α и β.

Теорема 3.2. $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$, *(4)*, $\boxed{A}$.

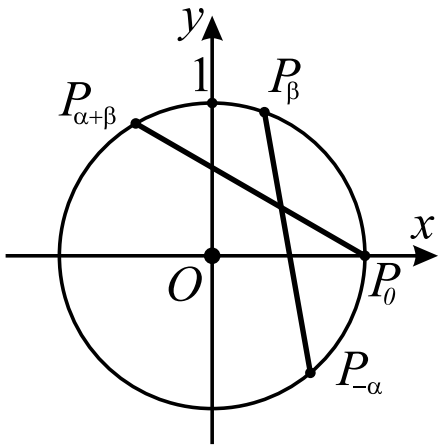

Рис. 39

Доказательство. Рассмотрим на ω_1 четыре точки (рис. 39): $P_0(1,0)$, $P_\beta(\cos\beta, \sin\beta)$, $P_{\alpha+\beta}(\cos(\alpha+\beta), \sin(\alpha+\beta))$ и $P_{-\alpha}(\cos\alpha, -\sin\alpha)$. В нахождении координат последней точки воспользовались четностью косинуса и нечетностью синуса: $\cos(-\alpha) = \cos\alpha$ и $\sin(-\alpha) = -\sin\alpha$. Теперь заметим, что при повороте вокруг начала координат на угол α будет выполняться: $R^\alpha_O(P_{-\alpha}) = P_0$ и $R^\alpha_O(P_\beta) = P_{\alpha+\beta}$. При повороте, как и при любом движении плоскости, расстояние между точками сохраняется, поэтому $|P_0P_{\alpha+\beta}| = |P_{-\alpha}P_\beta|$. Возведем обе части последнего уравнения в квадрат и воспользуемся формулой расстояния между точками в декартовой системе координат:

$$\Big(\cos(\alpha+\beta)-1\Big)^2 + \Big(\sin(\alpha+\beta)-0\Big)^2 = (\cos\beta-\cos\alpha)^2 + (\sin\beta+\sin\alpha)^2 \Leftrightarrow$$

$$\cos^2(\alpha+\beta) + \sin^2(\alpha+\beta) + 1 - 2\cos(\alpha+\beta) =$$

$$= \cos^2\beta + \sin^2\beta + \cos^2\alpha + \sin^2\alpha - 2\cos\alpha\cos\beta + 2\sin\alpha\sin\beta.$$

Трижды воспользуемся формулой (1), затем вычитаем двойку из обеих частей и, наконец, делим обе части на -2. Неизбежно приходим к тому, что $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$.

■

Следствие 1. $\cos(\alpha-\beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta$, *(5)*, $\boxed{A}$.

Доказательство. По формуле (4), используя четность косинуса и нечетность синуса, получим

$$\cos\Big(\alpha+(-\beta)\Big) = \cos\alpha\cos(-\beta) - \sin\alpha\sin(-\beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta.$$

■

Следствие 2. *1)* $\cos\left(\alpha+\dfrac{\pi}{2}\right)=-\sin\alpha$, *(6),* $\boxed{A}$.

2) $\cos\left(\alpha-\dfrac{\pi}{2}\right)=\sin\alpha$, *(7),* $\boxed{A}$.

3) $\sin\left(\beta+\dfrac{\pi}{2}\right)=\cos\beta$, *(8),* $\boxed{A}$.

4) $\sin\left(\beta-\dfrac{\pi}{2}\right)=-\cos\beta$, *(9),* $\boxed{A}$.

Доказательство. 1) воспользуемся формулой (4) и получим

$$\cos\left(\alpha+\frac{\pi}{2}\right)=\cos\alpha\cos\frac{\pi}{2}-\sin\alpha\sin\frac{\pi}{2}=-\sin\alpha.$$

2) аналогично предыдущей формуле, только используем (5).

3) пусть $\alpha=\beta+\pi/2$, отсюда $\beta=\alpha-\pi/2$ и из (7) получим, что $\cos\beta=\cos(\alpha-\pi/2)=\sin\alpha=\sin(\beta+\pi/2)$.

4) аналогично предыдущей формуле, только $\alpha=\beta-\pi/2$ и используем формулу (6).

■

Следствие 3. *1)* $\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta$, *(10),* $\boxed{A}$.
2) $\sin(\alpha-\beta)=\sin\alpha\cos\beta-\cos\alpha\sin\beta$, *(11),* $\boxed{A}$.

Доказательство. 1) используем формулы (7), (4), снова (7) и (9):

$$\sin(\alpha+\beta)=\cos\left(\alpha+\beta-\frac{\pi}{2}\right)=\cos\alpha\cos\left(\beta-\frac{\pi}{2}\right)-\sin\alpha\sin\left(\beta-\frac{\pi}{2}\right)=$$

$$=\sin\alpha\cos\beta+\cos\alpha\sin\beta.$$

2) аналогично доказательству предыдущей формулы.

■

Следствие 4. *1)* $\operatorname{tg}(\alpha+\beta)=\dfrac{\operatorname{tg}\alpha+\operatorname{tg}\beta}{1-\operatorname{tg}\alpha\operatorname{tg}\beta}$, *(12),* $\boxed{B}$,

D (л.ч.): $\alpha+\beta\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$; *D (п.ч.):* $\alpha+\beta\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$, $\alpha\neq\frac{\pi}{2}+\pi l$, $l\in\mathbb{Z}$, $\beta\neq\frac{\pi}{2}+\pi m$, $m\in\mathbb{Z}$.

2) $\operatorname{tg}(\alpha-\beta)=\dfrac{\operatorname{tg}\alpha-\operatorname{tg}\beta}{1+\operatorname{tg}\alpha\operatorname{tg}\beta}$, *(13),* $\boxed{B}$, *D (л.ч.):* $\alpha-\beta\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$;

D (п.ч.): $\alpha-\beta\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$, $\alpha\neq\frac{\pi}{2}+\pi l$, $l\in\mathbb{Z}$, $\beta\neq\frac{\pi}{2}+\pi m$, $m\in\mathbb{Z}$.

Доказательство. 1) расписываем тангенс по определению, затем применяем формулы (10) и (4) и в последнем переходе делим числитель и знаме-

натель на произведение $\cos\alpha\cos\beta$ (из-за чего и появляются новые ограничения):

$$\operatorname{tg}(\alpha+\beta)=\frac{\sin(\alpha+\beta)}{\cos(\alpha+\beta)}=\frac{\sin\alpha\cos\beta+\cos\alpha\sin\beta}{\cos\alpha\cos\beta-\sin\alpha\sin\beta}=\frac{\operatorname{tg}\alpha+\operatorname{tg}\beta}{1-\operatorname{tg}\alpha\operatorname{tg}\beta}\,.$$

2) аналогично доказательству предыдущей формулы, только с применение формул (11) и (5).

■

Следствие 5. *1)* $\operatorname{ctg}(\alpha+\beta)=\dfrac{\operatorname{ctg}\alpha\operatorname{ctg}\beta-1}{\operatorname{ctg}\alpha+\operatorname{ctg}\beta}$, *(14),* $\boxed{B}$,

D (л.ч.): $\alpha+\beta\neq\pi k$, $k\in\mathbb{Z}$; *D (п.ч.):* $\alpha+\beta\neq\pi k$, $k\in\mathbb{Z}$, $\alpha\neq\pi l$, $l\in\mathbb{Z}$, $\beta\neq\pi m$, $m\in\mathbb{Z}$.

2) $\operatorname{ctg}(\alpha-\beta)=\dfrac{\operatorname{ctg}\alpha\operatorname{ctg}\beta+1}{\operatorname{ctg}\beta-\operatorname{ctg}\alpha}$, *(15),* $\boxed{B}$, *D (л.ч.):* $\alpha-\beta\neq\pi k$, $k\in\mathbb{Z}$;

D (п.ч.): $\alpha-\beta\neq\pi k$, $k\in\mathbb{Z}$, $\alpha\neq\pi l$, $l\in\mathbb{Z}$, $\beta\neq\pi m$, $m\in\mathbb{Z}$.

Доказательство. 1) расписываем котангенс по определению, затем применяем формулы (4) и (10) и в последнем переходе делим числитель и знаменатель на произведение $\sin\alpha\sin\beta$ (из-за чего и появляются новые ограничения):

$$\operatorname{ctg}(\alpha+\beta)=\frac{\cos(\alpha+\beta)}{\sin(\alpha+\beta)}=\frac{\cos\alpha\cos\beta-\sin\alpha\sin\beta}{\sin\alpha\cos\beta+\cos\alpha\sin\beta}=\frac{\operatorname{ctg}\alpha\operatorname{ctg}\beta-1}{\operatorname{ctg}\alpha+\operatorname{ctg}\beta}\,.$$

2) аналогично доказательству предыдущей формулы, только с применение формул (5) и (11).

■

Формулы, доказанные в следующем утверждении, называются *формулами приведения.*

Следствие 6. *Пусть* $k\in\mathbb{Z}$, *тогда*

$$\textit{1)}\ \sin\left(\alpha+\frac{\pi}{2}\cdot k\right)=\begin{cases}\sin\alpha, & k\equiv 0 \pmod 4 & (16),\ \boxed{A},\\ \cos\alpha, & k\equiv 1 \pmod 4 & (17),\ \boxed{A},\\ -\sin\alpha, & k\equiv 2 \pmod 4 & (18),\ \boxed{A},\\ -\cos\alpha, & k\equiv 3 \pmod 4 & (19),\ \boxed{A}.\end{cases}$$

$$2)\cos\left(\alpha+\frac{\pi}{2}\cdot k\right)=\begin{cases}\cos\alpha, & k\equiv 0 \pmod 4 & (20),\ \boxed{A},\\ -\sin\alpha, & k\equiv 1 \pmod 4 & (21),\ \boxed{A},\\ -\cos\alpha, & k\equiv 2 \pmod 4 & (22),\ \boxed{A},\\ \sin\alpha, & k\equiv 3 \pmod 4 & (23),\ \boxed{A}.\end{cases}$$

$$3)\operatorname{tg}\left(\alpha+\frac{\pi}{2}\cdot k\right)=\begin{cases}\operatorname{tg}\alpha, & k\equiv 0 \pmod 2 & (24),\ \boxed{A},\\ -\operatorname{ctg}\alpha, & k\equiv 1 \pmod 2 & (25),\ \boxed{A}.\end{cases}$$

$$4)\operatorname{ctg}\left(\alpha+\frac{\pi}{2}\cdot k\right)=\begin{cases}\operatorname{ctg}\alpha, & k\equiv 0 \pmod 2 & (26),\ \boxed{A},\\ -\operatorname{tg}\alpha, & k\equiv 1 \pmod 2 & (27),\ \boxed{A}.\end{cases}$$

Доказательство. 1) разделим k на 4 с остатком ($k=4p+i$, где $i\in\{0,1,2,3\}$), воспользуемся формулой (10) и тем, что $2\pi p$ является периодом $\sin x$ и $\cos x$ или равно нулю:

$$\sin\left(\alpha+\frac{\pi}{2}\cdot k\right)=\sin\alpha\cos\left(2\pi p+\frac{\pi}{2}\cdot i\right)+\cos\alpha\sin\left(2\pi p+\frac{\pi}{2}\cdot i\right)=$$

$$=\sin\alpha\cos\left(\frac{\pi}{2}\cdot i\right)+\cos\alpha\sin\left(\frac{\pi}{2}\cdot i\right)=\begin{cases}(\sin\alpha)\cdot 1+(\cos\alpha)\cdot 0, & i=0,\\ (\sin\alpha)\cdot 0+(\cos\alpha)\cdot 1, & i=1,\\ (\sin\alpha)\cdot(-1)+(\cos\alpha)\cdot 0, & i=2,\\ (\sin\alpha)\cdot 0+(\cos\alpha)\cdot(-1), & i=3.\end{cases}$$

2) доказывается аналогично предыдущему утверждению.

3) расписываем тангенс по определению, а также применяем формулы двух предыдущих утверждений:

$$\operatorname{tg}\left(\alpha+\frac{\pi}{2}\cdot k\right)=\frac{\sin\left(\alpha+\frac{\pi}{2}\cdot k\right)}{\cos\left(\alpha+\frac{\pi}{2}\cdot k\right)}=\begin{cases}\operatorname{tg}\alpha, & k\equiv 0 \pmod 2,\\ -\operatorname{ctg}\alpha, & k\equiv 1 \pmod 2.\end{cases}$$

4) доказывается аналогично предыдущему утверждению.

■

Замечание. Существует правило чтобы запомнить результат формул приведения. Для его формулировки договоримся функции в каждой паре $\{\sin x,\cos x\}$ и $\{\operatorname{tg}x,\operatorname{ctg}x\}$ называть сходственными. Для преобразования $f\left(\alpha+\frac{\pi}{2}\cdot k\right)$ достаточно:

1) сохранить f, если k — четное; изменить f на сходственную, если k — нечетное целое число;

2) знак результата совпадает со знаком числа $f\left(\frac{\pi}{4}+\frac{\pi}{2}\cdot k\right)$.

П р и м е р 1. Преобразуем, используя последнее замечание, выражение $\sin\left(x+\dfrac{15\pi}{2}\right)$. Заметим, что $k=15$ — нечетное число, поэтому меняем $\sin$ на $\cos$. Знак результата совпадает со знаком исходной функции в точке $\dfrac{\pi}{4}+\dfrac{15\pi}{2}=7\pi+3\pi/4$ — угол из четвертой четверти, внутри которой $\sin$ отрицателен. В результате

$$\sin\left(x+\frac{15\pi}{2}\right)=-\cos x.$$

4.4. Формулы двойного и половинного аргументов

Продолжим нумерацию следствий теоремы 3.2.

Следствие 7. $\sin 2\alpha=2\sin\alpha\cos\alpha$, *(28)*, $\boxed{A}$.

Доказательство. Заметим, что $\sin 2\alpha=\sin(\alpha+\alpha)$ и достаточно применить формулу (10).

■

Следствие 8. *1)* $\cos 2\alpha=\cos^2\alpha-\sin^2\alpha$, *(29)*, $\boxed{A}$.

2) $\cos 2\alpha=2\cos^2\alpha-1$, *(30)*, $\boxed{A}$.

3) $\cos 2\alpha=1-2\sin^2\alpha$, *(31)*, $\boxed{A}$.

Доказательство. Заметим, что $\cos 2\alpha=\cos(\alpha+\alpha)$ и достаточно применить формулу (4). Формулы (30) и (31) выводятся из основного тригонометрического тождества и (29).

■

Следствие 9. $\operatorname{tg}2\alpha=\dfrac{2\operatorname{tg}\alpha}{1-\operatorname{tg}^2\alpha}$, *(32)*, $\boxed{B}$, *D (л.ч.):* $\alpha\neq\frac{\pi}{4}+\frac{\pi k}{2}$, $k\in\mathbb{Z}$; *D (п.ч.):* $\alpha\neq\frac{\pi}{4}+\frac{\pi k}{2}$, $k\in\mathbb{Z}$, $\alpha\neq\frac{\pi}{2}+\pi l$, $l\in\mathbb{Z}$.

Доказательство. Расписываем тангенс по определению, применяем формулы (28) и (29), а в последнем переходе делим числитель и знаменатель дроби на $\cos^2\alpha$ (из-за $\cos^2\alpha\neq 0$ появляются новые ограничения на α):

$$\operatorname{tg}2\alpha=\frac{\sin 2\alpha}{\cos 2\alpha}=\frac{2\sin\alpha\cos\alpha}{\cos^2\alpha-\sin^2\alpha}=\frac{2\operatorname{tg}\alpha}{1-\operatorname{tg}^2\alpha}.$$

■

Следствие 10. $\operatorname{ctg}2\alpha=\dfrac{\operatorname{ctg}^2\alpha-1}{2\operatorname{ctg}\alpha}$, *(33)*, $\boxed{A}$.

Доказательство. Расписываем котангенс по определению, применяем формулы (28) и (29), а в последнем переходе делим числитель и знаменатель дроби на $\sin^2\alpha$ (новых ограничений на α не появится, поскольку изначально $\sin\alpha, \cos\alpha \neq 0$):

$$\operatorname{ctg} 2\alpha = \frac{\cos 2\alpha}{\sin 2\alpha} = \frac{\cos^2\alpha - \sin^2\alpha}{2\sin\alpha\cos\alpha} = \frac{\operatorname{ctg}^2\alpha - 1}{2\operatorname{ctg}\alpha}\,.$$

■

Формулы, доказанные в следующем утверждении, называются *формулами понижения степени.*

Следствие 11. *1)* $\cos^2\dfrac{\alpha}{2} = \dfrac{1+\cos\alpha}{2}$, *(34),* $\boxed{A}$.

2) $\sin^2\dfrac{\alpha}{2} = \dfrac{1-\cos\alpha}{2}$, *(35),* $\boxed{A}$.

Доказательство. 1) пусть $\alpha = 2\beta$, тогда по формуле (30) получим $\cos 2\beta = 2\cos^2\beta - 1$, откуда $\cos^2\beta = (1+\cos 2\beta)/2$. Делая обратную замену $\beta = \alpha/2$, получаем требуемую формулу.

2) доказывается аналогично предыдущей формуле, только с использованием (31).

■

Следствие 12. *1)* $\operatorname{tg}^2\dfrac{\alpha}{2} = \dfrac{1-\cos\alpha}{1+\cos\alpha}$, *(36),* $\boxed{A}$.

2) $\operatorname{ctg}^2\dfrac{\alpha}{2} = \dfrac{1+\cos\alpha}{1-\cos\alpha}$, *(37),* $\boxed{A}$.

Доказательство. Для доказательства обеих формул применяем (34) и (35).

■

Следствие 13. *1)* $\operatorname{tg}\dfrac{\alpha}{2} = \dfrac{\sin\alpha}{1+\cos\alpha}$, *(38),* $\boxed{A}$.

2) $\operatorname{tg}\dfrac{\alpha}{2} = \dfrac{1-\cos\alpha}{\sin\alpha}$, *(39),* $\boxed{B}$, *D (л.ч.):* $\alpha \neq \pi + 2\pi k$, $k \in \mathbb{Z}$;
D (п.ч.): $\alpha \neq \pi + 2\pi k$, $k \in \mathbb{Z}$, $\alpha \neq 2\pi l$, $l \in \mathbb{Z}$.

3) $\operatorname{ctg}\dfrac{\alpha}{2} = \dfrac{\sin\alpha}{1-\cos\alpha}$, *(40),* $\boxed{A}$.

4) $\operatorname{ctg}\dfrac{\alpha}{2} = \dfrac{1+\cos\alpha}{\sin\alpha}$, *(41),* $\boxed{B}$. *D (л.ч.):* $\alpha \neq 2\pi k$, $k \in \mathbb{Z}$;
D (п.ч.): $\alpha \neq 2\pi k$, $k \in \mathbb{Z}$, $\alpha \neq \pi + 2\pi l$, $l \in \mathbb{Z}$.

Доказательство. 1) используем определение тангенса, затем числитель и знаменатель дроби умножим на ненулевую функцию $2\cos(\alpha/2)$ и затем используем формулы (28) и (34):

$$\operatorname{tg}\frac{\alpha}{2}=\frac{\sin\frac{\alpha}{2}}{\cos\frac{\alpha}{2}}=\frac{2\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}}{2\cos^2\frac{\alpha}{2}}=\frac{\sin\alpha}{1+\cos\alpha}\,.$$

2) также используем определение тангенса, но теперь числитель и знаменатель дроби умножим на функцию $2\sin(\alpha/2)$ (из-за нулей этой функции появляются новые ограничения на α), затем используем формулы (28) и (35):

$$\operatorname{tg}\frac{\alpha}{2}=\frac{\sin\frac{\alpha}{2}}{\cos\frac{\alpha}{2}}=\frac{2\sin^2\frac{\alpha}{2}}{2\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}}=\frac{1-\cos\alpha}{\sin\alpha}\,.$$

Формулы (40) и (41) доказываются аналогично (38) и (39).

■

Формулы, доказанные в следующем утверждении, называются *универсальной тригонометрической подстановкой*. Эти формулы позволяют все четыре основные тригонометрические функции выразить через $\operatorname{tg}\frac{\alpha}{2}$.

Следствие 14. *1)* $\cos\alpha=\dfrac{1-\operatorname{tg}^2\frac{\alpha}{2}}{1+\operatorname{tg}^2\frac{\alpha}{2}}$, *(42),* $\boxed{B}$, *D (л.ч.):* $\alpha\in\mathbb{R}$; *D (п.ч.):* $\alpha\neq\pi+2\pi k$, $k\in\mathbb{Z}$.

2) $\sin\alpha=\dfrac{2\operatorname{tg}\frac{\alpha}{2}}{1+\operatorname{tg}^2\frac{\alpha}{2}}$, *(43),* $\boxed{B}$, *D (л.ч.):* $\alpha\in\mathbb{R}$; *D (п.ч.):* $\alpha\neq\pi+2\pi k$, $k\in\mathbb{Z}$.

3) $\operatorname{tg}\alpha=\dfrac{2\operatorname{tg}\frac{\alpha}{2}}{1-\operatorname{tg}^2\frac{\alpha}{2}}$, *(44),* $\boxed{B}$, *D (л.ч.):* $\alpha\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$; *D (п.ч.):* $\alpha\neq\frac{\pi}{2}+\pi k$, $k\in\mathbb{Z}$, $\alpha\neq\pi+2\pi l$, $l\in\mathbb{Z}$.

4) $\operatorname{ctg}\alpha=\dfrac{1-\operatorname{tg}^2\frac{\alpha}{2}}{2\operatorname{tg}\frac{\alpha}{2}}$, *(45),* $\boxed{A}$.

Доказательство. 1) ниже, во втором переходе, используем формулы (29) и (1), затем числитель и знаменатель дроби делим на $\cos^2(\alpha/2)$ (из-за нулей этой функции появляются новые ограничения на α):

$$\cos\alpha=\frac{\cos\alpha}{1}=\frac{\cos^2\frac{\alpha}{2}-\sin^2\frac{\alpha}{2}}{\cos^2\frac{\alpha}{2}+\sin^2\frac{\alpha}{2}}=\frac{1-\operatorname{tg}^2\frac{\alpha}{2}}{1+\operatorname{tg}^2\frac{\alpha}{2}}\,.$$

Формулы (43) и (44) доказываются аналогично.

При доказательстве (45) дополнительных ограничений не появится, поскольку числитель и знаменатель дроби делим на $\cos^2(\alpha/2)$, а он уже ненулевой из-за первоначальной области определения $\operatorname{ctg}\alpha$:

$$\operatorname{ctg}\alpha = \frac{\cos\alpha}{\sin\alpha} = \frac{\cos^2\frac{\alpha}{2} - \sin^2\frac{\alpha}{2}}{2\cos\frac{\alpha}{2}\sin\frac{\alpha}{2}} = \frac{1-\operatorname{tg}^2\frac{\alpha}{2}}{2\operatorname{tg}\frac{\alpha}{2}}.$$

■

Формулы, доказанные в следующем утверждении, называются *формулами для преобразования суммы или разности функций в произведение.*

Следствие 15. *1)* $\sin\alpha + \sin\beta = 2\sin\dfrac{\alpha+\beta}{2}\cos\dfrac{\alpha-\beta}{2}$, *(46),* $\boxed{A}$.

2) $\sin\alpha - \sin\beta = 2\sin\dfrac{\alpha-\beta}{2}\cos\dfrac{\alpha+\beta}{2}$, *(47),* $\boxed{A}$.

3) $\cos\alpha + \cos\beta = 2\cos\dfrac{\alpha+\beta}{2}\cos\dfrac{\alpha-\beta}{2}$, *(48),* $\boxed{A}$.

4) $\cos\alpha - \cos\beta = -2\sin\dfrac{\alpha+\beta}{2}\sin\dfrac{\alpha-\beta}{2}$, *(49),* $\boxed{A}$.

Доказательство. 1) обозначим через $x = \frac{\alpha+\beta}{2}$ и $y = \frac{\alpha-\beta}{2}$, тогда выполняется $x+y=\alpha$ и $x-y=\beta$. Используя формулы (10) и (11), получим

$$\sin(x+y)+\sin(x-y) = \sin x\cos y + \cos x\sin y + \sin x\cos y - \cos x\sin y =$$

$$= 2\sin x\cos y = 2\sin\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}.$$

Формулы (47), (48) и (49) доказываются аналогично.

■

Следующие три формулы, называются *формулами для преобразования произведения функций в сумму или разность.*

Следствие 16. *1)* $\sin\alpha\cos\beta = \dfrac{1}{2}\Big(\sin(\alpha+\beta)+\sin(\alpha-\beta)\Big)$, *(50),* $\boxed{A}$.

2) $\cos\alpha\cos\beta = \dfrac{1}{2}\Big(\cos(\alpha+\beta)+\cos(\alpha-\beta)\Big)$, *(51),* $\boxed{A}$.

3) $\sin\alpha\sin\beta = \dfrac{1}{2}\Big(\cos(\alpha-\beta)-\cos(\alpha+\beta)\Big)$, *(52),* $\boxed{A}$.

Доказательство. 1) используем формулы (10) и (11) для преобразования правой части:

$$\frac{1}{2}\Big(\sin(\alpha+\beta)+\sin(\alpha-\beta)\Big)=$$

$$=\frac{1}{2}\Big(\sin\alpha\cos\beta+\cos\alpha\sin\beta+\sin\alpha\cos\beta-\cos\alpha\sin\beta\Big)=\sin\alpha\cos\beta.$$

Формулы (51) и (52) доказываются аналогично.

■

Ранее формулы для тройного аргумента были выведены из тригонометрического представления комплексного числа и формул Муавра. Приведем еще классическое доказательство этих формул.

Следствие 17. *1)* $\sin 3\alpha = 3\sin\alpha - 4\sin^3\alpha$, *(53),* $\boxed{A}$.

2) $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, *(54),* $\boxed{A}$.

Доказательство. 1) используем последовательно формулы (10), (31), (28) и (1):

$$\sin 3\alpha = \sin(\alpha+2\alpha) = \sin\alpha\cos 2\alpha + \cos\alpha\sin 2\alpha =$$

$$=\sin\alpha(1-2\sin^2\alpha)+2\sin\alpha\cos^2\alpha = \sin\alpha - 2\sin^3\alpha + 2\sin\alpha(1-\sin^2\alpha) =$$

$$=3\sin\alpha-4\sin^3\alpha.$$

Формула (54) доказывается аналогично.

■

4.5. Обратные тригонометрические функции

В третьей главе мы исследовали проблему существования обратной функции $g: B\to\mathbb{R}$ к данной функции $f: A\to\mathbb{R}$. В теореме 2.4 той главы было найдено необходимое и достаточное условие обратимости: функция f должна быть инъективной (т. е. $f(x_1)\neq f(x_2)$ при всех различных $x_1, x_2\in A$). Нетривиальные периодические функции (т. е. с непустой областью определения) не инъективны, поэтому не могут иметь обратную, это означает, что **все** основные тригонометрические функции **не** обратимы. Попробуем исправить эту ситуацию, ограничив тригонометрические функции на некоторые подмножества их области определения.

Определение. *Ограничением функции* $f: A\to\mathbb{R}$ *на подмножество* $A_1\subseteq A$ *называется функция* $f_1: A_1\to\mathbb{R}$, *заданная следующим образом:* $\forall x\in A_1 \Rightarrow f_1(x)=f(x)$. *Обозначение:* $f_1 = f|_{A_1}$.

Теорема 2.5 третьей главы гарантирует, что все строго монотонные функции имеют обратные, поэтому будем ограничивать тригонометрические функции на такие промежутки, расположенные близко от начала координат, на которых они строго монотонны. По этой теореме, с учетом ранее изученных свойств $\sin x|_{[-\pi/2;\pi/2]}\nearrow$, $\cos x|_{[0;\pi]}\searrow$, $\operatorname{tg} x|_{(-\pi/2;\pi/2)}\nearrow$, $\operatorname{ctg} x|_{(0;\pi)}\searrow$ получим четверку обратных функций: $\arcsin x$, $\arccos x$, $\operatorname{arctg} x$ и $\operatorname{arcctg} x$.

Определение. *Для любого* $x \in [-1;1]$ *арксинусом этого числа называется такой угол* $y \in [-\pi/2;\pi/2]$ *(обозначается* $y = \arcsin x$*), что* $\sin y = x$.

Определение. *Для любого* $x \in [-1;1]$ *арккосинусом этого числа называется такой угол* $y \in [0;\pi]$ *(обозначается* $y = \arccos x$*), что* $\cos y = x$.

Определение. *Для любого* $x \in \mathbb{R}$ *арктангенсом этого числа называется такой угол* $y \in (-\pi/2;\pi/2)$ *(обозначается* $y = \operatorname{arctg} x$*), что* $\operatorname{tg} y = x$.

Определение. *Для любого* $x \in \mathbb{R}$ *арккотангенсом этого числа называется такой угол* $y \in (0;\pi)$ *(обозначается* $y = \operatorname{arcctg} x$*), что* $\operatorname{ctg} y = x$.

Следствие 1. *1)* $\forall x \in [-1;1] \Rightarrow \sin(\arcsin x) = x$.

2) $\forall x \in [-\pi/2;\pi/2] \Rightarrow \arcsin(\sin x) = x$.

3) $\arcsin(\sin x) = x_1 \Leftrightarrow \Big(x_1 \in [-\pi/2;\pi/2]\ \&\ \sin x_1 = \sin x\Big)$.

Доказательство. 1) следует сразу из определения арксинуса.

2) из (1) получаем, что $f(x) = \sin x|_{[-\pi/2;\pi/2]}$ и $y = \arcsin x$ являются обратными к друг другу функциями, поэтому $\arcsin(\sin x) = x$ для любых x из области определения первой из применяемых функций, т. е. для всех $x \in [-\pi/2;\pi/2]$.

3) $\Rightarrow$) из определения арксинуса равенство $\arcsin(\sin x) = x_1$ нам дает, что $x_1 \in [-\pi/2;\pi/2]$ и $\sin x_1 = \sin x$.

$\Leftarrow$) поскольку любая функция однозначна, равенство $\sin x_1 = \sin x$ дает $\arcsin(\sin x) = \arcsin(\sin x_1)$. Для $x_1 \in [-\pi/2;\pi/2]$ по (2) получим $\arcsin(\sin x_1) = x_1$.

■

Пример 1. Найдем значение $\arcsin \sin \dfrac{4\pi}{3}$. С учетом того, что

$$\sin \frac{4\pi}{3} = \sin \frac{-\pi}{3} \quad \text{и} \quad -\pi/3 \in [-\pi/2;\pi/2],$$

используем утверждение (3) предыдущего следствия и приходим к тому, что $\arcsin \sin 4\pi/3 = -\pi/3$. На тригонометрической окружности самостоятельно отметьте точку $P_{4\pi/3}$, проведите через нее горизонтальную прямую и найдите точку на дуге $[-\pi/2;\pi/2]$ с такой же второй координатой.

Следствие 2. *1)* $\forall x \in [-1;1] \Rightarrow \cos(\arccos x) = x$.

2) $\forall x \in [-\pi/2;\pi/2] \Rightarrow \arccos(\cos x) = x$.

3) $\arccos(\cos x) = x_1 \Leftrightarrow \Big(x_1 \in [0;\pi] \ \&\ \cos x_1 = \cos x\Big)$.

Доказательство. Аналогично доказательству первого следствия. ■

Следствие 3. *1)* $\forall x \in \mathbb{R} \Rightarrow \operatorname{tg}(\operatorname{arctg} x) = x$.

2) $\forall x \in (-\pi/2;\pi/2) \Rightarrow \operatorname{arctg}(\operatorname{tg} x) = x$.

3) $\operatorname{arctg}(\operatorname{tg} x) = x_1 \Leftrightarrow \Big(x_1 \in (-\pi/2;\pi/2) \ \&\ \operatorname{tg} x_1 = \operatorname{tg} x\Big)$.

Доказательство. Аналогично доказательству первого следствия. ■

Следствие 4. *1)* $\forall x \in \mathbb{R} \Rightarrow \operatorname{ctg}(\operatorname{arcctg} x) = x$.

2) $\forall x \in (0;\pi) \Rightarrow \operatorname{arcctg}(\operatorname{ctg} x) = x$.

3) $\operatorname{arcctg}(\operatorname{ctg} x) = x_1 \Leftrightarrow \Big(x_1 \in (0;\pi) \ \&\ \operatorname{ctg} x_1 = \operatorname{ctg} x\Big)$.

Доказательство. Аналогично доказательству первого следствия. ■

Простейшие тригонометрические уравнения. Часто решение тригонометрического уравнения после конечной цепочки преобразований сводится к нахождению всех корней уравнений вида: $\sin x = a$, $\cos x = a$, $\operatorname{tg} x = a$ и $\operatorname{ctg} x = a$. Такие уравнения называются простейшими и обратные тригонометрические функции позволяют записать серии, которые содержат все их решения.

I. $$\sin x = a \Leftrightarrow \begin{cases} |a| \leqslant 1, \\ \left[\begin{array}{l} x = \arcsin a + 2\pi k, \ k \in \mathbb{Z}, \\ x = \pi - \arcsin a + 2\pi k, \ k \in \mathbb{Z}. \end{array}\right. \end{cases} \qquad (55) \qquad (*)$$

Ясно, что при $|a| > 1$ уравнение I не имеет решений; при $|a| \leqslant 1$ проведем через точку $(0, a)$ горизонтальную прямую (рис. 40) и пересечем ее с дугой окружности, соответствующей углам $[-\pi/2;\pi/2]$. Эта точка пересечения дает нам первое решение $x = \arcsin a$, и, учитывая основной период $T = 2\pi$, первую серию: $x = \arcsin a + 2\pi k, \ k \in \mathbb{Z}$. Вторая точка пересечения этой горизонтальной прямой с ω_1 будет симметрична найденной относительно оси (Oy) , соответствует решению $x = \pi - \arcsin a$ и порождает вторую серию: $x = \pi - \arcsin a + 2\pi k, \ k \in \mathbb{Z}$.

Замечания. 1. Обе серии в совокупности из $(*)$ можно объединить в одну: $x = (-1)^n \arcsin a + \pi n, \ n \in \mathbb{Z}$. Действительно, при четных n получим $n = 2k$ ($k \in \mathbb{Z}$) и $x = \arcsin a + 2\pi k, \ k \in \mathbb{Z}$ — первая из двух серий; а при

нечетных n получаем $n = 2k+1$ ($k \in Zu$) и $x = -\arcsin a + \pi(2k+1) = \pi - \arcsin a + 2\pi k,\ k \in \mathbb{Z}$ — вторая серия. *Совет:* лучше не использовать короткую форму записи ответа уравнения I. На это есть две причины. Во-первых, такой вид ответа может подтолкнуть к неправильному заключению, что $T_0 = \pi$ является периодом $f(x) = \sin x$. Во-вторых, при решении иррациональных тригонометрических уравнений, тригонометрических уравнений с модулем, или с дополнительными ограничениями на расположение корней, найденные решения надо подставлять в уравнения или неравенства, поэтому «объединенную» серию приходится снова разбивать на две, что приводит к потере времени и возможным ошибкам.

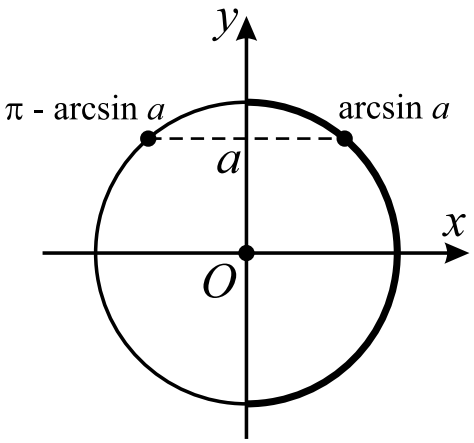

Рис. 40

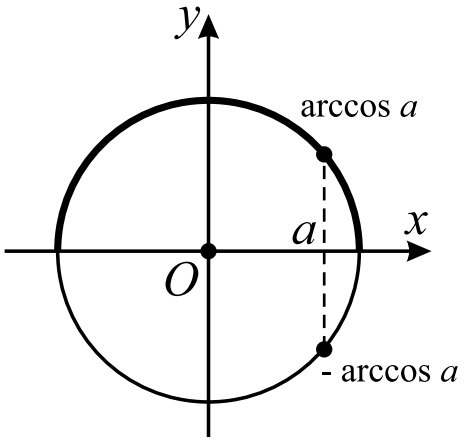

Рис. 41

2. Общей формой $(*)$ не надо пользоваться при решении двух уравнений $\sin x = 1$ или $\sin x = -1$, поскольку обе серии решений в этих уравнениях между собой совпадают и выписываются очевидно ($x = \frac{\pi}{2} + 2\pi k,\ k \in \mathbb{Z}$ — для первого уравнения и $x = -\frac{\pi}{2} + 2\pi k,\ k \in \mathbb{Z}$ — для второго).

3. В записи ответа вместо $\arcsin(1/2)$, $\arcsin(\sqrt{2}/2)$, $\arcsin(\sqrt{3}/2)$ надо использовать хорошо известные углы, рационально зависящие от π: $\pi/6$, $\pi/4$ и $\pi/3$ соответственно.

II. $$\cos x = a \Leftrightarrow \begin{cases} |a| \leqslant 1, \\ x = \pm\arccos a + 2\pi k,\ k \in \mathbb{Z}. \end{cases} \qquad (56)$$

Рассуждаем аналогично предыдущему случаю, но на этот раз через точку $(a, 0)$ проводим вертикальную прямую (рис. 41) и пересекаем ее с той дугой ω_1, которая соответствует углам из отрезка $[0; \pi]$. Так мы находим одно из решений и первую серию: $x = \arccos a + 2\pi k,\ k \in \mathbb{Z}$. Симметричная ей точка относительно оси (Ox) имеет такую же первую координату, поэтому второй серией решений будет $x = -\arccos a + 2\pi k,\ k \in \mathbb{Z}$.

Особенно просто решаются последние два простейших тригонометрических уравнения. В записи множества всех их решений используем то, что $\operatorname{arctg} x$ и $\operatorname{arcctg} x$ принимают все значения и $T = \pi$ является основным периодом $\operatorname{tg} x$ и $\operatorname{ctg} x$.

III. $\operatorname{tg} x = a \Leftrightarrow x = \operatorname{arctg} a + \pi k,\ k \in \mathbb{Z}.$ (57)

IV. $\operatorname{ctg} x = a \Leftrightarrow x = \operatorname{arcctg} a + \pi k,\ k \in \mathbb{Z}.$ (58)

При исследовании свойств обратных тригонометрических функций нам поможет следующий результат.

Теорема 5.1. *1) пусть $f : A \to \mathbb{R}$ — нечетная (или четная) функция. Тогда для любого $a > 0$ функции $f_1 = f|_{A\cap[-a;a]}$ и $f_1 = f|_{A\cap(-a;a)}$ также будут нечетны (соответственно четны).*

2) если $f : A \to \mathbb{R}$ — нечетная функция и существует обратная к ней функция $g = f^{-1} : B \to \mathbb{R}$, то g также нечетна.

Доказательство. 1) для каждого $x \in A \cap [-a;a]$ (или $x \in A \cap (-a;a)$) следует, что $-x \in A$ и $-x \in [-a;a]$ (или $-x \in (-a;a)$), поэтому верно $-x \in A \cap [-a;a]$ (соответственно $-x \in A \cap (-a;a)$) и свойство (а) определения четной или нечетной функции выполняется.

Также легко проверяется (б): $\forall x \in A \cap [-a;a]$ (или $x \in A \cap (-a;a)$) следует, что $f_1(-x) = f(-x) = -f(x) = -f_1(x)$ (для четной функции $f(x)$ получаем $f_1(-x) = f(-x) = f(x) = f_1(x)$).

2) снова проверим выполнение свойств (а) и (б) определения нечетной функции.

а) по определению обратной функции $E(f) = f(A) = B = D(g)$. Для каждого $y \in B$ найдется такой аргумент $x \in A$, что $f(x) = y$. Так как f — нечетна, то $-x \in A$ и $f(-x) = -f(x) = -y \in B$. Итак, свойство (а) для множества B выполняется.

б) для произвольного $y \in B$ обозначим $g(y) = x$, тогда $f(x) = y$. Используя нечетность f, получим

$$g(-y) = g\Big(-f(x)\Big) = g\Big(f(-x)\Big) = -x = -g(y).$$

Свойство (б) также доказано, поэтому $g(x)$ — нечетная функция.

■

Следствие. *Функции $\arcsin x$ и $\operatorname{arctg} x$ нечетны.*

Доказательство. Эти функции являются обратными к $\sin x|_{[-\pi/2;\pi/2]}$ и $\operatorname{tg} x|_{(-\pi/2;\pi/2)}$ соответственно и будут нечетны по утверждениям (1) и (2)

предыдущей теоремы.

■

Далее исследуем свойства и построим графики отдельно для каждой из обратных тригонометрических функций.

$y = \arcsin x$

По определению $y = \arcsin x$ и $\sin x|_{[-\pi/2;\pi/2]}$ обратны друг к другу, поэтому их области определения и множества значений меняются местами, одинаков характер монотонности и графики симметричны относительно прямой $y = x$.

I. $D(y) = [-1; 1]$.

II. $E(y) = \left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$.

III. $y = \arcsin x$ является нечетной функцией по следствию из последней теоремы.

IV. $y = \arcsin x$ не периодическая, поскольку область определения является ограниченным множеством и свойство $x \pm T \in D(y)$ не может выполняться для любого $x \in D(y)$.

V. Поскольку $\arcsin(0) = 0$ и функция строго монотонна, то $(0, 0)$ — единственная точка пересечения графика с осями координат.

VI. Участки знакопостоянства. 1) $y > 0 \Leftrightarrow x \in (0; 1])$.
2) $y < 0 \Leftrightarrow x \in [-1; 0)$.

VII. $y\nearrow$ как обратная к строго возрастающей функции.

VIII. Точек максимума и минимума нет, поскольку функция строго монотонна.

IX. Асимптот нет.

X. $\Gamma(y)$ изображен сплошной линией на рис. 42 как симметричный образ куска синусоиды (штриховая линия).

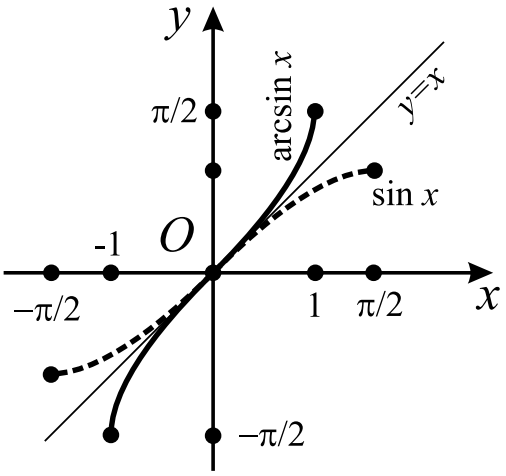

Рис. 42

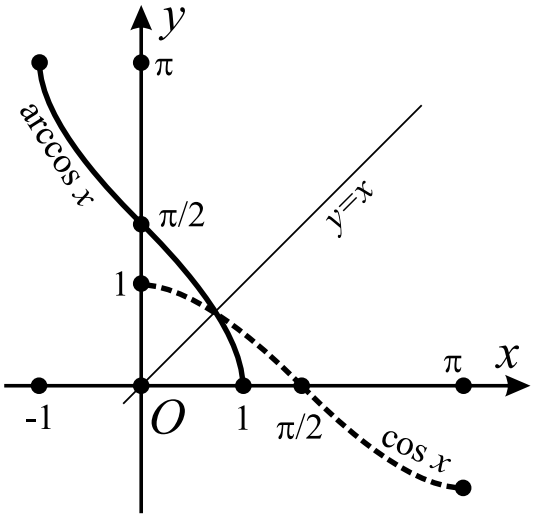

Рис. 43

$y = \arccos x$

По определению $y = \arccos x$ и $\cos x|_{[0;\pi]}$ обратны друг к другу, поэтому их области определения и множества значений меняются местами, одинаков характер монотонности и графики симметричны относительно прямой $y = x$.

I. $D(y) = [-1; 1]$.

II. $E(y) = [0; \pi]$.

III. $y = \arccos x$ по свойству четности-нечетности является функцией общего вида, поскольку $\arccos(1) = 0$, $\arccos(-1) = \pi$.

IV. $y = \arccos x$ не периодическая, поскольку область определения является ограниченным множеством и свойство $x \pm T \in D(y)$ не может выполняться для любого $x \in D(y)$.

V. Поскольку $\arccos(0) = \pi/2$, точка $(0, \pi/2)$ — пересечение графика с осью (Oy). Функция строго монотонна, поэтому $(1, 0)$ — единственная точка пересечения графика с осью (Ox).

VI. Участки знакопостоянства. 1) $y > 0 \Leftrightarrow x \in [-1; 1)$. 2) Отрицательные значения функция не принимает (см. II).

VII. $y\searrow$ как обратная к строго убывающей функции.

VIII. Точек максимума и минимума нет, поскольку функция строго монотонна.

IX. Асимптот нет.

X. $\Gamma(y)$ изображен сплошной линией на рис. 43 как симметричный образ куска косинусоиды (штриховая линия).

$y = \operatorname{arctg} x$

По определению $y = \operatorname{arctg} x$ и $\operatorname{tg} x|_{(-\pi/2;\pi/2)}$ обратны друг к другу, поэтому их области определения и множества значений меняются местами, одинаков характер монотонности и графики симметричны относительно прямой $y = x$.

I. $D(y) = \mathbb{R}$.

II. $E(y) = \left(-\dfrac{\pi}{2}; \dfrac{\pi}{2}\right)$.

III. $y = \operatorname{arctg} x$ является нечетной функцией по следствию из последней теоремы.

IV. $y = \operatorname{arctg} x$ не периодическая, поскольку строго монотонна и не принимает одинаковых значений при разных значениях аргумента.

V. Поскольку $\operatorname{arctg}(0) = 0$ и функция строго монотонна, то $(0, 0)$ — единственная точка пересечения графика с осями координат.

VI. Участки знакопостоянства. 1) $y > 0 \Leftrightarrow x > 0$. 2) $y < 0 \Leftrightarrow x < 0$.

VII. $y\nearrow$ как обратная к строго возрастающей функции.

VIII. Точек максимума и минимума нет, поскольку функция строго монотонна.

IX. Две горизонтальных асимптоты: $y = -\pi/2$ и $y = \pi/2$.

X. $\Gamma(y)$ изображен сплошной линией на рис. 44 как симметричный образ одной ветки тангенсоиды (штриховая линия).

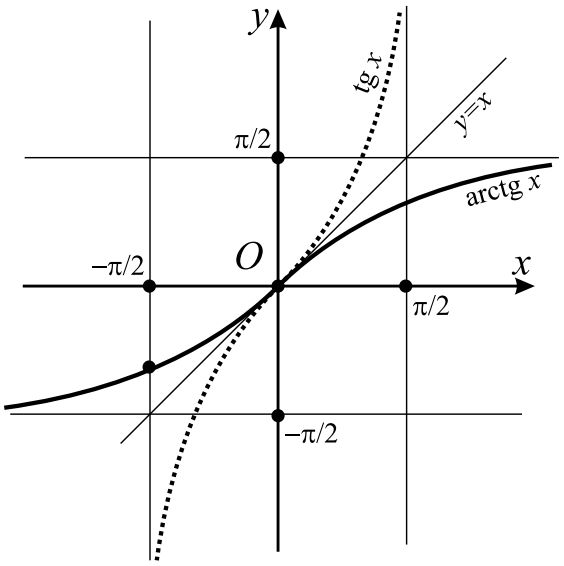

Рис. 44

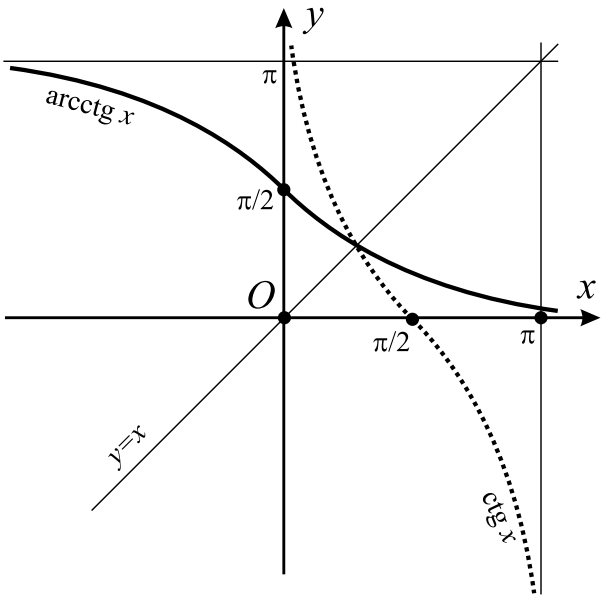

Рис. 45

$$\boxed{y = \operatorname{arcctg} x}$$

По определению $y = \operatorname{arcctg} x$ и $\operatorname{ctg} x|_{(0;\pi)}$ являются обратными друг к другу функциями, поэтому их области определения и множества значений меняются местами, одинаков характер монотонности и графики симметричны относительно прямой $y = x$.

I. $D(y) = \mathbb{R}$.

II. $E(y) = (0;\pi)$.

III. $y = \operatorname{arcctg} x$ по свойству четности-нечетности является функцией общего вида, поскольку $\operatorname{arcctg}(1) = \pi/4$, $\operatorname{arcctg}(-1) = 3\pi/4$.

IV. $y = \operatorname{arcctg} x$ не периодическая, поскольку строго монотонна и не принимает одинаковых значений при разных значениях аргумента.

V. Поскольку $\operatorname{arcctg}(0) = \pi/2$ и функция всюду положительна, то $(0, \pi/2)$ — единственная точка пересечения графика с осями координат.

VI. Участки знакопостоянства: $y > 0 \Leftrightarrow x \in \mathbb{R}$.

VII. $y\searrow$ как обратная к строго убывающей функции.

VIII. Точек максимума и минимума нет, поскольку функция строго монотонна.

IX. Две горизонтальных асимптоты: $y = 0$ и $y = \pi$.

X. $\Gamma(y)$ изображен сплошной линией на рис. 45 как симметричный образ одной ветки котангенсоиды (штриховая линия).

Для вывода двух замечательных формул, связывающих между собой обратные тригонометрические функции, нам понадобится небольшой кусочек теории следующей главы. Два уравнения $f(x) = g(x)$ и $f_1(x) = g_1(x)$ называются равносильными, если множества всех их решений совпадают. Обозначений для равносильных уравнений: $f(x) = g(x) \Leftrightarrow f_1(x) = g_1(x)$. Например, $\sin x = 2 \Leftrightarrow \sqrt{x} = -\pi$ или $\cos x = x^8 + 1 \Leftrightarrow x^2 = 0$. Следующая теорема описывает случай, когда можно применить функцию к левой и правой части уравнения.

Теорема 5.2. *Пусть* $f : A \to \mathbb{R}$, $g : A_1 \to \mathbb{R}$, $f(A), g(A_1) \subseteq B$, $h : B \to \mathbb{R}$. *Если функция* $h(x)$ *инъективна, то*

$$f(x) = g(x) \Leftrightarrow h\Big(f(x)\Big) = h\Big(g(x)\Big).$$

Доказательство. $\Rightarrow$) пусть x_0 выбран так, что $f(x_0) = g(x_0)$, но тогда $f(x_0) \in B$ и в силу однозначности функции $h(x)$ получим $h\Big(f(x_0)\Big) = h\Big(g(x_0)\Big)$.

$\Leftarrow$) пусть теперь x_0 выбран так, что $h\Big(f(x_0)\Big) = h\Big(g(x_0)\Big)$. Вспомним, что $h(x)$ инъективна, поэтому при равных значениях функции, ее аргументы также должны быть равны, т. е. $f(x_0) = g(x_0)$ и x_0 является корнем уравнения $f(x) = g(x)$.

■

Теорема 5.3. *1) для всех* $x \in [-1; 1]$ *выполняется следующее равенство* $\arcsin x + \arccos x = \frac{\pi}{2}$, *(59),* $\boxed{B}$, D *(л.ч.):* $x \in [-1; 1]$; D *(п.ч.):* $x \in \mathbb{R}$.

2) для любого $x \in \mathbb{R}$ *выполняется* $\operatorname{arctg} x + \operatorname{arcctg} x = \frac{\pi}{2}$, *(60),* $\boxed{A}$.

Доказательство. 1) преобразуем уравнение $\arcsin x + \arccos x = \frac{\pi}{2}$ к равносильному уравнению $\arcsin x = \frac{\pi}{2} - \arccos x$ и обозначим функции в левой части и в правой части через $f(x)$ и $g(x)$ соответственно. Нетрудно заметить, что $B = E(f) = E(g) = [-\pi/2; \pi/2]$. На этом множестве рассмотрим функцию $h(x) = \sin x|_{[-\pi/2;\pi/2]}$, она строго возрастает и поэтому инъективна. Применяя последнюю теорему, получим $f(x) = g(x) \Leftrightarrow h\Big(f(x)\Big) = h\Big(g(x)\Big)$.

Очевидно, что $h\Big(f(x)\Big) = \sin\Big(\arcsin(x)\Big) = x$ для всех $x \in [-1;1]$. Теперь преобразуем, используя одну из формул приведения, правую часть получившегося уравнения:

$$\sin\left(\frac{\pi}{2} - \arccos(x)\right) = \cos\Big(\arccos(x)\Big) = x$$

для всех $x \in [-1;1]$. Таким образом, исходное уравнение выполняется для всех $x \in [-1;1]$.

2) доказывается аналогично первому утверждению, с той лишь разницей, что к обеим частям преобразованного уравнения применяют строго возрастающую функцию $h_1(x) = \operatorname{tg} x|_{(-\pi/2;\pi/2)}$.

■

Глава 5

Уравнения и системы уравнений

5.1. Равносильные уравнения

Определение. *Обозначим через* $(*)$ *уравнение* $f(x) = g(x)$, *здесь* $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$ — *числовые функции. Областью допустимы значений уравнения* $(*)$ *называется множество* $\text{ОДЗ}\,(*) = A \cap B = D(f) \cap D(g)$. *Множеством всех решений (или множеством всех корней) уравнения* $(*)$ *называется множество* $\text{Sol}\,(*) = \{x_0 : f(x_0) = g(x_0)\}$.

Следствие. *Для уравнения* $(*)$ *выполняется* $\text{Sol}\,(*) \subseteq \text{ОДЗ}\,(*)$.

Доказательство. Если x_0 удовлетворяет равенству $f(x_0) = g(x_0)$, то $x_0 \in D(f) \cap D(g) = \text{ОДЗ}\,(*)$.

■

Определение. *Пусть* $(**)$ *обозначает уравнение* $f_1(x) = g_1(x)$. *Уравнения* $(*)$ *и* $(**)$ *называются равносильными (или эквивалентными), если выполнено равенство* $\text{Sol}\,(*) = \text{Sol}\,(**)$ *(обозначение:* $(*) \Leftrightarrow (**)$*). Уравнение* $(**)$ *является следствием уравнения* $(*)$, *если* $\text{Sol}\,(*) \subseteq \text{Sol}\,(**)$ *(обозначение:* $(*) \Rightarrow (**)$*).*

Пример 1. Любые два уравнения с пустым множеством решений равносильны друг другу, поэтому $\sin(5x + 3) = \pi \Leftrightarrow \sqrt{x^3 - 5x} = -7$.

Пример 2. Пример равносильных уравнений со счетным множеством решений: $\sin \pi x = 0 \Leftrightarrow \{x\} = 0$. (Напомним, что $\{x\}$ — дробная часть x.)

Пример 3. Из уравнения $\sqrt{x^2} = x$ следует уравнение $x^2 = x^2$, но они не равносильны между собой. Решением первого уравнения будет множество $[0; \infty)$, а решением второго — всё множество $\mathbb{R}$.

Теорема 1.1. *Обозначим через* $(***)$ *уравнение* $f_2(x) = g_2(x)$. *Тогда*
1) если $(*) \Leftrightarrow (**)$ *и* $(**) \Leftrightarrow (***)$, *то* $(*) \Leftrightarrow (***)$;

2) если $(*) \Rightarrow (**)$ *и* $(**) \Rightarrow (***)$, *то* $(*) \Rightarrow (***)$;

3) $\mathrm{Sol}\,(*) = \mathrm{Пр}_{(Ox)}(\Gamma(f) \cap \Gamma(g))$.

Доказательство. 1) если $\mathrm{Sol}\,(*) = \mathrm{Sol}\,(**)$ и $\mathrm{Sol}\,(**) = \mathrm{Sol}\,(***)$, то очевидно, что $\mathrm{Sol}\,(*) = \mathrm{Sol}\,(***)$.

2) если $\mathrm{Sol}\,(*) \subseteq \mathrm{Sol}\,(**)$ и $\mathrm{Sol}\,(**) \subseteq \mathrm{Sol}\,(***)$, то $\mathrm{Sol}\,(*) \subseteq \mathrm{Sol}\,(***)$.

3) проверим включение множеств сразу в обе стороны:

$$x_0 \in \mathrm{Sol}\,(*) \Leftrightarrow f(x_0) = g(x_0) \Leftrightarrow \Big(x_0, f(x_0)\Big) = \Big(x_0, g(x_0)\Big) \Leftrightarrow$$

$$\Leftrightarrow x_0 \in \mathrm{Пр}_{(Ox)}(\Gamma(f) \cap \Gamma(g)).$$

■

Определение. *Совокупностью (или дизъюнцией) уравнений* $f_1(x) = g_1(x)$, $f_2(x) = g_2(x), \ldots,\ f_n(x) = g_n(x)$ *называется*

$$\left[\begin{array}{l} f_1(x) = g_1(x), \\ f_2(x) = g_2(x), \\ \vdots \\ f_n(x) = g_n(x) \end{array}\right. \qquad \textit{или} \qquad \bigvee_{i=1}^{n} f_i(x) = g_i(x). \tag{$\heartsuit$}$$

Решением совокупности называется $\mathrm{Sol}\,(\heartsuit) = \bigcup\limits_{i=1}^{n} \mathrm{Sol}\,\Big(f_i(x) = g_i(x)\Big)$.

Определение. *Системой (или конъюнкцией) уравнений* $f_1(x) = g_1(x)$, $f_2(x) = g_2(x), \ldots,\ f_n(x) = g_n(x)$ *называется*

$$\left\{\begin{array}{l} f_1(x) = g_1(x), \\ f_2(x) = g_2(x), \\ \vdots \\ f_n(x) = g_n(x) \end{array}\right. \qquad \textit{или} \qquad \bigwedge_{i=1}^{n} f_i(x) = g_i(x). \tag{$\diamondsuit$}$$

Решением системы называется $\mathrm{Sol}\,(\diamondsuit) = \bigcap\limits_{i=1}^{n} \mathrm{Sol}\,\Big(f_i(x) = g_i(x)\Big)$.

5.2. Основные способы преобразования уравнений

В этом параграфе исследуем на равносильность основные способы преобразований уравнений. Чтобы избежать сложных обозначений, договоримся нумерацию уравнений (точнее, число звездочек) в каждом способе начинать

заново. Перекрестных ссылок между способами не будет, поэтому не должно возникнуть когнитивного диссонанса. Во многих способах перед очередной теоремой будут приведены примеры неравносильных уравнений, полученных этими способами.

I. Перенос из одной части в другую.

$$f(x)+g(x)=h(x) \qquad (*)$$

$$f(x)=h(x)-g(x) \qquad (**)$$

Теорема 2.1. *Уравнения* $(*)$ *и* $(**)$ *равносильны.*

Доказательство. Действительно, $x_0 \in \mathrm{Sol}\,(*) \Leftrightarrow f(x_0)+g(x_0)=h(x_0) \Leftrightarrow$ $\Leftrightarrow f(x_0)=h(x_0)-g(x_0) \Leftrightarrow x_0 \in \mathrm{Sol}\,(**)$.

■

II. Приведение подобных.

$$f(x)+g(x)-g(x)=h(x) \qquad (*)$$

$$f(x)=h(x) \qquad (**)$$

П р и м е р 1. Уравнения $x^2+\frac{1}{x}-\frac{1}{x}=x$ и $x^2=x$ не равносильны. Множеством решений первого будет $\{1\}$, второго — $\{0,1\}$.

Теорема 2.2. *1)* $(*) \Rightarrow (**)$.
2) если $\mathrm{Sol}\,(**) \subseteq D(g)$, *то* $(*) \Leftrightarrow (**)$.

Доказательство. 1) если $x_0 \in \mathrm{Sol}\,(*)$, то $f(x_0)+g(x_0)-g(x_0)=h(x_0)$, откуда $f(x_0)=h(x_0)$, поэтому $x_0 \in \mathrm{Sol}\,(**)$.

2) осталось доказать, что при этом дополнительном условии, будет верно $(**) \Rightarrow (*)$. Для этого выберем $x_0 \in \mathrm{Sol}\,(**)$ тогда $f(x_0)=h(x_0)$ и, благодаря дополнительному условию, существует число $g(x_0)$. Поэтому

$$f(x_0)=h(x_0) \Rightarrow f(x_0)+g(x_0)-g(x_0)=h(x_0) \Rightarrow x_0 \in \mathrm{Sol}\,(*).$$

■

III. Умножение (деление) на функцию.

$$f(x)=g(x) \qquad (*)$$

$$f(x)\cdot h(x)=g(x)\cdot h(x) \qquad (**)$$

П р и м е р 2. Из уравнения $x^2=x$ (с множеством корней $\{0,1\}$) не следует уравнение $x^2\cdot\frac{1}{x}=x\cdot\frac{1}{x}$ (с множеством всех решений $\{1\}$). В этом примере $h(x)=\frac{1}{x}$.

П р и м е р 3. С другой стороны, само уравнение $x^2 = x$ (с тем же множеством корней $\{0, 1\}$) не является следствием уравнения $x^2 \cdot 0 = x \cdot 0$ (с множеством всех решений $\mathbb{R}$). В этом примере $h(x) = 0$ для всех $x \in \mathbb{R}$.

Теорема 2.3. *1) если* $\mathrm{Sol}\,(*) \subseteq D(h)$, *то* $(*) \Rightarrow (**)$.

2) если для каждого $x \in \mathrm{ОДЗ}\,(*)$ *выполняется* $h(x) \neq 0$, *то* $(*) \Leftrightarrow (**)$.

Доказательство. 1) для любого $x_0 \in \mathrm{Sol}\,(*)$ выполняются два условия: $f(x_0) = g(x_0)$ и существует число $h(x_0)$. Поэтому $f(x_0) \cdot h(x_0) = g(x_0) \cdot h(x_0)$. Последнее означает, что $x_0 \in \mathrm{Sol}\,(**)$.

2) с учетом предыдущего, достаточно доказать, что первое уравнение является следствием второго. Пусть $x_0 \in \mathrm{Sol}\,(**)$, тогда одновременно выполняются два условия: $f(x_0) \cdot h(x_0) = g(x_0) \cdot h(x_0)$ и $h(x_0) \neq 0$. Сократив на ненулевое число, получим $f(x_0) = g(x_0)$, что дает $x_0 \in \mathrm{Sol}\,(*)$.

■

IV. Переход к совокупности.

$$f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_n(x) = 0 \qquad (*)$$

$$\bigvee_{i=1}^{n} f_i(x) = 0 \qquad (**)$$

П р и м е р 4. Уравнение $x \cdot \frac{1}{x} = 0$ (с пустым множеством решений) не равносильна совокупности: $x = 0$ или $1/x = 0$ (объединяя множества решений уравнений совокупности, получим непустое множество $\{0\}$).

Теорема 2.4. *1)* $(*) \Rightarrow (**)$.

2) если для любого $i \in \{1, 2, \ldots, n\}$ *выполняется* $\mathrm{Sol}\left(f_i(x) = 0\right) \subseteq$ $\subseteq \mathrm{ОДЗ}\,(*)$, *то* $(*) \Leftrightarrow (**)$.

Доказательство. 1) для любого $x_0 \in \mathrm{Sol}\,(1)$ выполняется числовое равенство $f_1(x_0) \cdot f_2(x_0) \cdot \ldots \cdot f_n(x_0) = 0$, поэтому найдется такое $i \in \{1, 2, \ldots, n\}$, что $f_i(x_0) = 0$, что означает $x_0 \in \cup_{i=1}^{n} \mathrm{Sol}\left(f_i(x) = 0\right) = \mathrm{Sol}\,(**)$.

2) с учетом предыдущего утверждения, достаточно проверить, что $(**) \Rightarrow (*)$. Для этого выберем произвольный $x_0 \in \mathrm{Sol}\,(**)$, отсюда найдется такое $i \in \{1, 2, \ldots, n\}$, что $f_i(x_0) = 0$. Учитывая условие $\mathrm{Sol}\left(f_i(x) = 0\right) \subseteq$ $\subseteq \mathrm{ОДЗ}\,(*)$, в x_0 определены все функции из уравнения $(*)$, поэтому существуют числа $f_1(x_0)$, $f_2(x_0)$, $\ldots$, $f_n(x_0)$. Одно из этих чисел равно нулю, поэтому $f_1(x_0) \cdot f_2(x_0) \cdot \ldots \cdot f_n(x_0) = 0$, откуда $x_0 \in \mathrm{Sol}\,(*)$.

■

V. Применение функции к обеим частям уравнения.

$$f(x) = g(x) \qquad (*)$$

$$h\Big(f(x)\Big) = h\Big(g(x)\Big) \qquad (**)$$

П р и м е р 5. К левой и правой части уравнения $-x^2 = x$ (с множеством решений $\{0, -1\}$) зачем-то применим функцию $h(x) = \sqrt{x}$ и получим уравнение $\sqrt{-x^2} = \sqrt{x}$ (с множеством решений $\{0\}$). Видим, что в общем случае не выполняется $(*) \Rightarrow (**)$.

П р и м е р 6. К левой и правой части того же уравнения $-x^2 = x$ (с множеством решений $\{0, -1\}$) теперь применим функцию $h(x) = 0$ для каждого $x \in \mathbb{R}$ и получим уравнение $0 = 0$ (с множеством решений $\mathbb{R}$). Видим, что в общем случае не выполняется $(**) \Rightarrow (*)$.

Теорема 2.5. *1) если* $E(f) \cup E(g) \subseteq D(h)$, *то* $(*) \Rightarrow (**)$.

2) если $E(f) \cup E(g) \subseteq D(h)$ *и* $h(x)$ *инъективна на* $E(f) \cup E(g)$, *то* $(*) \Leftrightarrow (**)$.

Доказательство. 1) для любого $x_0 \in \mathrm{Sol}\,(*) \Rightarrow f(x_0) = g(x_0) \in D(h)$. В силу однозначности $h(x)$, получим $h\Big(f(x_0)\Big) = h\Big(g(x_0)\Big)$, т. е. $x_0 \in \mathrm{Sol}\,(**)$.

2) осталось проверить $(**) \Rightarrow (*)$. Для любого $x_0 \in \mathrm{Sol}\,(**)$ выполняется $h\Big(f(x_0)\Big) = h\Big(g(x_0)\Big)$. Теперь инъективность $h(x)$ дает $f(x_0) = g(x_0)$, поэтому $x_0 \in \mathrm{Sol}\,(*)$.

■

Следствие 1. *Для любого* $n \in \mathbb{N}$ *выполняется равносильность двух уравнений:* $f(x) = g(x) \Leftrightarrow f^{2n-1}(x) = g^{2n-1}(x)$.

Доказательство. Для любого $n \in \mathbb{N}$ функция $h(x) = x^{2n-1} \nearrow\nearrow$, поэтому инъективна на всем множестве $\mathbb{R}$. Применяя вторую часть последней теоремы, получим нужный результат.

■

Следствие 2. *Пусть* $f(x) \cdot g(x) \geqslant 0$. *Для любого* $n \in \mathbb{N}$ *выполняется* $f(x) = g(x) \Leftrightarrow f^n(x) = g^n(x)$.

Доказательство. 1-й случай: $f(x), g(x) \geqslant 0$. Функция $h(x) = x^n|_{x \geqslant 0} \nearrow\nearrow$, поэтому инъективна на множестве $[0; \infty)$. Применяя вторую часть последней теоремы, получим нужный результат.

2-й случай: $f(x), g(x) \leqslant 0$. Функция $h(x) = x^n|_{x \leqslant 0} \searrow\searrow$, поэтому инъективна на множестве $(-\infty; 0]$. Далее аналогично первому случаю.

■

VI. Замена переменной.

Чтобы обозначения следующей теоремы были абсолютно понятны, разберем типичный пример на замену переменной.

П р и м е р 7. Решим уравнение $(x+1)(x+2)(x+3)(x+4)=24$. Перемножив крайние и средние скобки попарно между собой, придем к равносильному уравнению $(x^2+5x+4)(x^2+5x+6)=24$. Сделав замену $t=g(x)=x^2+5x$, получим $(t+4)(t+6)=24$ или $t^2+10t=0$ с корнями $t=0$ и $t=-10$. Сделав обратную замену, получим совокупность: $x^2+5x=0$ или $x^2+5x+10=0$. Второе уравнение действительных корней не имеет, поэтому множеством решений первого (и исходного) уравнения является $\{-5,0\}$.

Теорема 2.6. *Обозначим через* $(*)$ *уравнение* $f\Big(g(x)\Big)=0$. *Пусть* $\mathrm{Sol}\Big(f(t)=0\Big)=\{t_1,t_2,\ldots,t_n\}$ *и совокупность уравнений* $\bigvee\limits_{i=1}^{n} g(x)=t_i$ *обозначим через* $(**)$. *Тогда* $(*)\Leftrightarrow(**)$.

Доказательство. Равенство двух множеств решений будем доказывать одновременным включением в обе стороны:

$$x_0\in\mathrm{Sol}\,(*)\Leftrightarrow f\Big(g(x_0)\Big)=0\Leftrightarrow g(x_0)\in\{t_1,t_2,\ldots,t_n\}\Leftrightarrow$$

$$\Leftrightarrow g(x_0)=t_i \text{ для некоторого } i\leqslant n\Leftrightarrow x_0\in\mathrm{Sol}\,(**).$$

■

5.3. Системы уравнений

Определение. *Пусть* $A\subseteq\mathbb{R}^2$ *и* $f:A\to\mathbb{R}$ *— функция. Тогда* $f(x,y)$ *называют функцией двух переменных, а множество* A *— областью определения функции* f *и обозначают через* $D(f)$.

П р и м е р 1. Функция $f(x,y)=x-y$ определена для любой пары $(x,y)\in\mathbb{R}^2$, т. е. $D(f)=\mathbb{R}^2$. Функция $g(x,y)=\sqrt{-xy}$ определена только при $x\cdot y\leqslant 0$, поэтому $D(g)$ является объединением второй и четвертой координатных четвертей.

Для разбора более сложных примеров, нам понадобится уравнение окружности. Рассмотрим две произвольные точки $A(x_1,y_1)$ и $B(x_2,y_2)$ координатной плоскости. Если прямая AB не параллельна координатным осям, легко получается прямоугольный треугольник ABC (на рис. 46 прямые

AC и BC параллельны координатным осям) с катетами, длины которых равны $AC = |x_2 - x_1|$ и $BC = |y_2 - y_1|$. Применяя теорему Пифагора, получим формулу для вычисления расстояния между точками A и B: $AB = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ (эта формула остается верной и в случае, когда прямая AB параллельна одной из координатных осей). Поэтому точка $M(x, y)$ лежит на окружности с центром в $O'(x_0, y_0)$ и радиусом $r \geqslant 0$ тогда и только тогда, когда

$$(x - x_0)^2 + (y - y_0)^2 = r^2 \qquad \textit{(уравнение окружности).}$$

Хорошо известно, что кругом с центром в точке O' и радиусом $r \geqslant 0$ называется множество всех точек M плоскости, удовлетворяющих неравенству $O'M \leqslant r$. Поэтому неравенство $(x - x_0)^2 + (y - y_0)^2 \leqslant r^2$ на координатной плоскости задает круг с центром в $O'(x_0, y_0)$ и радиусом $r \geqslant 0$. Воспользуемся этим замечанием в следующем примере.

П р и м е р 2. Найдем области определения функций

$$f_1(x, y) = \sqrt{4x - x^2 - y^2} \quad \text{и} \quad f_2(x, y) = \frac{1}{\sqrt{x^2 + y^2 - 2x + 4y}}.$$

Функция $f_1(x, y)$ определена, если $x^2 - 4x + y^2 \leqslant 0$ или $x^2 - 4x + 4 + y^2 \leqslant 4$. Последнее неравенство равносильно $(x-2)^2 + y^2 \leqslant 2^2$ и задает на плоскости круг радиуса 2, с центром в точке $(2, 0)$ (рис. 47). Для функции f_2 получаем неравенство $x^2 + y^2 - 2x + 4y > 0$. Выделяя полные квадраты, приходим к $(x-1)^2 + (y+2)^2 > (\sqrt{5})^2$. Это неравенство на плоскости задает область вне круга с центром в точке $(1, -2)$ и радиуса $\sqrt{5}$ (рис. 48).

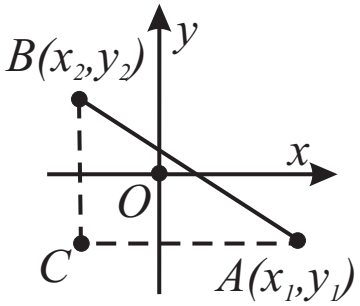

Рис. 46

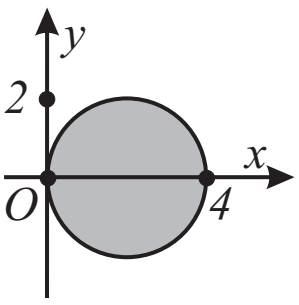

Рис. 47

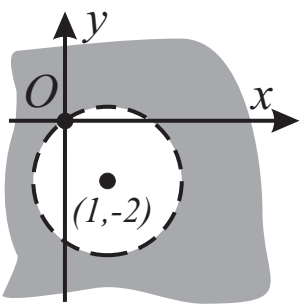

Рис. 48

Замечание. Обратите внимание, что граница круга на последнем рисунке не входит в область определения функции $f_2(x, y)$. Линии, не входящие в область определения функции, изображают **штриховыми**.

Определение. *Уравнение с двумя переменными в общем случае выглядит так:* $f(x,y)=g(x,y)\quad(1)$. *Его* ОДЗ *— это общая часть областей определения функций* $f(x,y)$ *и* $g(x,y)$, *т. е.* $\text{ОДЗ}\,(1)=D(f)\cap D(g)$. *Решением уравнения* (1) *называется множество* $\text{Sol}\,(1)=\{(x_0,y_0):f(x_0,y_0)=g(x_0,y_0)\}$.

Равносильные уравнения и уравнения-следствия определяются точно так же, как и в первом параграфе этой главы.

Определение. *Система двух уравнений с двумя неизвестными записывается следующим образом:*

$$(*)\qquad \begin{cases} f(x,y)=g(x,y), & (1)\\ f_1(x,y)=g_1(x,y). & (2)\end{cases}$$

$\text{ОДЗ}\,(*)=\text{ОДЗ}\,(1)\cap\text{ОДЗ}\,(2)$, $\text{Sol}\,(*)=\text{Sol}\,(1)\cap\text{Sol}\,(2)$.

Определение. *Уравнение* $F(x,y)=G(x,y)\quad(3)$ *называется следствием системы* $(*)$, *если* $\text{Sol}\,(*)\subseteq\text{Sol}\,(3)$.

Теорема 3.1. *1) при замене любого уравнения системы* $(*)$ *на равносильное уравнение, получается равносильная система.*

2) при добавлении к системе $(*)$ *ее следствия, получается равносильная система.*

Доказательство. 1) очевидно следует из определения $\text{Sol}\,(*)$, поскольку замена одного из пересекающихся множеств на равное ему, не изменит пересечение.

2) пусть $F(x,y)=G(x,y)\quad(3)$ — следствие системы $(*)$. Для краткости обозначим через $A=\text{Sol}\,(1)$, $B=\text{Sol}\,(2)$ и $C=\text{Sol}\,(3)$. Из определения уравнения-следствия получим включение $A\cap B\subseteq C$, тогда

$$\text{Sol}\,(*)=A\cap B=A\cap B\cap C=\text{Sol}\,\Big((*)\ \&\ (3)\Big).$$

■

Рассмотрим пример нетривиального использования последней теоремы.

П р и м е р 3. Решим систему $\begin{cases} xy+24=\frac{x^3}{y}, \\ xy-6=\frac{y^3}{x}.\end{cases}$ Перемножая уравнения этой системы, получим ее следствие

$$(xy+24)(xy-6)=x^2y^2\Leftrightarrow x^2y^2+18xy-144=x^2y^2\Leftrightarrow xy=8.$$

Добавим к исходной системе это следствие и сделаем несколько равносильных преобразований (во втором переходе мы умножили первые два уравнения на

третье — это приведет к равносильной системе, поскольку $8 \neq 0$):

$$\left\{\begin{array}{l} xy+24=\frac{x^3}{y}, \\ xy-6=\frac{y^3}{x}, \\ xy=8 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} 32=\frac{x^3}{y}, \\ 2=\frac{y^3}{x}, \\ xy=8 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} 2^8=x^4, \\ 2^4=y^4 \\ xy=8 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \left[\begin{array}{l} x=4, \\ x=-4, \end{array}\right. \\ \left[\begin{array}{l} y=2, \\ y=-2, \end{array}\right. \\ xy=8 \end{array}\right. \Leftrightarrow$$

$(x,y) \in \{(4,2),(-4,-2)\}$.

5.4. Преобразование систем

Мы уже знаем, что перенос из одной части в другую является равносильным преобразованием уравнений. Обозначим через $F(x,y)=f(x,y)-g(x,y)$ и $G(x,y)=f_1(x,y)-g_1(x,y)$, тогда система $(*)$ из предыдущего параграфа по теореме 3.1 равносильна системе с меньшим количеством символов в записи:

$$\left\{\begin{array}{l} F(x,y)=0, \\ G(x,y)=0. \end{array}\right. \qquad (\heartsuit)$$

Именно эта система будет исходной во многих из следующих методах.

I. Метод линейного преобразования.

Определение. *Пусть* $a,b,c,d \in \mathbb{R}$. *Система*

$$\left\{\begin{array}{l} aF(x,y)+bG(x,y)=0, \\ cF(x,y)+dG(x,y)=0 \end{array}\right. \qquad (\diamondsuit)$$

получена из системы $(\heartsuit)$ *с помощью линейного преобразования, причем число* $\Delta = \left|\begin{array}{cc} a & b \\ c & d \end{array}\right| = ad-bc$ *называется определителем линейного преобразования.*

Теорема 4.1. *Если* $\Delta \neq 0$, *то* $(\heartsuit) \Leftrightarrow (\diamondsuit)$.

Доказательство. $\Rightarrow$) выберем произвольное решение первой системы, тогда равенства $F(x_0,y_0)=0$ и $G(x_0,y_0)=0$ выполняются одновременно, поэтому $(x_0,y_0) \in \mathrm{Sol}\,(\diamondsuit)$. Мы доказали, что при любом определителе выполняется $(\heartsuit) \Rightarrow (\diamondsuit)$.

$\Leftarrow$) пусть теперь $(x_0,y_0) \in \mathrm{Sol}\,(\diamondsuit)$. Обозначим через $u_0=F(x_0,y_0)$ и $v_0=G(x_0,y_0)$, получим числовую систему $\left\{\begin{array}{l} au_0+bv_0=0, \\ cu_0+dv_0=0. \end{array}\right.$ Учитывая, что

$\Delta = ad - bc \neq 0$, то $a \neq 0$ или $b \neq 0$. Б.о.о. будем считать, что $a \neq 0$. Выразим из первого уравнения число $u_0 = -bv_0/a$ и подставим его во второе уравнение последней системы. Получим $\left(\dfrac{ad-bc}{a}\right)\cdot v_0 = 0$. Снова вспомним, что $ad - bc \neq 0$, поэтому коэффициент при v_0 отличен от нуля. Отсюда $v_0 = 0$ и $u_0 = 0$. В результате, $(x_0, y_0) \in \mathrm{Sol}\,(\heartsuit)$.

■

Следствие. *Если* $a, b \in \mathbb{R}$ *и* $b \neq 0$, *то* $(\heartsuit) \Leftrightarrow \begin{cases} F(x,y) = 0, \\ aF(x,y) + bG(x,y) = 0. \end{cases}$

Доказательство. Достаточно посчитать $\Delta = \begin{vmatrix} 1 & 0 \\ a & b \end{vmatrix} = b \neq 0$ и применить предыдущую теорему.

■

П р и м е р 1. Решим систему $\begin{cases} 2x + 3y = 5, \\ x - 4y = -3 \end{cases}$ методом линейного преобразования. На первом шаге избавимся от переменной x, используя коэффициенты $a = 1$ и $b = -2$. На втором шаге уничтожим переменную y, домножая уравнения исходной системы на коэффициенты $c = 4$ и $d = 3$. Сразу посчитаем определитель преобразования $\Delta = 3 + 8 = 11 \neq 0$, поэтому

$$\begin{cases} 2x + 3y = 5, \\ x - 4y = -3 \end{cases} \Leftrightarrow \begin{cases} 11y = 11, \\ 11x = 11 \end{cases} \Leftrightarrow \begin{cases} x = 1, \\ y = 1. \end{cases}$$

II. Метод подстановки (или исключения неизвестных).

Теорема 4.2. *Пусть* $F(x,y) = 0 \Leftrightarrow x = f(y)$.

Тогда $(\heartsuit) \Leftrightarrow \begin{cases} x = f(y), \\ G\Big(f(y), y\Big) = 0. \end{cases} \qquad (**)$

Доказательство. Проверим равенство двух множеств решений:

$$(x_0, y_0) \in \mathrm{Sol}\,(\heartsuit) \Leftrightarrow F(x_0, y_0) = 0 \;\&\; G(x_0, y_0) = 0 \Leftrightarrow$$

$$\Leftrightarrow x_0 = f(y_0) \;\&\; G(x_0, y_0) = 0 \Leftrightarrow x_0 = f(y_0) \;\&\; G\Big(f(y_0), y_0\Big) = 0 \Leftrightarrow$$

$$\Leftrightarrow (x_0, y_0) \in \mathrm{Sol}\,(**).$$

■

III. Переход к совокупности.

Теорема 4.3. *Пусть уравнение* $F(x,y)=0$ *равносильно совокупности двух уравнений:* $p(x,y)=0$ *или* $q(x,y)=0$. *Тогда система* $(\heartsuit)$ *равносильна совокупности двух систем*

$$\left[\begin{array}{l}\left\{\begin{array}{l}p(x,y)=0,\\ G(x,y)=0,\end{array}\right.\\ \left\{\begin{array}{l}q(x,y)=0,\\ G(x,y)=0.\end{array}\right.\end{array}\right. \qquad (***)$$

Доказательство. Пусть $A=\mathrm{Sol}\Big(F(x,y)=0\Big)$, $B=\mathrm{Sol}\Big(G(x,y)=0\Big)$, $P=\mathrm{Sol}\Big(p(x,y)=0\Big)$ и $Q=\mathrm{Sol}\Big(q(x,y)=0\Big)$. Из условия сразу получаем, что $A=P\cup Q$, тогда

$$\mathrm{Sol}\,(\heartsuit)=A\cap B=(P\cup Q)\cap B=(P\cap B)\cup(Q\cap B)=\mathrm{Sol}\,(***).$$

■

IV. Однородные системы.

Определение. *Многочлен двух переменных* $f(x,y)\in\mathbb{R}[x,y]$ *называется однородным многочленом степени* $n\in\mathbb{N}$, *если*

$$f(x,y)=a_nx^n+a_{n-1}x^{n-1}y+a_{n-2}x^{n-2}y^2+\ldots+a_2x^2y^{n-2}+a_1xy^{n-1}+a_0y^n$$

и хотя бы один из его коэффициентов не равен нулю. Однородным уравнением степени $n\in\mathbb{N}$ *называется уравнение* $f(x,y)=0$, *где* $f(x,y)$ — *однородный многочлен степени* $n\in\mathbb{N}$.

Определение. *Система называется однородной, если хотя бы одно уравнение этой системы является однородным.*

Теорема 4.4. *Дана однородная система*

$$\left\{\begin{array}{ll}a_nx^n+a_{n-1}x^{n-1}y+\ldots+a_1xy^{n-1}+a_0y^n=0, & (1)\\ G(x,y)=0, & (2)\end{array}\right. \qquad (3)$$

в которой $a_n\neq 0$. *Пусть также* $\{t_1,t_2\ldots,t_p\}$ — *множество всех решений уравнения* $a_nt^n+a_{n-1}t^{n-1}+\ldots+a_1t+a_0=0$. *Тогда система (3) равносильна совокупности систем*

$$\bigvee_{i=1}^{p}\left\{\begin{array}{l}x=t_i\cdot y,\\ G(t_i\cdot y,y)=0.\end{array}\right. \qquad (4)$$

Доказательство. Выберем произвольную пару (x_0, y_0) и рассмотрим два случая.

1-й случай: $y_0 = 0$. Тогда $(x_0, 0) \in \mathrm{Sol}\,(3) \Leftrightarrow\ x_0 = 0$ (здесь мы использовали то, что при ненулевом коэффициенте a_n равенство $a_n x_0^n = 0$ возможно только если $x_0 = 0$) и одновременно $G(0,0) = 0 \Leftrightarrow (0,0) \in \mathrm{Sol}\,(4)$.

2-й случай: $y_0 \neq 0$. Тогда $(x_0, y_0) \in \mathrm{Sol}\,(3) \Leftrightarrow$

$$\Leftrightarrow a_n \left(\frac{x_0}{y_0}\right)^n + a_{n-1}\left(\frac{x_0}{y_0}\right)^{n-1} + \ldots + a_1\left(\frac{x_0}{y_0}\right) + a_0 = 0 \ \&\ G(x_0, y_0) = 0 \Leftrightarrow$$

$\dfrac{x_0}{y_0}$ является корнем уравнения $a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 = 0$ (т. е. $\exists i \leqslant p$, что $\dfrac{x_0}{y_0} = t_i$) $\ \&\ G(x_0, y_0) = 0 \Leftrightarrow\ x_0 = t_i \cdot y_0 \ \&\ G(x_0, y_0) = 0 \Leftrightarrow$

$$\Leftrightarrow \begin{cases} x_0 = t_i \cdot y_0, \\ G(t_i \cdot y_0, y_0) = 0, \end{cases} \quad \text{для некоторого} \quad i \leqslant p \quad \Leftrightarrow \quad (x_0, y_0) \in \mathrm{Sol}\,(4).$$

■

Следствие 1. *Система* $\begin{cases} ax^2 + bxy + cy^2 = d, \\ a_1x^2 + b_1xy + c_1y^2 = d_1 \end{cases}$ *может быть сведена к равносильной однородной системе.*

Доказательство. Если $d = 0$ или $d_1 = 0$, данная система уже является однородной. Пусть $dd_1 \neq 0$. Используем линейное преобразование с определителем, равным $\Delta = \begin{vmatrix} d_1 & -d \\ 0 & 1 \end{vmatrix} = d_1 \neq 0$. Получим равносильную исходной однородную систему

$$\begin{cases} Ax^2 + Bxy + Cy^2 = 0, \\ a_1x^2 + b_1xy + c_1y^2 = d_1. \end{cases}$$

■

Следствие 2. *Пусть* $p(x,y), q(x,y), p_1(x,y), q_1(x,y)$ *— однородные многочлены, для которых* $\deg\Big(p(x,y)\cdot q_1(x,y)\Big) = \deg\Big(p_1(x,y)\cdot q(x,y)\Big)$. *Тогда система* $\begin{cases} p(x,y) = q(x,y), \\ p_1(x,y) = q_1(x,y) \end{cases}$ *может быть сведена к равносильной однородной системе.*

Доказательство. Уравнение $p(x,y)\cdot q_1(x,y) = p_1(x,y)\cdot q(x,y)$ является следствием данной системы. Очевидно, что этому уравнению равносильно $p(x,y)\cdot q_1(x,y) - p_1(x,y)\cdot q(x,y) = 0$ которое является однородным уравнением из-за данного нам равенства степеней (в силу однородности каждого из

многочленов, все слагаемые после перемножения будут иметь одну и ту же степень). Добавляя это уравнение к исходной системе, по теореме 3.1 получим равносильную исходной однородную систему.

■

П р и м е р 2. Решим систему $\begin{cases} x^3+xy^2=40y, \\ y^3+x^2y=10x. \end{cases}$ Перемножая многочлены, как это сделано в предыдущем утверждении, получим уравнение-следствие $10x^4+10x^2y^2=40y^4+40x^2y^2$ или $x^4-3x^2y^2-4y^4=0$. Теперь, согласно последней теореме, необходимо найти корни уравнения $t^4-3t^2-4=0$. Легко сводим его к совокупности: $t^2=-1$ или $t^2=4$. Откуда $t=2$ или $t=-2$. Используя предыдущее следствие и последнюю теорему, сводим данную систему к совокупности систем

$$\left[\begin{cases} x=2y, \\ x^3+xy^2=40y, \\ y^3+x^2y=10x \end{cases} \begin{cases} x=-2y, \\ x^3+xy^2=40y, \\ y^3+x^2y=10x \end{cases} \right. \Leftrightarrow \left[\begin{cases} x=2y, \\ y^3=4y, \\ y^3=4y \end{cases} \begin{cases} x=-2y, \\ y^3=-4y, \\ y^3=-4y \end{cases} \right. \Leftrightarrow \left[\begin{cases} x=2y, \\ y\in\{0,2,-2\} \end{cases} \begin{cases} x=-2y, \\ y=0. \end{cases} \right.$$

Откуда находим три пары решений: $(0,0)$, $(4,2)$, $(-4,-2)$.

V. Замена переменных. Начнем с примера, проясняющего замысловатую систему обозначений очередной теоремы.

П р и м е р 3. Решим систему $\begin{cases} \dfrac{2}{3x-y}-\dfrac{5}{x-3y}=3, \\ \dfrac{1}{3x-y}+\dfrac{2}{x-3y}=\dfrac{3}{5}. \end{cases}$ Сначала введем две новые переменные: $u=u(x,y)=1/(3x-y)$ и $v=v(x,y)=1/(x-3y)$. Сделав замену, получим систему двух линейных уравнений, которую будем решать методом линейного преобразования с определителем, который равен $\Delta=\begin{vmatrix} 1 & -2 \\ 2 & 5 \end{vmatrix}=9\neq 0$:

$$\begin{cases} 2u-5v=3, \\ u+2v=\frac{3}{5} \end{cases} \Leftrightarrow \begin{cases} -9v=\frac{9}{5}, \\ 9u=9 \end{cases} \Leftrightarrow \begin{cases} v=-\frac{1}{5}, \\ u=1. \end{cases}$$

Вернемся к первоначальным переменным и получим систему, которую также будем решать линейным преобразованием, но уже с определителем, равным

$\Delta = \begin{vmatrix} 1 & -3 \\ -3 & 1 \end{vmatrix} = -8 \neq 0$:

$$\begin{cases} 3x - y = 1, \\ x - 3y = -5 \end{cases} \Leftrightarrow \begin{cases} 8y = 16, \\ -8x = -8 \end{cases} \Leftrightarrow \begin{cases} x = 1, \\ y = 2. \end{cases}$$

Теорема 4.5. *Пусть* $(\heartsuit) \Leftrightarrow \begin{cases} H\Big(u(x,y), v(x,y)\Big) = 0, \\ K\Big(u(x,y), v(x,y)\Big) = 0. \end{cases}$ *Обозначим через (5) систему* $\begin{cases} H(u,v) = 0, \\ K(u,v) = 0, \end{cases}$ u $\mathrm{Sol}\,(5) = \{(u_1, v_1), \ldots, (u_n, v_n)\}$. *Тогда* $(\heartsuit) \Leftrightarrow \bigvee_{i=1}^{n} \begin{cases} u(x,y) = u_i, \\ v(x,y) = v_i. \end{cases}$

Доказательство. Аналогично доказательству теоремы 2.6. ■

VI. Симметрические системы. Напомним, что $S[x_1, x_2, \ldots, x_n]$ — множество всех симметрических многочленов от переменных x_1, x_2, $\ldots$, x_n. Если $f(x_1, x_2, \ldots, x_n) \in S[x_1, x_2, \ldots, x_n]$, то уравнение $f(x_1, x_2, \ldots, x_n) = 0$ называется симметрическим.

Определение. *Система называется симметрической, если каждое уравнение этой системы является симметрическим.*

Нам уже известно, что каждый симметрический многочлен от переменных x_1, x_2, $\ldots$, x_n может быть представлен в виде многочлена от элементарных симметрических. Поэтому при решении симметрических систем часто вводят новые переменные: σ_1, σ_2, $\ldots$, σ_n. На этапе обратной замены поможет следующая теорема.

Определение. *Элементарными симметрическими системами от двух и трех переменных называются соответственно следующие две системы:*

$$(6) \quad \begin{cases} x + y = a, \\ xy = b, \end{cases} \qquad (7) \quad \begin{cases} x + y + z = a, \\ xy + xz + yz = b, \\ xyz = c. \end{cases}$$

Теорема 4.6. *1) пусть* t_1 *и* t_2 *— корни уравнения* $t^2 - at + b = 0$, *тогда* $\mathrm{Sol}\,(6) = \{(t_1, t_2), (t_2, t_1)\}$.

2) пусть t_1, t_2 *и* t_3 *— корни уравнения* $t^3 - at^2 + bt - c = 0$, *тогда* $\mathrm{Sol}\,(7) = \{(t_1, t_2, t_3), (t_1, t_3, t_2), (t_2, t_1, t_3), (t_2, t_3, t_1), (t_3, t_1, t_2), (t_3, t_2, t_1)\}$.

Доказательство. Утверждения (1) и (2) — это частные случаи теоремы Виета для многочленов второй и третьей степени (см. теорему 7.3).

■

VII. Деление одного уравнения на другое.

Теорема 4.7. *Рассмотрим следующие две системы:*

$$(8)\quad \begin{cases} F(x,y) = a, \\ G(x,y) = b, \end{cases} \qquad (9)\quad \begin{cases} F(x,y) = a, \\ \dfrac{G(x,y)}{F(x,y)} = \dfrac{b}{a}. \end{cases}$$

Если $a \neq 0$, *то* $(8) \Leftrightarrow (9)$.

Доказательство. Заметим, что $(x_0, y_0) \in \mathrm{Sol}\,(8) \Leftrightarrow$

$$\Leftrightarrow \begin{cases} F(x_0,y_0) = a, \\ G(x_0,y_0) = b \end{cases} \Leftrightarrow \begin{cases} F(x_0,y_0) = a, \\ \dfrac{G(x_0,y_0)}{F(x_0,y_0)} = \dfrac{b}{a} \end{cases} \Leftrightarrow (x_0,y_0) \in \mathrm{Sol}\,(9).$$

■

5.5. Нестандартные способы решений уравнений и неравенств

В этом параграфе мы будем использовать различные свойства функций, которые изучали во втором параграфе третьей главы.

I. Использование ОДЗ.

Теорема 5.1. *Обозначим через* $(*)$ *уравнение* $f(x) = g(x)$. *Если* $\mathrm{ОДЗ}\,(*) = \{x_1, x_2, \ldots, x_n\}$, *то для нахождения* $\mathrm{Sol}\,(*)$ *достаточно подставить в* $(*)$ *числа* x_i *для* $i \in \{1, 2, \ldots, n\}$.

Доказательство. Очевидно, поскольку $\mathrm{Sol}\,(*) \subseteq \mathrm{ОДЗ}\,(*)$.

■

Пример 1. При всех значениях параметра a решим уравнение

$$\frac{\sqrt{-x^2 + x} \cdot \sqrt[4]{x^4 - 1}}{\sqrt{a + x}} + |a| = 3.$$

ОДЗ этого уравнения состоит их всех x, удовлетворяющих системе неравенств: $-x^2+x \geqslant 0$, $x^4-1 \geqslant 0$ и $a+x>0$. Решением первого неравенства является отрезок $[0;1]$, второго неравенства — объединение двух лучей $(-\infty;-1]\cup[1;\infty)$. Пересечением этих множеств будет единственное значение аргумента: $x=1$. Это число лежит в ОДЗ, если $a+1>0$ или $a>-1$. Подставляя при этих значениях параметра $x=1$ в данное уравнение, получим $|a|=3$ или $a=\pm 3$. При $a=-3$ ОДЗ является пустым множеством, поэтому решений нет. Ответ: при $a=3$ корнем будет $x=1$, при других значениях параметра решений нет.

В некоторых тригонометрических уравнениях ОДЗ удается разбить на конечное число серий и подставить каждую из них в исходное уравнение.

Пример 2. Решим уравнение $\sqrt{|\sin x|}=\sqrt[4]{-|\sin x|}+\operatorname{tg} x$. ОДЗ этого уравнения состоит их всех x, удовлетворяющих неравенству $-|\sin x| \geqslant 0$. Решением этого неравенства является серия $x=\pi k$, где $k\in\mathbb{Z}$. Подставляя эту серию в данное уравнение, получим $0=0$. Ответ: $x=\pi k$, где $k\in\mathbb{Z}$.

При решении некоторых неравенств бывает полезным разбить ОДЗ на конечное число подмножеств и провести анализ неравенства на каждом из этих подмножеств.

Пример 3. Решим неравенство $\sqrt{x+3}+\sqrt[4]{9-x} \leqslant \sqrt{3}$. Начинаем с ОДЗ: $x\in[-3;9]$. Рассмотрим три случая.

1-й случай: $x\in[-3;0)$. На множестве $[-3;0]$ функция $\sqrt[4]{9-x}$ строго убывает, поэтому $\sqrt[4]{9-x}>\sqrt[4]{9}=\sqrt{3}$ для всех $x\in[-3;0)$. Учитывая, что на этом множестве $\sqrt{x+3}\geqslant 0$, получим, что левая часть неравенства строго больше $\sqrt{3}$. Делаем вывод, что на этом множестве решений нет.

2-й случай: $x=0$. Получим неверное неравенство $\sqrt{3}+\sqrt[4]{9}<\sqrt{3}$.

3-й случай: $x\in(0;9]$. На множестве $[0;9]$ функция $\sqrt{x+3}$ строго возрастает, поэтому $\sqrt{x+3}>\sqrt{3}$ для всех $x\in(0;9]$. Учитывая, что на этом множестве $\sqrt[4]{9-x}\geqslant 0$, получим, что левая часть неравенства строго больше $\sqrt{3}$. Делаем вывод, что и на этом множестве решений нет.

Ответ: неравенство не имеет решений.

II. Использование монотонности.

Определение. *Уравнения* $(*)\ f(x)=g(x)$ *и* $(**)\ f_1(x)=g_1(x)$ *равносильны на множестве* M, *если* $\operatorname{Sol}(*)\cap M=\operatorname{Sol}(**)\cap M$. *Обозначение:* $(*)\overset{M}{\Longleftrightarrow}(**)$.

Теорема 5.2. *1) если* $f(x)$ *строго монотонна на множестве* M, *то* $\left|M \cap \mathrm{Sol}\left(f(x)=0\right)\right| \leqslant 1$.

2) пусть $f(x)$ *строго монотонна на множестве* M, *и* $g(x)$ *монотонна на этом множестве, причем* $f(x)$ *и* $g(x)$ *имеют разный характер монотонности. Тогда* $|\mathrm{Sol}\,(*) \cap M| \leqslant 1$.

Доказательство. 1) б.о.о. $f(x)\nearrow\!\!\!\nearrow_M$ и нашлись такие $x_1, x_2 \in M$, что $x_1 < x_2$ и $f(x_1) = 0 = f(x_2)$. Строгое возрастание функции на M дает $0 = f(x_1) < f(x_2) = 0$. $\lightning$.

2) б.о.о. $f(x)\nearrow\!\!\!\nearrow_M$ и $g(x)\searrow_M$. Тогда $(*) \overset{M}{\Longleftrightarrow} f(x) - g(x) = 0$. Обозначим через $h(x) = f(x) - g(x)$. Тогда $h(x)\nearrow\!\!\!\nearrow_M$ и по первому утверждению получим требуемое: $\left|M \cap \mathrm{Sol}\left(h(x)=0\right)\right| \leqslant 1$.

■

П р и м е р 4. Решим уравнение $-\sqrt[8]{x-2} + \sqrt[4]{18-x} = 2$. Легко находим ОДЗ: $x \in [2;18]$. На этом множестве левая часть уравнения является строго убывающей функцией, а правая — возрастающей функцией (любая константа на любом множестве является одновременно возрастающей и убывающей функцией). По предыдущей теореме это уравнение не может иметь более одного корня. Очевидно, что значение аргумента $x_0 = 2$ удовлетворяет уравнению. Ответ: $x = 2$.

П р и м е р 5. Решим неравенство $\sqrt[8]{2-x^2} > x^3 + x - 1$. Легко находим ОДЗ: $x \in [-\sqrt{2};\sqrt{2}]$. Разобьем ОДЗ на два промежутка.

1-й случай: $x \in [-\sqrt{2};0)$. На этом множестве левая часть уравнения положительна, а правая не превосходит -1, поэтому неравенство выполняется для всех $x \in [-\sqrt{2};0)$.

2-й случай: $x \in [0;\sqrt{2}]$. На этом множестве левая часть является строго убывающей функцией, а правую можно представить в виде двух строго возрастающий функций: x^3 и $x-1$. Предыдущая теорема гарантирует, что на рассматриваемом множестве уравнение $\sqrt[8]{2-x^2} = x^3 + x - 1$ имеет не более одного корня. Легко угадывается, что этим корнем будет $x = 1$. Учитывая характер монотонности, получим, что на множестве $[0;1)$ данное неравенство выполняется, а на множестве $[1;\sqrt{2}]$ — нет. Ответ: $x \in [-\sqrt{2};1)$.

III. Использование ограниченности (или метод разделяющего числа).

В первом утверждении следующей теоремы число a называется *разделяющим*, а во втором — *строго разделяющим числом.*

Теорема 5.3. *1) если для любого $x \in M$ выполняются неравенства $f(x) \geqslant a$ и $g(x) \leqslant a$, то $f(x) = g(x) \overset{M}{\Longleftrightarrow} \begin{cases} f(x) = a, \\ g(x) = a. \end{cases}$*

2) если для любого $x \in M$ одновременно выполняются два неравенства $f(x) > a$ и $g(x) \leqslant a$, то уравнение $f(x) = g(x)$ на множестве M не имеет решений.

Доказательство. 1) $\Rightarrow$) пусть $x_0 \in \mathrm{Sol}\,(*)$ и $x \in M$, тогда $f(x_0) \geqslant a$ и $g(x_0) = f(x_0) \leqslant a$, откуда $g(x_0) = f(x_0) = a$.

$\Leftarrow$) если $g(x_0) = a = f(x_0)$, то $g(x_0) = f(x_0)$ и $x_0 \in \mathrm{Sol}\,(*)$.

2) о/п: найдется такое число $x_0 \in M$, что $f(x_0) = g(x_0)$. Тогда одновременно должно выполняться: $f(x_0) > a$ и $g(x_0) = f(x_0) \leqslant a$. $\lightning$.

■

П р и м е р 6. Решим уравнение $\sin\left(x^3 + 2x^2 + 1\right) = x^2 + 2x + 3$. Оценка для правой части: $x^2 + 2x + 3 = x^2 + 2x + 1 + 2 = (x+1)^2 + 2 \geqslant 2$. Очевидно, что $\sin\left(x^3 + 2x^2 + 1\right) < 2$, поэтому $a = 2$ является строго разделяющим числом и уравнение решений не имеет.

П р и м е р 7. Решим уравнение $\cos x = x^{2020} + 1$. Для каждого $x \in \mathbb{R}$ выполняются два неравенства $\cos x \leqslant 1$ и $x^{2020} + 1 \geqslant 1$ ($a = 1$ является разделяющим числом). По предыдущей теореме данное уравнение равносильно системе: $\cos x = 1$ и $x^{2020} + 1 = 1$. Единственным решением второго уравнения является $x = 0$. К счастью, это число является корнем и первого уравнения. Ответ: $x = 0$.

IV. Использование четности или нечетности функций.

Теорема 5.4. *Если $f(x)$ — четная (или нечетная) функция, то $x_0 \in \mathrm{Sol}\left(f(x) = 0\right) \Leftrightarrow -x_0 \in \mathrm{Sol}\left(f(x) = 0\right)$.*

Доказательство. Сразу заметим, что x_0 и $-x_0$ одновременно лежат или не лежат в $\mathrm{ОДЗ}\left(f(x) = 0\right) = D(f)$.

$\Rightarrow$) если $f(x_0) = 0$, то $f(-x_0) = f(x_0) = 0$ (или $f(-x_0) = -f(x_0) = 0$), что означает $-x_0 \in \mathrm{Sol}\left(f(x) = 0\right)$.

$\Leftarrow$) пусть теперь выполняется $f(-x_0) = 0$, тогда $f(x_0) = f(-x_0) = 0$ (или $f(x_0) = -f(-x_0) = 0$), что означает $x_0 \in \mathrm{Sol}\left(f(x) = 0\right)$.

■

П р и м е р 8. При каких значениях параметров a и b единственное ре-

шение имеет система

$$\begin{cases} xyz + z = a, \\ xyz^4 + z = b, \\ x^2 + y^2 + z^2 = 4? \end{cases} \qquad (***)$$

Заметим, что при одновременной смене знака у переменных x и y уравнения системы не изменятся (в этом случае говорят, что уравнения четны относительно пары переменных $\{x, y\}$). Это означает, что выполняется утверждение: $(x_0, y_0, z_0) \in \mathrm{Sol}\,(***) \Rightarrow (-x_0, -y_0, z_0) \in \mathrm{Sol}\,(***)$. Требование единственности решения у $(***)$ дает нам, что решение **необходимо** имеет вид $(0, 0, z_0)$. Подставляя $x = y = 0$ в систему, получим: $z = a = b$, $z^2 = 4$. Отсюда получаем два случая: $z = a = b = 2$ и $z = a = b = -2$.

1-й случай: $z = a = b = 2$. Немного преобразуем систему, заменив его второе уравнение на разность второго и первого уравнения:

$$\begin{cases} xyz + z = 2, \\ xyz^4 + z = 2, \\ x^2 + y^2 + z^2 = 4 \end{cases} \Leftrightarrow \begin{cases} xyz + z = 2, \\ xyz(z^3 - 1) = 0, \\ x^2 + y^2 + z^2 = 4 \end{cases} \Leftrightarrow \begin{cases} xyz + z = 2, \\ \left[\begin{array}{l} x = 0, \\ y = 0, \\ z = 0, \\ z = 1, \end{array}\right. \\ x^2 + y^2 + z^2 = 4. \end{cases}$$

При $z = 0$ первое уравнение превращается в противоречивое $0 = 2$.

При значениях переменных $x = 0$ или $y = 0$ из первого уравнения получаем $z = 2$. Подстановка этого значения в последнее уравнение дает $y = 0$ или $x = 0$. Получим первое решение системы — $(0, 0, 2)$.

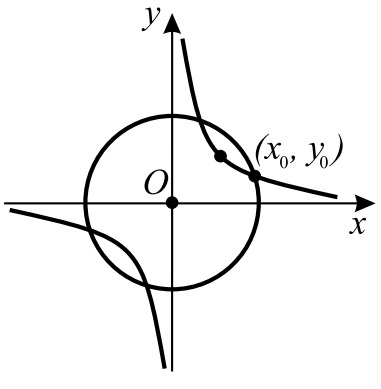

Рис. 49

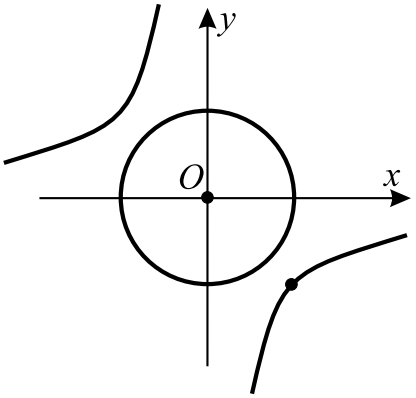

Рис. 50

Рассмотрим случай, когда $z = 1$. Система имеет вид $\begin{cases} xy = 1, \\ x^2 + y^2 = 3. \end{cases}$ Подстановка $y = 1/x$ дает биквадратное уравнение $x^4 - 3x^2 + 1 = 0$, откуда $x^2 = \dfrac{3 \pm \sqrt{5}}{2}$, что приводит еще к четырем решениям исходной системы. Эти значения параметров не

удовлетворяют условиям задачи. На рис. 49 видно, что новые решения появились из-за того, что точка гиперболы $(1,1)$ лежит внутри окружности радиуса $\sqrt{3}$ с центром в начале координат, поэтому гипербола и окружность пересекаются.

2-й случай: $z = a = b = -2$. Немного преобразуем систему, заменив его второе уравнение на разность второго и первого уравнения:

$$\left\{\begin{array}{l} xyz + z = -2, \\ xyz^4 + z = -2, \\ x^2 + y^2 + z^2 = 4 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} xyz + z = -2, \\ xyz(z^3 - 1) = 0, \\ x^2 + y^2 + z^2 = 4 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} xyz + z = -2, \\ \left[\begin{array}{l} x = 0, \\ y = 0, \\ z = 0, \\ z = 1, \end{array}\right. \\ x^2 + y^2 + z^2 = 4. \end{array}\right.$$

При $z = 0$ первое уравнение превращается в противоречивое $0 = -2$.

При $x = 0$ или $y = 0$ из первого уравнения получаем $z = -2$, подстановка которого в последнее уравнение дает $y = 0$ или $x = 0$. Получим первое решение системы — $(0, 0, -2)$.

Остается рассмотреть случай $z = 1$. Система имеет вид $\left\{\begin{array}{l} xy = -3, \\ x^2 + y^2 = 3. \end{array}\right.$ Подстановка $y = -3/x$ дает биквадратное уравнение $x^4 - 3x^2 + 9 = 0$ без корней. На рис. 50 видно, что точка гиперболы $(\sqrt{3}, -\sqrt{3})$ лежит вне окружности радиуса $\sqrt{3}$ с центром в начале координат, поэтому гипербола и окружность не пересекаются.

Ответ: $a = b = -2$.

V. Многократное применение строго возрастающей функции.

Теорема 5.5. *Введем обозначения для следующих двух уравнений:* $(\heartsuit)\ f(x) = x$ *и* $(\diamondsuit)\ f\Big(f(x)\Big) = x$.

1) $(\heartsuit) \Rightarrow (\diamondsuit)$.

2) если $f \nearrow\!\!\nearrow$, *то* $(\heartsuit) \Leftrightarrow (\diamondsuit)$.

3) если $f \nearrow\!\!\nearrow$ *и* $g(x)$ *— обратная к* $f(x)$ *функция, то выполняется* $f(x) = g(x) \Leftrightarrow f(x) = x$.

Доказательство. 1) пусть $x_0 \in \mathrm{Sol}\,(\heartsuit)$, тогда $f(x_0) = x_0 \in D(f)$ и, в силу однозначности функции $f(x)$, получаем $f\Big(f(x_0)\Big) = f(x_0) = x_0$, откуда $x_0 \in \mathrm{Sol}\,(\diamondsuit)$.

2) в силу уже доказанного в (1), достаточно проверить, что $(\diamondsuit) \Rightarrow (\heartsuit)$. О/п: $f\Big(f(x_0)\Big) = x_0$, но $f(x_0) \neq x_0$. Рассмотрим два случая.

1-й случай: $x_0 < f(x_0)$. С учетом того, что f строго возрастает, получим $f(x_0) < f\Big(f(x_0)\Big) = x_0$. $\not\nearrow$.

2-й случай: $x_0 > f(x_0)$. С учетом того, что f строго возрастает, получим $f(x_0) > f\Big(f(x_0)\Big) = x_0$. $\not\nearrow$.

3) используя то, что $E(g) = D(f)$ и тот факт, что строго монотонные функции инъективны, получим $f(x) = g(x) \Leftrightarrow f\Big(f(x)\Big) = f\Big(g(x)\Big) = x$. По (2) уравнение $f\Big(f(x)\Big) = x$ равносильно уравнению $f(x) = x$, что и завершает доказательство.

■

П р и м е р 9. Найдем все значения параметра a, при которых на отрезке $[3;4]$ существует хотя бы одно решение уравнения $x^2 - a = \sqrt{x+a}$. Рассмотрим функции $f(x) = (x^2 - a)|_{x \geqslant 0}$ и $g(x) = \sqrt{x+a}$. Для них выполняется $E(f) = [-a;\infty) = D(g)$, $f(x) \nearrow\!\!\nearrow$ и

$$g\Big(f(x)\Big) = \sqrt{(x^2-a)+a} = \sqrt{x^2} = |x| = x, \text{ так как } x \geqslant 0.$$

Таким образом, $g(x)$ — обратная функция к $f(x)$ и данное уравнение равносильно при $x \geqslant 0$ уравнению $x^2 - a = x$ или $x^2 - x - a = 0$. Функция $h(x) = x^2 - x - a$ строго возрастает на отрезке $[3;4]$, поэтому существование на $[3;4]$ нуля у этой непрерывной функции равносильно

$$\begin{cases} h(3) \leqslant 0, \\ h(4) \geqslant 0 \end{cases} \Leftrightarrow \begin{cases} 6 - a \leqslant 0, \\ 12 - a \geqslant 0 \end{cases} \Leftrightarrow a \in [6;12].$$

Ответ: $a \in [6;12]$.

П р и м е р 10. Найдем все значения параметра a, при которых на отрезке $[-3;-2]$ существует хотя бы одно решение уравнения $x^2 - a = \sqrt{a-x}$. Сразу применить предыдущую теорему не получится, поскольку функция в левой части уравнения строго убывает на отрезке $[-3;-2]$. Сделаем замену $t = -x$. Получим уравнение $t^2 - a = \sqrt{t+a}$, которое на отрезке $[2;3]$ должно иметь хотя бы одно решение. Далее, следуя предыдущему примеру, найдем $a \in [2;6]$.

Учебное издание

Сергей Александрович Ануфриенко

АЛГЕБРА 10

Учебное пособие

Редактор
Корректор
Компьютерный набор и верстка С. А. Ануфриенко

Подписано в печать .12.2021. Формат $60 \times 84\ 1/16$.
Уч.-изд.л. . Бумага офсетная.
Тираж экз. Заказ № .

Издательство
620000, Екатеринбург-83, ул. Тургенева, 4

Университетское издательство
620017, Екатеринбург, ул. Вали Котика, 13, под. 1а

Отпечатано в Издательско-полиграфическом центре УрФУ
620000, Екатеринбург-83, ул. Тургенева, 4
Тел.: +7 (343) 358-93-06, 350-90-13, 358-93-22, 350-58-20
Факс: +7 (343) 358-93-06
E-mail: press-urfu@mail.ru
http: //print.urfu.ru