Е.А. Голикова

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Часть I: математическая логика и общая алгебра

Электронный текстовый ресурс

Научный редактор: доц., канд. физ.-мат. наук Ю.Б. Мельников

Учебное пособие представляет собой расширенный курс лекций по дисциплине “Дискретная математика”, который читается для студентов физических и информационных специальностей Физико-технологического института и Института радиоэлектроники и информационных технологий УрФУ.

Екатеринбург

2017

Оглавление

ВВЕДЕНИЕ

Содержание курса «Дискретная математика» также обширно, как и содержание курса «Математический анализ». «Дискретная математика» – это математическая логика, общая алгебра и другие дисциплины «чистой» математики, выводы которых являются основой для построения теории программирования и создания актуальных для различных приложений алгоритмов. Теория алгоритмов также является частью дискретной математики, но это не есть список популярных на сегодняшний день алгоритмов. Исходя из этих соображений, в данном курсе будет сделан акцент на изучение основных понятий алгебры, логики и теории чисел. Высокий уровень абстракции, характерный для этих понятий, делает их изучение непростым для студентов. Тем более важно разобраться в определениях и свойствах групп, полей, алгебр и т. п., чтобы понимать теорию кодов или алгоритм электронной подписи.

Первая глава посвящена множествам, высказываниям и отношениям. Но сразу отметим, что это все – примеры алгебр.

Определение. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется функция n переменных, определенная на Ω.*

Нам привычны числовые бинарные операции. Например, операция сложения целых чисел есть функция двух переменных, определенная на множестве $\mathbb{Z}$, она *паре* целых чисел a, b ставит в соответствие целое число $a + b$.

Определение. Алгеброй (универсальной алгеброй) *называется упорядоченная пара $\mathcal{A} = \langle A, \mathcal{F} \rangle$, где A – некоторое непустое множество, называемое* **носителем** *алгебры $\mathcal{A}$, и $\mathcal{F}$ – множество операций, определенных на A, называемое* **сигнатурой** *алгебры $\mathcal{A}$.*

Множество целых чисел с операцией сложения и операцией умножения – универсальная алгебра. Ее носитель – множество целых чисел, сигнатура состоит из двух операций – сложение и умножение. (Более подробно см. раздел 2.1.) Теперь, используя понятие алгебры, можем сформулировать первую цель: изучение алгебры множеств.

ГЛАВА 1

МНОЖЕСТВА, ВЫСКАЗЫВАНИЯ, ОТНОШЕНИЯ

1.1. Множества

Как известно, математика оперирует понятиями и теоремами. Каждое понятие вводится с помощью определения, которое в свою очередь использует уже известные понятия. Спускаясь таким образом, мы получим понятия, которые определить в строгом смысле невозможно. К таким фундаментальным относится понятие множества. Заметим здесь, что в современной математике основным способом определения фундаментальных понятий является *аксиоматический метод*. Всякая аксиоматическая теория начинается с формулировки набора аксиом и предполагает использование развитого логического аппарата для построения строгих доказательств теорем. В частности, для теории множеств предложено несколько систем аксиом и, соответственно, существует несколько аксиоматических теорий множеств. Каждая из таких теорий сопровождается доказательством непротиворечивости соответствующей системы аксиом. Эта задача является трудной и не всегда разрешимой. Поэтому мы изложим здесь основы так называемой «наивной» теории множеств, опираясь при этом не на строгую аксиоматику, а на интуицию и здравый смысл. При этом мы заведомо получим противоречивую теорию, что иллюстрируется «парадоксами теории множеств» (см. стр. 7). Итак, определим понятия *множество* и *элемент множества*, как фундаментальные, следующим образом:
множество – любая определенная совокупность **элементов**, элементы множества различны и отличимы друг от друга.

1.1.1. *Множество, подмножество, элемент*

Чтобы задать множество, нужно указать, какие элементы ему принадлежат. Описание элементов данного множества может быть сделано двумя способами:
1) перечисление всех элементов: $A = \{a, b, c, \ldots, z\}$;

2) выделение элементов x, удовлетворяющих характеристическому свойству (предикату, см. 1.2.8) $P(x)$: $A = \{x|P(x)\}$.

Иногда (например в программировании) указывают процедуру, с помощью которой можно распознать лежит ли элемент в множестве, либо процедура вычисляет элементы множества. Однако, это частный случай второго способа задания множеств. Тот факт, что x является элементом множества A обозначаем $x \in A$. Противоположное высказывание: x не является элементом множества A обозначается $x \notin A$.

Пример. $A = \{1, 2, 3, 4\} = \{x| \begin{cases} x \in \mathbb{N} \\ x < 5 \end{cases}\}$. Характеристическое свойство $P(x)$ в данном случае формулируется так: x – натуральное число меньше пяти. Это же свойство мы можем сформулировать, используя союз «и»: x – натуральное число **и** x – меньше пяти. Применяя вместо союза «и» логический символ &, можем задать множество так: $A = \{x|x \in \mathbb{N}\ \&\ x < 5\}$.

В приведенном примере для удобства записи использовался логический символ. Имея в виду не только удобство и краткость записей, но и их логическую структуру (о чем подробнее см. раздел 1.2) будем использовать следующие обозначения.

Если A и B некоторые множества, то

$x \in A$ – x является элементом множества A;

$x \notin A$ – x не является элементом множества A;

$A \subseteq B$ – A подмножество множества B;

$A \setminus B = \{x|x \in A\ \&\ x \notin B\}$ – разность множеств A и B.

Если A и B некоторые высказывания, то

$\overline{A}$ (или $\neg A$)– не A;

$A \wedge B$ (или $A\&B$) – A и B;

$A \vee B$ – A или B;

$A \Rightarrow B$ – если A, то B;

$A \Leftrightarrow B$ – A равносильно B;

$\forall A$ – для любого A;

$\exists A$ – существует A.

Используя фундаментальные понятия множества и элемента множества, дадим определение подмножества.

Определение 1.1.1. *Множество B является* **подмножеством** *множества A, если каждый элемент множества B является элементом A. Символьная запись:* $(B \subseteq A) \Leftrightarrow (x \in B \Rightarrow x \in A)$.

По определению всякое множество есть подмножество самого себя. Заметим, что используют также обозначение $B \subset A$, как правило для того, чтобы подчеркнуть, что B не совпадает с A. В этом случае множество B называется *собственным* подмножеством множества A.

Определение 1.1.2. *Множество B* **равно** *множеству A, если каждый элемент множества B является элементом A и наоборот. Символьная запись:*

$$(B = A) \Leftrightarrow (B \subseteq A \ \& \ A \subseteq B).$$

В конкретных задачах обычно элементы всех рассматриваемых множеств принадлежат одному достаточно широкому множеству Ω, которое называется **универсальным** (или универсумом). Другим предельным случаем является **пустое** множество $\emptyset$, которое, по определению, не содержит никаких элементов.

Пример. Покажем, что в множестве $A = \{\emptyset, \ \{\emptyset\}\}$ каждый элемент является одновременно и подмножеством.

Действительно, $\emptyset \in A$. Но для каждого множества, по определению пустого множества и определению подмножества $\emptyset \subseteq A$. Для второго элемента A имеем $\{\emptyset\} \in A$. С другой стороны, одноэлементное подмножество, образованное первым элементом, содержится в A как подмножество: $\{\emptyset\} \subseteq A$.

Парадокс Рассела. В отличае от рассмотренной в примере ситуации, каждое подмножество являться элементом не может. Более того, если предположить, что существует множество Y, такое, что $Y \in Y$, то это приводит к логическому противоречию, т. н. парадоксу Рассела.

Действительно, рассмотрим множество Y, состоящее из всех множеств, не содержащих себя в качестве элемента:

$$Y = \{X | X \notin X\}.$$

Тогда зададимся вопросом: верно ли, что $Y \in Y$? Если неверно, т. е. $Y \notin Y$, то по построению Y имеем $Y \in Y$. Получено противоречие. Если утверждение $Y \in Y$ верно, то по построению Y имеем $Y \notin Y$. Получено противоречие для любого из возможных предположений.

При построении аксиоматической теории множеств в список аксиом включают т. н. аксиому регулярности: множество не может являться своим элементом. Такое требование позволяет избежать парадокса Рассела. Однако есть и другие способы избежать противоречивости системы аксиом.

1.1.2. *Мощность множества*

В этом разделе вводится понятие мощности множества, которое позволяет сравнивать множества по «количеству элементов» в них.

Определение 1.1.3. *Говорят, что* **мощность** *множества A* **не превосходит мощности** *множества B, если существует взаимно однозначное отображение f* [1] *из множества A в множество B.*

Тот факт, что мощность множества A не превосходит мощности множества B коротко записывается следующим образом: $|A| \leq |B|$.

Определение 1.1.4. *Говорят, что множества A и B* **равномощны** *или, иными словами, что* **мощности множеств** *A и B* **равны** *тогда и только тогда, когда $|A| \leq |B|$ и $|B| \leq |A|$.*

Утверждение, что мощности множеств A и B равны записывается так: $|A| = |B|$.

Замечание. По определению, если $|A| = |B|$, то существуют взаимно однозначные функции $h : A \mapsto B$ и $g : B \mapsto A$, причем, вообще говоря, может быть $h(A) \subset B$, где $h(A)$ – множество значений h (в частности, $h(A) \neq B$) или $g(B) \subset A$ (в частности, $g(B) \neq A$). Однако, с помощью этих функций h и g, а также обратных к ним, всегда можно построить взаимно однозначную функцию f из A в B, такую, что $f(A) = B$. Во многих случаях удобно пользоваться именно таким признаком равномощности множеств:

$$|A| = |B| \;\Leftrightarrow\; \exists f : A \mapsto B(\forall a_1, a_2 \in A\ (a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2))\ \&\ f(A) = B.)$$

Пример. Множества $\mathbb{N}$ и $\mathbb{Z}$ равномощны. В качестве f можно взять $f(z) = 2|z| + \frac{1}{2}(\mathrm{sign}(z + 0.5) + 1)$, то есть функцию, имеющую таблицу значений

x	$\ldots$	-2	-1	0	1	2	$\ldots$
$f(x)$	$\ldots$	4	2	1	3	5	$\ldots$

которую можно записать и так:

x	0	-1	1	-2	2	$\ldots$
$f(x)$	1	2	3	4	5	$\ldots$

Определение 1.1.5. *Множество, равномощное множеству $\mathbb{N}$, называется* **счетным**.

[1] f – взаимно однозначное отображение из множества A в множество B, если $(a \in A, b \in A, a \neq b) \Rightarrow (f(a) \neq f(b))$.

Из определения легко получить следующие свойства равномощности множеств.

Свойства равномощности множеств:

1) $\forall A\ (|A| = |A|)$;

2) $\forall A, B\ (|A| = |B| \Rightarrow |B| = |A|)$;

3) $\forall A, B, C\ ((|A| = |B|\ \&\ |B| = |C|) \Rightarrow |A| = |C|)$.

Понятие мощности множества позволяет определить конечные и бесконечные множества.

Определение 1.1.6. *Множество A называется* **конечным**, *если у него нет собственного подмножества равномощного A (обозначение: $|A| < \infty$). В противном случае: если найдется собственное подмножество из A, равномощное A, то A называется* **бесконечным** *(обозначение: $|A| = \infty$).*

Пример. В примере на стр. 8 доказано, что множества $\mathbb{N}$ и $\mathbb{Z}$ равномощны и при этом $\mathbb{N} \subset \mathbb{Z}$. По определению получили, что множество целых чисел $\mathbb{Z}$ бесконечно.

Теорема 1.1.1 (о бесконечном подмножестве). *Множество, обладающее бесконечным подмножеством, бесконечно:*

$$(B \subseteq A\ \&\ |B| = \infty) \Rightarrow (|A| = \infty)$$

Доказательство. По определению 1.1.6, существует собственное подмножество $C \subset B$, равномощное B. Воспользуемся признаком равномощности, сформулированном в замечании на стр. 8. Поскольку $|B| = |C|$, существует взаимно однозначная функция $f : B \mapsto C$, такая, что $f(B) = C$. Доопределим эту функцию на все множество A и построим взаимно однозначную функцию f_1 из множества A в его собственное подмножество $f_1(A)$:

$$f_1(a) = \begin{cases} f(a),\ a \in B \\ a,\ a \notin B \end{cases}.$$

Теперь имеем:

$$\begin{cases} f_1(B) = f(B) = C \subset B \subset A \\ f_1(A \setminus B) = A \setminus B \end{cases} \Rightarrow f_1(A) \subset A.$$

Таким образом, множество A содержит собственное подмножество $f_1(A)$ (оно не содержит $B \setminus C$,) равномощное A в силу взаимной однозначности f_1 (см. рис. 1.1). Поэтому доказано, что $|A| = \infty$.

Теорема 1.1.2 (о свойствах конечных множеств). *Пусть множество A – отрезок натурального ряда, т. е. $A = \{1, 2, \ldots, n\}$. Тогда*

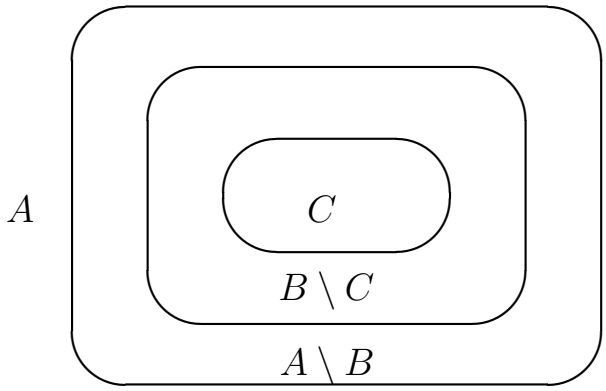

Рис. 1.1. Диаграмма подмножеств

1) $|A| < \infty$;
2) $(B = \{1, 2, \ldots, m\} \ \& \ m \neq n) \Rightarrow |A| \neq |B|$;
3) $\forall B(B \neq \emptyset \ \& \ |B| < \infty) \Rightarrow \exists\, n \in \mathbb{N}(|A| = |B|)$.

Доказательство. 1. Докажем, что $|A| < \infty$ от противного.

Пусть $|A| = \infty$ и число n – наименьшая длина бесконечного отрезка натурального ряда A. Тогда по определению 1.1.6 найдется собственное подмножество $B \subset A$, равномощное A. Пусть $f : A \mapsto B$ – соответствующая взаимно однозначная функция. Тогда $f(n) = i$ для некоторого $1 \leq i \leq n$. Рассмотрим множества $A_1 = A \setminus \{n\} = \{1, 2, \ldots, n-1\}$ и $B_1 = B \setminus \{i\}$. Но функция f осуществляет взаимно однозначное соответствие $f : A_1 \mapsto B_1$, причем $B_1 \subset A_1$. Но тогда $|A_1| = \infty$ в то время как длина отрезка натурального ряда A_1 равна $n - 1$, что противоречит выбору n.

2. Докажем, что $|\{1, 2, \ldots, n\}| \neq |\{1, 2, \ldots, m\}|$ $(m \neq n)$ от противного.

Пусть $n > m$ и $|\{1, 2, \ldots, n\}| = |\{1, 2, \ldots, m\}|$. Однако $\{1, 2, \ldots, m\} \subset \{1, 2, \ldots, n\}$, следовательно, по определению 1.1.6, $|\{1, 2, \ldots, n\}| = \infty$. Получено противоречие с пунктом 1 теоремы.

3. Пусть B – конечное непустое множество. Построим процедуру перенумерации его элементов.

Выберем некоторый элемент $x_1 \in B$ (это возможно, т. к. $B \neq \emptyset$) и положим $f(x_1) = 1$. Затем рассмотрим множество $B_1 = B \setminus \{x_1\}$. Если $B_1 = \emptyset$, то нумерация закончена, если $B_1 \neq \emptyset$, то выберем элемент $x_2 \in B_1$ и положим $f(x_2) = 2$. В общем виде:

$$\begin{gathered} B_i \neq \emptyset \Rightarrow \exists x_{i+1} \in B_i \ \& \ f(x_{i+1}) = i + 1 \text{ либо} \\ B_i = \emptyset \Rightarrow |B| = |\{1, 2, \ldots, i\}| \end{gathered} .$$

Если процедура не заканчивается, т. е. $\forall i \ B_i \neq \emptyset$, то f – взаимно однозначная

функция $f : B^* \mapsto \mathbb{N},\ B^* = \{x_1, x_2, \ldots\} \subseteq B$, что противоречит конечности множества B. Теорема доказана.

Итак, понятие мощности обобщает понятие «количество элементов» конечного множества. Мы уже разобрались с мощностями простейших множеств:

$$|\emptyset| = 0, |\{1, 2, \ldots, n\}| = n,\ |\mathbb{N}| = \infty.$$

В частности, конечные множества могут иметь разные мощности. То же самое имеет место и для бесконечных множеств. Множества, равномощные $\mathbb{N}$, называются счетными. Счетная мощность самая маленькая из бесконечных и имеет обозначение: $|\mathbb{N}| = \aleph_0$ (читается «алеф-ноль»). Рассмотрим отрезок $[0;1]$ – подмножество множества действительных чисел. Понятно, что $|\mathbb{N}| = \aleph_0 \leq |[0;1]|$ хотя бы потому, что числа вида $\frac{1}{n},\ n \in \mathbb{N}$ образуют подмножество из $[0;1]$. Покажем,что мощность $[0;1]$ больше, чем счетная.

Теорема 1.1.3 (о несчетности континуума). *Множество всех действительных чисел, принадлежащих отрезку* $[0;1]$*, является несчетным.*

Доказательство. Всякое действительное число из $[0;1]$ можно однозначно представить в виде десятичной дроби $0, \alpha_1\alpha_2\ldots$, где для сколь угодно большого номера N найдется такой номер $n > N$, что $\alpha_n \neq 9$. Последнее уточнение вызвано тем, что, например, $1 = 0,99999\ldots$.

Пусть удалось построить взаимно однозначную функцию $f : [0;1] \mapsto \mathbb{N}$. Распишем подробнее функцию f, параллельно подбирая специальное число β :

$f(0, \alpha_{11}\alpha_{12}\alpha_{13}\ldots\alpha_{1n}\ldots) = 1$ обозначим $0, \alpha_{11}\alpha_{12}\alpha_{13}\ldots\alpha_{1n}\ldots \mapsto 1$ и т. д.:

$0, \alpha_{11}\alpha_{12}\alpha_{13}\ldots\alpha_{1n}\ldots \mapsto 1$	$\beta_1 \in \{0;1;\ldots;8\},\ \beta_1 \neq \alpha_{11}$
$0, \alpha_{21}\alpha_{22}\alpha_{23}\ldots\alpha_{2n}\ldots \mapsto 2$	$\beta_2 \in \{0;1;\ldots;8\},\ \beta_2 \neq \alpha_{22}$
$0, \alpha_{31}\alpha_{32}\alpha_{33}\ldots\alpha_{3n}\ldots \mapsto 3$	$\beta_3 \in \{0;1;\ldots;8\},\ \beta_3 \neq \alpha_{33}$
$\ldots$	$\ldots$
$0, \alpha_{n1}\alpha_{n2}\alpha_{n3}\ldots\alpha_{nn}\ldots \mapsto n$	$\beta_n \in \{0;1;\ldots;8\},\ \beta_n \neq \alpha_{nn}$
$\ldots$	$\ldots$

$$\beta = 0, \beta_1\beta_2\beta_3\ldots\beta_n\ldots$$

Пусть $f(0, \beta_1\beta_2\beta_3\ldots) = k$. Тогда $f(0, \beta_1\beta_2\beta_3\ldots) = k = f(0, \alpha_{k1}\alpha_{k2}\alpha_{k3}\ldots\alpha_{kk}\ldots)$, но, по выбору элементов β_i, имеем $\beta_k \neq \alpha_{kk}$.

Это противоречит взаимной однозначности f, то есть множество $[0,1]$ несчетно. Теорема доказана.

Определение 1.1.7. *Множество, равномощное множеству всех действительных чисел из* $[0;1]$, *называется* **континуальным**, *или* **множеством мощности континуум**. *Обозначение:* $|[0;1]| = \mathbf{c}$.

В теореме 1.1.3 доказано, что $\aleph_0 < \mathbf{c}$. В следующей теореме показано как для любого множества можно построить множество большей мощности.

Теорема 1.1.4 (о мощности множества подмножеств). *Если* X – *множество и* 2^X – *множество всех его подмножеств, то* $|X| < \left|2^X\right|$.

Доказательство. Очевидно, что $|X| \leq \left|2^X\right|$.

Пусть $|X| = \left|2^X\right|$. Тогда существует взаимно однозначная функция $f : 2^X \mapsto X$.

Рассмотрим $Y = \left\{y \,\middle|\, y \notin f^{-1}(y)\right\}$. По определению обратной функции для любого $Y \subseteq X$ имеем $Y = f^{-1}(f(Y))$. Возможны 2 случая:
1) $f(Y) \in Y = f^{-1}(f(Y)) \;\Rightarrow\; y = f(Y) \in f^{-1}(f(Y)) \;\Rightarrow\; y = f(Y) \notin Y$;
2) $f(Y) \notin Y \;\Rightarrow\; y = f(Y) \notin f^{-1}(f(Y)) = Y \;\Rightarrow\; f(Y) \in Y$.
Противоречие получено в любом случае. Теорема доказана.

Замечание. 1. Если конечное множество A содержит k элементов, то число его подмножеств $|2^A| = 2^k$.

2. $\aleph_0 < 2^{\aleph_0} \leq \mathbf{c} < 2^{\mathbf{c}}$. Вопрос о равенстве $2^{\aleph_0} = \mathbf{c}$ носит название *гипотеза континуума.*

3. Для любого множества найдется множество большей мощности.

Определение 1.1.8. *Множество всех подмножеств множества* X *называется* **булеан** [2] *множества* X. *Обозначение:* 2^X.

1.1.3. *Алгебра множеств*

Рассмотрим булеан множества Ω, т. е. все подмножества $A, B, C, \ldots$ универсального множества Ω. На элементах множества 2^Ω определим операции, тем самым построив алгебру множеств. Определения теоретикомножественных операций хорошо известны из начального курса математики. Здесь мы сформулируем их с использованием языка логики.

Определение 1.1.9. *Пусть* $A, B, C \in 2^\Omega$, *тогда*
C – **объединение** A *и* B: $C = A \cup B = \{x | x \in A \vee x \in B\}$;
C – **пересечение** A *и* B: $C = A \cap B = \{x | x \in A \& x \in B\}$;
C – **дополнение** A: $C = \overline{A} = \{x | x \in \Omega \& x \notin A\}$;
C – **разность** A *и* B: $C = A \setminus B = \{x | x \in A \& x \notin B\}$.

[2] Джордж Буль (George Boole 1815–1864) – английский математик, основоположник информатики.

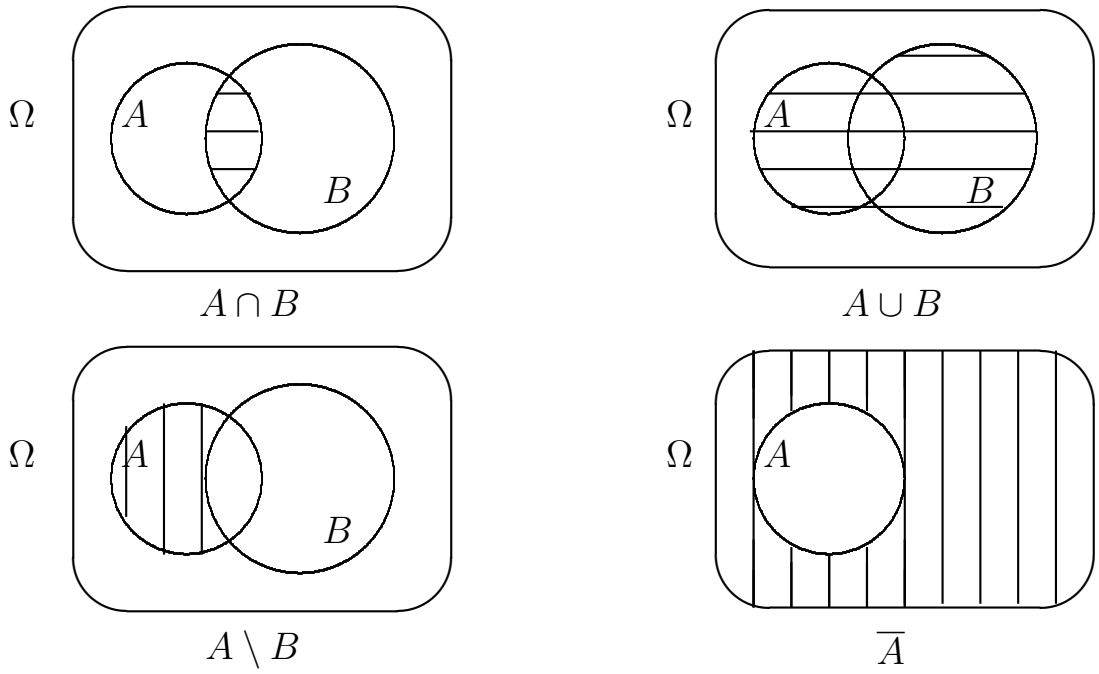

Рис. 1.2. Диаграммы Венна

Иногда удобно использовать наглядное изображение множеств в виде диаграмм Венна.[3] См. рис. 1.2.

Свойства теоретикомножественных операций:

1) *идемпотентность:* $A \cup A = A, \quad A \cap A = A$;
2) *коммутативность:* $A \cup B = B \cup A, \quad A \cap B = B \cap A$;
3) *ассоциативность:* $A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$;
4) *дистрибутивность:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$$
5) *поглощение:* $A \cup (B \cap A) = A, \quad A \cap (B \cup A) = A$;
6) *свойства нуля:* $A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset$;
7) *свойства единицы:* $A \cup \Omega = \Omega, \quad A \cap \Omega = A$;
8) *инволютивность:* $\overline{\overline{A}} = A$;
9) *законы двойственности де Моргана* [4]*:* $\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$;
10) *свойства дополнения:* $A \cup \overline{A} = \Omega, \quad A \cap \overline{A} = \emptyset$;
11) *вычисление разности:* $A \setminus B = A \cap \overline{B}$.

Все перчисленные свойства являются следствием определений операций и определения равенства множеств. В качестве примера приведем доказательство одного из законов де Моргана.

Доказательство 9). По определению 1.1.2 имеем:

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \Leftrightarrow (\overline{A \cap B} \subseteq \overline{A} \cup \overline{B} \ \& \ \overline{A} \cup \overline{B} \subseteq \overline{A \cap B}).$$

[3] Джон Венн (John Venn 1834–1923) – английский логик и философ.
[4] Огастес де Морган (1806–1871) – шотландский математик и логик.

По определению 1.1.1 докажем первое включение $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$:

$$x \in \overline{A \cap B} \Leftrightarrow x \notin A \cap B \Leftrightarrow x \in \overline{A} \vee x \in \overline{B} \Leftrightarrow x \in \overline{A} \cup \overline{B}$$

Обратное включение $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ легко получается из приведенной цепочки эквивалентностей, если читать ее справа налево. Доказательство равенства множеств закончено.

Пример. С помощью полученных свойств теоретикомножественных операций упростить выражение $(\overline{A \cap \overline{B}}) \cup B$; доказать равенство
$(\overline{A} \cup \overline{B}) \cap C = \overline{(A \cap B) \cup \overline{C}}$.

Решение. Над равенствами в преобразованиях подписаны номера использованных свойств.
1. $(\overline{A \cap \overline{B}}) \cup B \overset{9}{=} (\overline{A} \cup \overline{\overline{B}}) \cup B \overset{8}{=} (\overline{A} \cup B) \cup B \overset{3}{=} \overline{A} \cup (B \cup B) \overset{1}{=} \overline{A} \cup B$.
2. $(\overline{A} \cup \overline{B}) \cap C \overset{9,8}{=} (\overline{A \cap B}) \cap \overline{\overline{C}} \overset{9}{=} \overline{(A \cap B) \cup \overline{C}}$.

Замечание. 1. Если множества A и B конечны, тогда

$$|A \cup B| = |A| + |B| - |A \cap B|; \quad |A \setminus B| = |A| - |A \cap B|.$$

Это утверждение хорошо иллюстрируется диаграммами Венна (см. рис. 1.2) и доказывается легко.

2. Возможно обобщение операций объединения и пересечения множеств на любое число операндов: пусть I – произвольное (конечное или бесконечное) множество индексов, тогда

$$\bigcup_{i \in I} A_i = \{x | \exists i \in I (x \in A_i)\}; \quad \bigcap_{i \in I} A_i = \{x | \forall i \in I (x \in A_i)\}.$$

Определение 1.1.10. Разбиением *множества A называется семейство его подмножеств A_i, $i \in I$, если*

$$A = \bigcup_{i \in I} A_i \ \& \ (i \neq j \Rightarrow A_i \cap A_j = \emptyset).$$

Обозначение: $A = \dot{\bigcup}_{i \in I} A_i$.

Отметим еще одну операцию – «произведение» множеств.

Определение 1.1.11. Декартово (прямое) произведение *множеств A и B есть множество всех упорядоченных пар, в которых первый элемент принадлежит A, а второй – B:*

$$A \times B = \{(a, b) | a \in A \ \& \ b \in B\}.$$

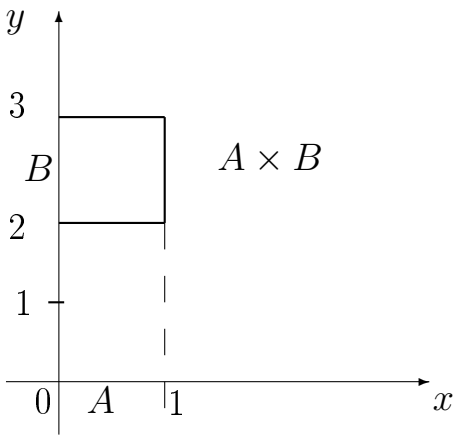

Рис. 1.3. Пример декартова произведения

Пример. 1. Если $A = \{1, 2, 3\}$, $B = \{1, 2\}$, то

$A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$, причем $|A \times B| = |A| \cdot |B| = 6$.

2. Если $A = [0, 1]$, $B = [2, 3]$ – отрезки действительных чисел, то

$$A \times B = \{(x, y) | x \in [0, 1] \ \& \ y \in [2, 3]\},$$

Изображая каждую пару (x, y) точкой на плоскости, множеству $A \times B$ сопоставим квадрат на плоскости xOy (см. рис. 1.3).

Можно рассматривать не только упорядоченные пары, но и упорядоченные тройки и т. д.

Определение 1.1.12. Упорядоченная n-ка (кортеж) *элементов a_i множеств A_i, $i = 1, 2, \ldots, n$ есть набор вида $(a_1, a_2, \ldots, a_n)$:*

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow \ a_1 = b_1 \ \& \ a_2 = b_2 \ \& \ \ldots a_n = b_n.$$

Используя понятие кортежа, можно говорить о декартовом произведении любого конечного числа множеств.

Определение 1.1.13. Декартово (прямое) произведение *множеств $A_i, i = 1, \ldots, m$ есть множество всех упорядоченных m-к , в которых $a_i \in A_i, i = 1, \ldots, m$:*

$$A_1 \times A_2 \times \ldots \times A_m = \{(a_1, a_2, \ldots, a_m) | \forall i (a_i \in A_i)\}.$$

Пример. 1. Каждое имя гражданина России есть элемент декартова произведения множества Ф – всех фамилий, И – всех имен, О – множества всех отчеств.

2. Множество комплексных чисел есть декартов квадрат множества действительных чисел: $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

3. Множество действительных матриц-строк длины m можно рассматривать как $m-$ю декартову степень множества действительных чисел: $\{(a_1\, a_2\, \ldots\, a_m)|\forall i(a_i \in \mathbb{R})\} = \mathbb{R} \times \mathbb{R} \ldots \times \mathbb{R} = \mathbb{R}^m$.

Замечание. Если множества $A_i, i = 1, \ldots, m$ конечны, тогда

1) $|A_1 \times A_2 \times \ldots \times A_m| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|$;

2) $|\dot{\bigcup\limits_{i=1\ldots m}} A_i| = \sum\limits_{i=1}^{m} |A_i|$ (здесь имеется в виду разбиение).

Доказательства этих утверждений о мощностях конечных множеств проводятся по индукции.

1.2. Высказывания

1.2.1. *Алгебра высказываний*

Определение 1.2.1. Высказыванием *мы назовем любую фразу, относительно которой осмысленным (корректным) является вопрос «верна эта фраза или нет».*

Например, алгебраическое выражение $2x^2 - 1$ высказыванием не является, а утверждения $2x^2 - 1 > 0$, или «Снег белый», или «Снег синий» – это высказывания. Фраза «Закройте, пожалуйста, дверь» высказыванием не является. Всякая теорема в математике является высказыванием, истинность которого устанавливается с помощью доказательства. Высказывания будем обозначать большими латинскими буквами: $A, B, C, \ldots$.

Определение 1.2.2. A **и** B **логически эквивалентны** *(равносильны), если в любой ситуации либо и* A*, и* B *– истинны, либо и* A*, и* B *– ложны* ($A \equiv B$).

Пример. 1. Высказывания

A: «в равнобедренном треугольнике одна из медиан совпадает с высотой»,

B: «если треугольник равнобедренный, то одна из его медиан совпадает с высотой» и

C: «одна из медиан треугольника совпадает с высотой при условии, что этот треугольник равнобедренный»

логически эквивалентны, то есть мы их будем считать одним высказыванием.

2. Для всех действительных значений переменной x высказывания

$A : (x+1)^2 \geq 0$ и $B : x^2 + 2x + 1 \geq 0$ логически эквивалентны.

Из простых высказываний строятся более сложные с помощью *логических связок* (операций на множестве высказываний). Определим основные.

Определение 1.2.3. Отрицанием *высказывания A называется высказывание «не A», обозначаемое $\overline{A}$ (или $\neg A$), которое истинно тогда и только тогда, когда A ложно.*

Определение 1.2.4. Конъюнкцией *высказываний A и B называется высказывание «A и B», обозначаемое $A \wedge B$ (или $A\&B$), которое истинно тогда и только тогда, когда оба высказывания A и B истинны.*

Определение 1.2.5. Дизъюнкцией *высказываний A и B называется высказывание «A или B», обозначаемое $A \vee B$, которое истинно тогда и только тогда, когда хотя бы одно из высказываний A или B истинно.*

Определение 1.2.6. Импликацией *высказываний A и B называется высказывание «если A,то B», обозначаемое $A \Rightarrow B$ (или $A \to B$) , которое ложно тогда и только тогда, когда A истинно, а B ложно.*

Определение 1.2.7. Эквиваленцией *высказываний A и B называется высказывание « A тогда и только тогда, когда B» (« A эквивалентно B»), обозначаемое $A \Leftrightarrow B$ (или $A \leftrightarrow B$) , которое истинно тогда и только тогда, когда оба высказывания A и B истинны или оба ложны.*

То, что мы раньше использовали на интуитивном уровне «для сокращения и упрощения» записей (см. стр. 6), введено теперь определениями как понятия. Заметим, что в определениях логических операций истинность высказывания-результата каждой операции полностью определяется набором истинности операндов. Поэтому можно расчитывать истинность результата операций. Удобным инструментом для этого служат таблицы истинности. Значения истинности высказываний в них обозначают по разному: истина=И=Т=1, ложь=Л=F=0. Мы используем в основном 0 и 1.

Таблицы истинности

A	B	$A\&B = A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

1.2.2. *Предикаты*

Определение 1.2.8. n-местным предикатом $P(x_1, \ldots, x_n)$ *на множестве A называется высказывание, истинность или ложность которого определяется значениями n переменных, $x_i \in A$.*

Определение 1.2.9. Функция истинности предиката $P(x_1, \ldots, x_n)$ *есть функция из множества* $\underbrace{A \times A \times \ldots \times A}_{n \text{ раз}} = A^n$ *в множество* $\{0, 1\}$*:* $\varphi_P(x_1, \ldots, x_n)$*, задаваемая формулой*

$$\varphi_P(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если} \quad P(x_1, \ldots, x_n); \\ 0, & \text{если} \quad \neg P(x_1, \ldots, x_n). \end{cases}$$

Пример. Рассмотрим высказывание P: x – простое число, где $x \in \mathbb{N}$. Высказывание содержит переменную, значение которой определяет истнно P или ложно. $P(x)$ – одноместный предикат.

x	1	2	3	4	5	6	...
$\varphi_P(x)$	1	1	1	0	1	0	...

Теперь имеем табличное задание функции истинности $\varphi_P(x)$ предиката $P(x)$. Область определения этой функции – $\mathbb{N}$, множество значений $\{0, 1\}$.

Теперь заметим, что истинность предиката может зависеть от смыслового значения входящих в него переменных, а может зависеть только от значения истинности переменных. Например, истинность высказывания «если A, то x простое число» зависит от содержания высказывания A, а не только от значения истинности A. Но истинность высказывания «если A, то B» – зависит только от значений истинности высказываний A и B. Соответственно переменные в предикате могут быть высказывательные или нет.

Определение 1.2.10. Пропозициональная (высказывательная) переменная – *переменная, значениями которой являются только высказывания.*

Поскольку каждому высказыванию можно сопоставить значение – «истина» («true») или «ложь» («false»), то зачастую областью изменения пропозициональных переменных считают двухэлементное множество $\{T = 1, F = 0\}$ и дают другое определение высказывательных переменных (см. определение 1.2.11). Обозначаются пропозициональные переменные как правило большими буквами: $A, B, P, \ldots$.

Определение 1.2.11. *Если переменная* x_i *предиката* $P(x_1, \ldots, x_n)$ *принимает значения из множества* $\{0, 1\}$*, то она называется* **высказывательной.**

Набор переменных $x_1, x_2, \ldots, x_n$ предиката $P(x_1, x_2, \ldots, x_n)$ (см. определение 1.2.8) может содержать как пропозициональные переменные $x_j \in \{0, 1\}$, так и непропозициональные переменные $x_k \in B$, значения которых находятся в некотором множестве $B \neq \{0, 1\}$. Такие переменные будем называть **предметными.**

Определение 1.2.12. *Если множество изменения всех переменных x_i предиката $P(x_1, \ldots, x_n)$ есть $A = \{0, 1\}$ (т. е. все переменные являются высказывательными), то функция истинности предиката $P(x_1, \ldots, x_n)$ называется* **булевой функцией.**

Пример. Таблицы истинности простейших логических операций на стр. 17 есть табличное задание булевых функций $\varphi_P(A, B)$ от высказывательных переменных A и B. Например, если $P = A\&B = A \wedge B$, то

A	B	$\varphi_P(A, B)$
0	0	0
0	1	0
1	0	0
1	1	1

Область определения n-местного предиката, определенного на множестве A есть область определения его функции истинности, т. е. некоторое подмножество D из A^n.

Определение 1.2.13. *Будем говорить, что набор значений $(a_1, \ldots, a_n)$ принадлежит* **области истинности** *I_P предиката $P(x_1, \ldots, x_n)$, если $P(a_1, \ldots, a_n)$ истинное высказывание. Если высказывание $P(a_1, \ldots, a_n)$ ложно, то $(a_1, \ldots, a_n)$ принадлежит* **области ложности** *F_P предиката $P(x_1, \ldots, x_n)$.*

Таким образом $D = I_P \cup F_P$. Эквивалентная определению запись:
$I_P = \{(x_1, \ldots, x_n) | P(x_1, \ldots, x_n)\}$ или $F_P = \{(x_1, \ldots, x_n) | \neg P(x_1, \ldots, x_n)\} = \overline{I_P}$ – дополнение до множества D.

Замечание. Предикат есть высказывание, следовательно операции на множестве предикатов есть ограничения операций на высказываниях.

Операции на предикатах и области истинности

Пусть n-местные предикаты P и Q определены на множестве A и имеют одну область определения $D \subset A^n$. Тогда на этом же множестве определены предикаты:

1) $\neg P(x_1, \ldots, x_n)$ с областью истинности $\{(x_1, \ldots, x_n) | \neg P(x_1, \ldots, x_n)\} = \overline{I_P}$;

2) $P(x_1, \ldots, x_n) \wedge Q(x_1, \ldots, x_n)$ с областью истинности
$\{(x_1, \ldots, x_n) | P(x_1, \ldots, x_n) \wedge Q(x_1, \ldots, x_n)\} = I_P \cap I_Q$;

3) $P(x_1, \ldots, x_n) \vee Q(x_1, \ldots, x_n)$ с областью истинности
$\{(x_1, \ldots, x_n) | P(x_1, \ldots, x_n) \vee Q(x_1, \ldots, x_n)\} = I_P \cup I_Q$;

4) $P(x_1, \ldots, x_n) \Rightarrow Q(x_1, \ldots, x_n)$ что логически эквивалентно
$\neg P(x_1, \ldots, x_n) \vee Q(x_1, \ldots, x_n)$ с областью истинности: $\overline{I_P} \cup I_Q$;

5) $P(x_1,\ldots,x_n) \Leftrightarrow Q(x_1,\ldots,x_n)$ что логически эквивалентно $(P(x_1,\ldots,x_n) \Rightarrow Q(x_1,\ldots,x_n)) \wedge (Q(x_1,\ldots,x_n) \Rightarrow P(x_1,\ldots,x_n))$
с областью истинности: $(\overline{I_P} \cup I_Q) \cap (\overline{I_Q} \cup I_P)$.

Заметим, что указанные свойства областей истинности сопоставляют операциям на предикатах простейшие операции на множествах.

1.2.3. *Формулы логики высказываний*

В предыдущих разделах была проведена работа по переходу от анализа истинности высказывания с точки зрения его содержания (семантики) к анализу истинности высказывания с точки зрения его логического строения (синтаксиса). Здесь мы исследуем логическую конструкцию высказываний.

Определение 1.2.14. Пропозициональная формула (формула логики высказываний ФЛВ) – *это*
а) логические константы $1, 0$ *(это не числа, а значения истинности);*
б) пропозициональные переменные $A, B, C, \ldots$*;*
в) выражения вида $\neg\Phi, \Phi \vee \Psi, \Phi \wedge \Psi, \Phi \to \Psi, \Phi \leftrightarrow \Psi$*, если* $\Phi,\ \Psi$ *– ФЛВ.*

Пример.
1. Выражение $(A \to B) \vee (\neg C)$ есть ФЛВ, а $(A \to B)\neg C$ – не ФЛВ.
2. Выражение $(\neg(\neg A \to B)) \vee ((\neg C) \wedge 0)$ – ФЛВ, а $(\neg(\neg A \to B)) \vee \neg C \wedge 0$ не является ФЛВ, т. к. не расставлены скобки и операнды логических операций не определены. Однако подобные выражения мы будем рассматривать как ФЛВ, если примем соглашениео силе связок.

Соглашение. Для упрощения записи и уменьшения количества скобок упорядочим связки по старшинству:

$$\neg,\ \wedge,\ \vee,\ \to,\ \leftrightarrow .$$

Пример. В силу соглашения о старшинстве связок, выражение $(\neg(\neg A \to B)) \vee \neg C \wedge 0$ есть ФЛВ, причем скобки восстанавливаются однозначно:

$$(\neg(\neg A \to B)) \vee \neg C \wedge 0 = (\neg(\neg A \to B)) \vee ((\neg C) \wedge 0).$$

Но большее количество скобок в левой части уже убрать нельзя.

Определение 1.2.15. *Пусть* $\Phi(P_1, P_2, \ldots, P_n)$ *– ФЛВ, где* P_i *– пропозициональные переменные. Произвольное отображение множества переменных* P_i *в множество логических констант* $\{1, 0\}$ *называется* **интерпретацией формулы** Φ.

Формула, истинная при одной интерпретации, может быть ложной при другой. Значение истинности формулы Φ для интерпретации J будем обозначать $J(\Phi)$, т. е. $J(\Phi) \in \{1, 0\}$. Легко видеть, что если формула Φ зависит от n переменных, то Φ имеет в точности 2^n различных интерпретаций. Таблицу, в которой для каждой интерпретации формулы указывается ее истинностное значение, называют *таблицей истинности* ФЛВ. (Сравните с таблицами истинности для высказываний на стр. 17.)

Пример. Приведем таблицу истинности для ФЛВ Φ, оформив постепенное вычисление истинности, где $\Phi(A, B, C) = (A \to B \wedge C) \wedge (\neg A \to \neg B)$.

A	B	C	$\neg A$	$\neg B$	$B \wedge C$	$A \to B \wedge C$	$\neg A \to \neg B$	Φ
1	1	1	0	0	1	1	1	1
1	1	0	0	0	0	0	1	0
1	0	1	0	1	0	0	1	0
1	0	0	0	1	0	0	1	0
0	1	1	1	0	1	1	0	0
0	1	0	1	0	0	1	0	0
0	0	1	1	1	0	1	1	1
0	0	0	1	1	0	1	1	1

Определение 1.2.16. *Формула, истинная при некоторой интерпретации, называется* **выполнимой**. *Формула, истинная при всех возможных интерпретациях, называется* **общезначимой или тавтологией**. *Формула, ложная при всех возможных интерпретациях, называется* **невыполнимой или противоречием**.

Пример. $A \vee \neg A$ – тавтология, $A \wedge \neg A$ – противоречие. $A \to \neg A$ – выполнимая формула, т. к. импликация истинна если посылка A ложна (если $J(A) = 0$, то $J(A \to \neg A) = 1$). Если $J(A) = 1$, то $J(A \to \neg A) = 0$, значит формула выполнимая, но не тавтология.

Определение 1.2.17. *Пусть Φ, Ψ – пропозициональные формулы и для любой интерпретации J значения истинности совпадают: $J(\Phi) = J(\Psi)$, тогда Φ и Ψ* **логически эквивалентны.** *Обозначение: $\Phi \equiv \Psi$.*

Теорема 1.2.1. *Если Φ, Ψ, Ω – пропозицилональные формулы, то имеют место следующие свойства (законы логики высказываний):*
1) идемпотентность $\Phi \vee \Phi \equiv \Phi$, $\Phi \wedge \Phi \equiv \Phi$;
2) коммутативность $\Phi \vee \Psi \equiv \Psi \vee \Phi$, $\Phi \wedge \Psi \equiv \Psi \wedge \Phi$;

3) ассоциативность $\Phi \vee (\Psi \vee \Omega) \equiv (\Phi \vee \Psi) \vee \Omega$, $\Phi \wedge (\Psi \wedge \Omega) \equiv (\Phi \wedge \Psi) \wedge \Omega$;
4) дистрибутивность $\Phi \vee (\Psi \wedge \Omega) \equiv (\Phi \vee \Psi) \wedge (\Phi \vee \Omega)$,
$\Phi \wedge (\Psi \vee \Omega) \equiv (\Phi \wedge \Psi) \vee (\Phi \wedge \Omega)$;
5) поглощение $(\Phi \wedge \Psi) \vee \Phi \equiv \Phi$, $(\Phi \vee \Psi) \wedge \Phi \equiv \Phi$;
6) свойства нуля $\Phi \wedge 0 \equiv 0$, $\Phi \vee 0 \equiv \Phi$;
7) свойства единицы $\Phi \wedge 1 \equiv \Phi$, $\Phi \vee 1 \equiv 1$;
8) инволютивность $\neg(\neg\Phi) \equiv \Phi$;
9) законы двойственности де Моргана $\neg(\Phi \wedge \Psi) \equiv \neg\Phi \vee \neg\Psi$, $\neg(\Phi \vee \Psi) \equiv \neg\Phi \wedge \neg\Psi$;
10)закон исключенного третьего $\Phi \vee \neg\Phi \equiv 1$, *закон противоречия* $\Phi \wedge \neg\Phi \equiv 0$.

Доказательство приведенных свойств сводится к сравнению соответствующих таблиц истинности. Проверим, например, один из законов де Моргана:

$$\neg(\Phi \wedge \Psi) \equiv \neg\Phi \vee \neg\Psi$$

Φ	Ψ	$\Phi \wedge \Psi$	$\neg(\Phi \wedge \Psi)$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

Φ	Ψ	$\neg\Phi$	$\neg\Psi$	$\neg\Phi \vee \neg\Psi$
1	1	0	0	0
1	0	0	1	1
0	1	1	0	1
0	0	1	1	1

Замечание. 1. В теореме приведены свойства основных логических связок $\neg$, $\wedge$, $\vee$. Однако, импликация и эквиваленция могут быть выражены через них:

$$11)\Phi \to \Psi \equiv \neg\Phi \vee \Psi, \quad 12)\Phi \leftrightarrow \Psi \equiv (\Phi \to \Psi) \wedge (\Psi \to \Phi).$$

Также приведем «закон конртапозиции:»

$$13)\Phi \to \Psi \equiv \neg\Psi \to \neg\Phi.$$

Доказательство проводится с помощью таблиц истинности.

2. Теорема 1.2.1 почти дословно повторяет свойства теоретико-множественных операций, приведенных на стр. 13. Также, как и для множеств, свойства логических операций будем применять для преобразования ФЛВ.

Пример. Упростить ФЛВ $\neg A \wedge \neg(\neg A \wedge \neg B) \to B$.
Выпишем последовательность равносильных формул, указывая номер примененного закона из списка в теореме 1.2.1.

$$\neg A\wedge\neg(\neg A\wedge\neg B) \to B \overset{11}{\equiv} \neg(\neg A\wedge\neg(\neg A\wedge\neg B))\vee B \overset{9}{\equiv} (\neg\neg A\vee\neg\neg(\neg A\wedge\neg B))\vee B \overset{8}{\equiv}$$
$$\overset{8}{\equiv} (A\vee(\neg A\wedge\neg B))\vee B \overset{4}{\equiv} (A\vee\neg A)\wedge(A\vee\neg B)\vee B \overset{10}{\equiv} 1\wedge(A\vee\neg B)\vee B \overset{7}{\equiv} (A\vee\neg B)\vee B \overset{3}{\equiv}$$
$$\overset{3}{\equiv} A \vee (\neg B \vee B) \overset{10}{\equiv} A \vee 1 \overset{7}{\equiv} 1.$$

В частности эта формула является тавтологией.

1.2.4. *Логическое следование*

Далее на языке алгебры высказываний формализуем понятие теоремы. Как правило, теорема имеет следующую формулировку: пусть выполнены утверждения $A_1, A_2, \ldots, A_n$, тогда верно утверждение B.

Определение 1.2.18. *Пусть* Γ *– некоторое множество ФЛВ и* F *– произвольная ФЛВ. Будем говорить, что* F **логически следует из** Γ*, если для любой интерпретации множества формул* $\Gamma \cup \{F\}$ *из того, что каждая формула из* Γ *истинна следует, что и* F *истинна. Обозначение:* $\Gamma \models F$.

Пример. Пользуясь определением логического следования, покажем, что $\Gamma = \{A, A \to B\} \models B$. Действительно, рассмотрим интерпретацию формул из множества Γ такую, что обе формулы истинны. Но тогда

$$(J(A) = 1 \& J(A \to B) = 1) \Rightarrow (J(A) = 1 \& J(B) = 1).$$

Значит доказано, что B логически следует из Γ. Однако, также легко доказывается, что $\Gamma = \{B, A \to B\} \not\models A$.

Замечание. 1. Для любых ФЛВ F, G верно что $F \equiv G$ тогда и только тогда, когда $F \models G$ и $G \models F$.

2. В дальнейшем обозначение $\Gamma = \{F_1, \ldots, F_n\} \models G$ будем писать короче: $F_1, \ldots, F_n \models G$.

Теорема 1.2.2. *Для любых ФЛВ* $F_1, \ldots, F_n, G$ *выполнено:*

а) $F_1, \ldots, F_n \models G$ *тогда и только тогда, когда формула* $F_1 \wedge F_2 \ldots \wedge F_n \to G$ *является тавтологией;*

б) $F_1, \ldots, F_n \models G$ *тогда и только тогда, когда формула* $F_1 \wedge F_2 \ldots \wedge F_n \wedge \neg G$ *является противоречием.*

Доказательство. Докажем пункт а). Пусть $F_1, \ldots, F_n \models G$ и J – произвольная интерпретация формулы $F_1 \wedge F_2 \ldots \wedge F_n \to G$. Тогда если для некоторого $i \in \{1, \ldots, n\}$ выполнено $J(F_i) = 0$, то $J(F_1 \wedge F_2 \ldots \wedge F_n) = 0$ и, следовательно, $J(F_1 \wedge F_2 \ldots \wedge F_n \to G) = 1$. Если же для каждого $i \in \{1, \ldots, n\}$ имеем $J(F_i) = 1$, то ввиду $F_1, \ldots, F_n \models G$ выполнено $J(G) = 1$ и поэтому $J(F_1 \wedge F_2 \ldots \wedge F_n \to G) = 1$. Т. к. интерпретация выбрана произвольно, то доказано, что $F_1 \wedge F_2 \ldots \wedge F_n \to G$ является тавтологией.

Обратно, пусть $F_1 \wedge F_2 \ldots \wedge F_n \to G$ тавтология и $J(F_1) = 1, J(F_2) = 1, \ldots, J(F_n) = 1$. Тогда $J(F_1 \wedge F_2 \ldots \wedge F_n) = 1$ и $J(F_1 \wedge F_2 \ldots \wedge F_n \to G) = 1$, тогда $J(G) = 1$. Т. к. интерпретация J произвольная, то $F_1, \ldots, F_n \models G$.

Докажем пункт б). Заметим, что

$$\neg(F_1 \wedge F_2 \ldots \wedge F_n \to G) \equiv \neg(\neg(F_1 \wedge F_2 \ldots \wedge F_n) \vee G) \equiv$$

$$\equiv \neg\neg(F_1 \wedge F_2 \ldots \wedge F_n) \wedge \neg G \equiv F_1 \wedge F_2 \ldots \wedge F_n \wedge \neg G.$$

Поэтому формула $F_1 \wedge F_2 \ldots \wedge F_n \to G$ является тавтологией тогда и только тогда, когда формула $F_1 \wedge F_2 \ldots \wedge F_n \wedge \neg G$ – противоречие. Отсюда и из доказанного утверждения а) следует б). Теорема доказана.

Следствие. *Для ФЛВ F и G условие $F \vDash G$ равносильно тому, что $F \to G$ является тавтологией.* [1]

Понятие логического следования используется для анализа правильности рассуждений. Причем анализируется корректность именно логической конструкции, вне зависимости от смысла участвующих в ней высказываний.

Пример. Футбольная команда либо выигрывает матч, либо проигрывает, либо сводит его к ничьей. Если матч выигран или проигран, то он не перенесен. Команда матч не выиграла и не свела его к ничьей. Седовательно, матч не перенесен и проигран.

Проверим логичность приведенного рассуждения. Введем обозначения:
A – «матч выигран»,
B – «матч проигран»,
C – «матч закончился ничьей»,
D – «матч перенесен».
Тогда высказывания, входящие в рассуждение можно записать в виде ФЛВ:
$F_1 = A \vee B \vee C$ – «команда либо выигрывает матч, либо проигрывает, либо сводит его к ничьей»,
$F_2 = A \vee B \to \neg D$ – «если матч выигран или проигран, то он не перенесен»,
$F_3 = \neg A \wedge \neg C$ – «команда матч не выиграла и не свела его к ничьей»,
$G = \neg D \wedge B$ – «матч не перенесен и проигран».

Нужно проверить, что $F_1, F_2, F_3 \vDash G$.

Первый способ. Действуя по определению логического следования, рассмотрим произвольную интерпретацию J, такую, что $J(F_1) = J(F_2) = J(F_3) = 1$. Получим отсюда, что $J(G) = 1$. Итак,

$$\left.\begin{array}{l} J(F_3) = J(\neg A \wedge \neg C) = 1 \Leftrightarrow J(A) = J(C) = 0 \\ J(F_1) = J(A \vee B \vee C) = 1 \end{array}\right\} \Rightarrow J(B) = 1$$

$$\left.\begin{array}{l} J(A) = 0 \\ J(B) = 1 \end{array}\right\} \Rightarrow J(A \vee B) = 1$$

[1] Однако, логическое следование и импликация не является одним и тем же.

$$\left.\begin{array}{l} J(F_2) = J(A \vee B \to \neg D) = 1 \\ J(A \vee B) = 1 \end{array}\right\} \Rightarrow J(\neg D) = 1$$

$$\left.\begin{array}{l} J(B) = 1 \\ J(\neg D) = 1 \end{array}\right\} \Rightarrow J(\neg D \wedge B) = 1 = J(G).$$

Что и требовалось доказать.

Второй способ. Здесь воспользуемся теоремой, по которой достаточно проверить, что формула $F_1 \wedge F_2 \wedge F_3 \to G$ является тавтологией. Сделать это можно как с помощью таблицы истинности, так и преобразуя формулу с помощью свойств логических операций к 1.

Вычислим таблицу истинности:

A	B	C	D	F_1	F_2	F_3	G	$F_1 \wedge F_2 \wedge F_3 \to G$
1	1	1	1	1	0	0	0	1
1	1	1	0	1	1	0	1	1
1	0	1	1	1	0	0	0	1
1	1	0	1	1	0	0	0	1
1	0	0	0	1	1	1	0	1
0	1	1	1	1	0	0	0	1
...	...	...	...	...	...	...	...	...
0	0	1	1	1	1	0	0	1
0	0	0	1	0	1	0	1	1
0	0	0	0	0	1	1	1	1

В силу того, что в формуле 4 пропозициональные переменные, в таблице должно быть 16 строк. Из приведенных девяти, в подчеркнутой строке $J(F_1) = J(F_2) = J(F_3) = 1$. По свойствам импликации достаточно, вообще говоря, просчитать именно такие строки. Этот способ простой, но требует долгих вычислений.

Третий способ. Теперь преобразуем формулу с помощью свойств логических операций (см. стр. 21). Заметим, что следствием закона дистрибутивности и свойств 0 и 1 являются тождества:
(1) $(X \vee Y) \wedge \neg Y = X \wedge \neg Y$; (2) $(X \wedge Y) \vee \neg Y = X \vee \neg Y$.
Итак, нужно доказать:

$$(A \vee B \vee C) \wedge (A \vee B \to \neg D) \wedge (\neg A \wedge \neg C) \to G = 1.$$

Доказательство:
1) $F_2 = A \vee B \to \neg D = \neg(A \vee B) \vee \neg D = (\neg A \wedge \neg B) \vee \neg D = (\neg A \vee \neg D) \wedge (\neg B \vee \neg D)$;
2) $F_2 \wedge F_1 = (\neg A \vee \neg D) \wedge (\neg B \vee \neg D) \wedge (\neg A \wedge \neg C) =$ (закон поглощения)

$= ((\neg A \vee \neg D) \wedge \neg A) \wedge (\neg B \vee \neg D) \wedge \neg C = \neg A \wedge (\neg B \vee \neg D) \wedge \neg C$;
3) $F_1 \wedge F_2 \wedge F_3 = (A \vee (B \vee C)) \wedge (\neg A \wedge (\neg B \vee \neg D) \wedge \neg C) =$
$= [(A \vee (B \vee C)) \wedge \neg A] \wedge (\neg B \vee \neg D) \wedge \neg C =$ (см. (1))
$= [(B \vee C) \wedge \neg A] \wedge (\neg B \vee \neg D) \wedge \neg C = ((B \vee C) \wedge \neg C) \wedge \neg A \wedge (\neg B \vee \neg D) =$
$= (B \wedge \neg C) \wedge \neg A \wedge (\neg B \vee \neg D) = [B \wedge (\neg B \vee \neg D)] \wedge \neg A \wedge \neg C =$
$[B \wedge \neg D] \wedge \neg A \wedge \neg C$;
4) $F_1 \wedge F_2 \wedge F_3 \to G =$(закон импликации)$= \neg(B \wedge \neg D \wedge \neg A \wedge \neg C) \vee (\neg D \wedge B) =$
(закон двойственности)$= \neg B \vee D \vee A \vee C \vee (\neg D \wedge B) = \neg B \vee A \vee C \vee [(\neg D \wedge B) \vee D] =$
(см. (2)) $= \neg B \vee A \vee C \vee [B \vee D] = D \vee (B \vee \neg B) \vee A \vee C = D \vee 1 \vee A \vee C = 1$.

1.3. Булевы функции

Напомним, что мы отождествляем все логически эквивалентные (см. 1.2.2) высказывания. С другой стороны, логически эквивалентные высказывания реализуются эквивалентными ФЛВ (см. 1.2.17). А равносильные ФЛВ имеют одинаковые таблицы истинности. Но таблицы истинности есть таблично заданные функции нескольких переменных из множества $\{0,1\}$ в $\{0,1\}$. Используя понятие булевой функции (см. 1.2.12), имеем, что представителем класса эквивалентных высказываний является однозначно определенная булева функция.

1.3.1. *Элементарные булевы функции*

Дадим еще одно, независимое от понятия «высказывание» определение.

Определение 1.3.1. Булевой функцией *от n переменных называется функция с областью определения* $\underbrace{\{0,1\} \times \{0,1\} \times \ldots \times \{0,1\}}_{n \text{ раз}}$, *и областью значений, включающейся в* $\{0,1\}$.

Стандартными способами задания функций являются: формула, таблица, график. Например, функция $f(x,y)$ задается таблицей:

x	y	$f(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0

Иногда используют сокращенную таблицу, оставляя лишь те строки, в которых

$f(x, y) = 1$:

x	y	$f(x, y)$
0	1	1
1	0	1

.

Для небольшого количества переменных таблицей можно задать все булевы функции. Заметим, что количество булевых функций от n переменных равно 2^{2^n} (проверьте). Приведем все булевы функции от одной и от двух переменных.

Булевы функции одной переменной

	Переменная x	0	1
Название	Обозначение $f(x)$		
нуль	0	0	0
тождественная	x	0	1
отрицание	$\overline{x}$	1	0
единица	1	1	1

.

Булевы функции двух переменных

	Переменная x	0	0	1	1
	Переменная y	0	1	0	1
Название	Обозначение $f(x, y)$				
нуль	0	0	0	0	0
конъюнкция	$x \wedge y$	0	0	0	1
		0	0	1	0
		0	0	1	1
		0	1	0	0
		0	1	0	1
исключающее «или»	$x \oplus y$	0	1	1	0
дизъюнкция	$x \vee y$	0	1	1	1
стрелка Пирса	$x \downarrow y$	1	0	0	0
эквиваленция	$x \leftrightarrow y$	1	0	0	1
		1	0	1	0
		1	0	1	1
		1	1	0	0
импликация	$x \rightarrow y$	1	1	0	1
штрих Шеффера	$x \mid y$	1	1	1	0
единица	1	1	1	1	1

.

Замечание. 1. В приведенных таблицах перебор значений переменных x и y упорядочен по возрастанию чисел, представленных двоичной записью

$$xy : 00, 01, 10, 11.$$

Если придерживаться этой договоренности (лексикографического порядка), то каждая из булевых функций от n переменных может быть однозначно записана двоичной последовательностью длины 2^n. Например, последовательность (1001) соответствует эквиваленции. Такую запись называют *двоичный набор.*

2. Поскольку $x \wedge y = xy,\ x, y \in \{0, 1\}$ (конъюнкция совпадает с результатом обычного произведения чисел) функцию $x \wedge y$ называют *булево произведение.* По аналогии, а также в силу того, что дизъюнкция обладает некоторыми свойствами сложения чисел, функцию $x \vee y$ называют *булево сложение.* А таблица функции $x \oplus y$ в точности соответствует *сложению по модулю два* (см. на стр. 74 таблицу Кэли по сложению).

В таблицах отмечены **элементарные булевы функции: отрицание, конъюнкция, дизъюнкция, импликация, эквиваленция.**

На введенном множестве элементарных булевых функций рассмотрим операцию суперпозиции. Это способ получить более сложные функции с увеличением количества аргументов из элементарных функций двух и менее аргуменов. При этом можно одну и ту же функцию задать разными способами, записав ее разными формулами. В этом случае говорят о *реализации функции формулами.*

Определение 1.3.2. *Пусть $F = \{f_1, \ldots, f_m\}$ – некоторое множество булевых функций от n переменных.* **Формулой** $\mathcal{F}$ *над F называется выражение (цепочка символов) вида*

$$\mathcal{F}[F] = f(t_1, \ldots, t_n),$$

где $f \in F$ и t_i – либо переменная, либо формула над F. Множество F называется **базисом**, *функция f –* **главной (внешней)** *операцией, а t_i –* **подформулы** *формулы $\mathcal{F}$.*

Это определение практически эквивалентно определению ФЛВ. Таким образом, каждой формуле (ФЛВ) мы можем сопоставить (через таблицу истинности, например) булеву функцию, реализованную этой формулой. Но верно и обратное: для всякой булевой функции (заданной таблично) существует формула (ФЛВ), реализующая данную функцию. Прежде, чем доказывать это утверждение, отметим важные свойства элементарных булевых функций.

Свойства элементарных булевых функций

1) $x \wedge x = x;\ x \vee x = x;$

2) $x \wedge y = y \wedge x;\ x \vee y = y \vee x;$

3) $(x \wedge y) \wedge z = x \wedge (y \wedge z);\ (x \vee y) \vee z = x \vee (y \vee z);$

4) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z); \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z);$

5) $x \wedge (x \vee y) = x; \quad x \vee (x \wedge y) = x;$

6) $\overline{(\overline{x})} = x;$

7) $\overline{x \wedge y} = \overline{x} \vee \overline{y}$; $\overline{x \vee y} = \overline{x} \wedge \overline{y}$; законы де-Моргана

8) $\overline{x} \wedge x = 0;\ \overline{x} \vee x = 1;$

9) $x \to y = \overline{x} \vee y = \overline{x \wedge \overline{y}}$; $\overline{x \to y} = x \wedge \overline{y};$

10) $x \leftrightarrow y = (x \to y) \wedge (y \to x) = (x \wedge y) \vee (\overline{x} \wedge \overline{y});$

11) $x \wedge 1 = x, \quad x \wedge 0 = 0, \quad x \vee 1 = 1, \quad x \vee 0 = x.$

Докажем соотношение 6: $\overline{(\overline{x})} = x$.

Сравнивая таблицы истинности, получаем:

x	$\overline{x}$	$\overline{(\overline{x})}$
0	1	0
1	0	1

.

Откуда следует доказываемое равенство. В частности формулы x и $\overline{(\overline{x})}$ реализуют одну и ту же тождественную булеву функцию. Так же можно доказать и остальные соотношения.

Определение 1.3.3. *Система булевых функций* $\{f_1, f_2, \ldots, f_n\}$ *называется* **полной системой булевых функций**, *если любая булева функция может быть представлена формулой, содержащей только обозначения переменных, обозначения функций (логических связок) из списка* $\{f_1, \ldots, f_n\}$, *и скобки.*

Теорема 1.3.1 (о полных системах булевых функций). *Следующие системы булевых функций (логических связок) являются полными: 1)* $\{\&, \vee, \neg, \to, \leftrightarrow\}$; *2)* $\{\&, \vee, \neg\}$; *3)* $\{\&, \neg\}$; *4)* $\{\vee, \neg\}$.

В теореме утверждается, что любая булева функция, которая (по определению) реализуется формулой, содержащей связки из пункта 1) теоремы, может быть реализована с помощью связок из пункта 4) (или 2) или 3)). Более того, следующей нашей целью станет нахождение стандартных (нормальных) форм записи для логических функций.

1.3.2. *Дизъюнктивные нормальные формы*

Определение 1.3.4. *Пусть x – переменная булевой функции. Назовем выражение $x^{\sigma(a)}$* **литерой** *переменной x, если*

$$x^{\sigma(a)} = \begin{cases} x^{\sigma(1)} = x, & \text{если } a = 1 \\ x^{\sigma(0)} = \overline{x} = \neg x, & \text{если } a = 0 \end{cases}$$

Соответственно **элементарной конъюнкцией** *назовем конъюнкцию одной или нескольких литер различных переменных.*

Заметим, что элементарные конъюнкции, которые различаются перестановкой литер, мы не различаем. Элементарные конъюнкции: $\neg z \wedge y \wedge \neg x = \neg x \wedge \neg z \wedge y$. Но функции $\neg x \wedge x$ и $\neg x \wedge \neg z \vee y$ не являются элементарными конъюнкциями.

Теорема 1.3.2 (теорема о дизъюнктивной нормальной форме). *Для любой булевой функции f, не равной нулю тождественно, справедливо равенство*

$$f(x_1; \ldots; x_n) = \bigvee_{f(a_1;\ldots;a_n)=1} \left(x_1^{\sigma(a_1)} \wedge \ldots \wedge x_n^{\sigma(a_n)} \right).$$

Доказательство. Проверим, что для всякого набора $(b_1; \ldots; b_n)$ значений переменных $(x_1; \ldots; x_n)$ значения функции f в левой части совпадает со значением функции в правой части формулы из заключения теоремы. Очевидно, что

$$\left(b_1^{\sigma(a_1)} \wedge \ldots \wedge b_n^{\sigma(a_n)} \right) = \begin{cases} 1, \text{ если } (a_1; \ldots; a_n) = (b_1; \ldots; b_n), \\ 0, \text{ если } (a_1; \ldots; a_n) \neq (b_1; \ldots; b_n), \end{cases}$$

поскольку $0^{\sigma(0)} = \overline{0} = \neg 0 = 1 = 1^{\sigma(1)}$, $\quad 0^{\sigma(1)} = 0 = \overline{1} = \neg 1 = 1^{\sigma(0)}$. Следовательно, если $f(b_1; \ldots; b_n) = 1$, то

$$\bigvee_{f(a_1;\ldots;a_n)=1} \left(b_1^{\sigma(a_1)} \wedge \ldots \wedge b_n^{\sigma(a_n)} \right) = \left(b_1^{\sigma(b_1)} \wedge \ldots \wedge b_n^{\sigma(b_n)} \right) \vee \ldots = 1.$$

Наоборот, если $f(b_1; \ldots; b_n) = 0$, то в выражении $\bigvee_{f(a_1;\ldots;a_n)=1} \left(b_1^{\sigma(a_1)} \wedge \ldots \wedge b_n^{\sigma(a_n)} \right)$ все «дизъюнкты» («слагаемые» относительно операции $\vee$) равны 0. Значит, и все это выражение равно 0. Теорема доказана.

Пример. Построим формулу, задающую булеву функцию $f(x_1, x_2, x_3)$, которая принимает значение 1 тогда и только тогда, когда большинство ее переменных принимает значение 1. Построим сокращенную таблицу значений (истин-

ности) для функции f:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1

.

По условию, для остальных наборов переменных x_i функция принимает значение 0. Действуя по доказанной теореме, составляем формулу, содержащую 4 элементарные конъюнкции:

$$f(x_1, x_2, x_3) = (x_1^{\sigma(1)} \wedge x_2^{\sigma(1)} \wedge x_3^{\sigma(1)}) \vee (x_1^{\sigma(1)} \wedge x_2^{\sigma(1)} \wedge x_3^{\sigma(0)}) \vee$$

$$\vee (x_1^{\sigma(1)} \wedge x_2^{\sigma(0)} \wedge x_3^{\sigma(1)}) \vee (x_1^{\sigma(0)} \wedge x_2^{\sigma(1)} \wedge x_3^{\sigma(1)}) =$$

$$= (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3).$$

Определение 1.3.5. *Реализация булевой функции формулой называется дизъюнктивной нормальной формой –* **ДНФ**, *если эта формула является дизъюнкцией одной или нескольких элементарных конъюнкций. Если ДНФ состоит из элементарных конъюнкций, зависящих от одного и того же набора переменных, то она называется совершенной –* **СДНФ**.

Пример. 1. Формула, полученная в предыдущем примере:
$(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3)$ – СДНФ.
2. Формула $(x \vee y) \wedge (x \vee \neg z)$ не является ДНФ, но может быть эквивалентными преобразованиями приведена как к ДНФ $x \vee (y \wedge \neg z)$ так и к ДНФ $(x \wedge \neg y) \vee (y \wedge \neg z) \vee (x \wedge y)$.

Как доказано в теореме 1.3.2, всякая булева функция реализуется некоторой СДНФ. Более того, такая реализация единственна (покажем в следующей теореме). Таким образом, если есть алгоритм построения СДНФ для булевой функции (по таблице или по некоторой, реализующей функцию формуле), то значит есть алгоритм проверки равенства булевых функций. В частности, решен вопрос о распознавании эквивалентных логических формул (имеет место *разрешимость*).

Теорема 1.3.3 (теорема о СДНФ). *Всякая булева функция, тождественно не равная 0, реализуется СДНФ, которая определяется по набору переменных однозначно с точностью до перестановки элементарных конъюнкций.*

Доказательство. В теореме 1.3.2 доказано существование СДНФ для каждой булевой функции. Докажем единственность, т. е. покажем, что набор элементарных конъюнкций в каждой СДНФ одинаков. Рассмотрим элементарную конъюнкцию в некоторой СДНФ для функции $f(x_1, x_2, \ldots, x_n)$:

$$x_1^{\sigma(a_1)} \wedge \ldots \wedge x_n^{\sigma(a_n)}, \quad a_i \in \{0, 1\}.$$

Поскольку СДНФ – дизъюнкция элементарных конъюнкций, то если для набора $(b_1; \ldots; b_n)$ имеем $b_1^{\sigma(a_1)} \wedge \ldots \wedge b_n^{\sigma(a_n)} = 1$, то (как было показано в доказательстве теоремы 1.3.2) $(b_1; \ldots; b_n) = (a_1; \ldots; a_n)$. Верно и обратное. Другими словами: для любой элементарной конъюнкции из произвольной СДНФ имеем:

$$x_1^{\sigma(a_1)} \wedge \ldots \wedge x_n^{\sigma(a_n)}, \quad f(a_1, \ldots, a_n) = 1.$$

Тем самым доказано, что всякая СДНФ вычисляется по формуле из теоремы 1.3.2. Единственность доказана.

Рассмотрим два способа нахождения СДНФ заданной булевой функции: табличный (по табличному заданию функции) и с помощью эквивалентных преобразований формулы, реализующей данную функцию. В примере на стр. 30 СДНФ была найдена **табличным способом**.

Способ эквивалентных преобразований преобразует формулу, используя свойства булевых функций (см. стр. 29):
1) избавляемся от эквиваленции и импликации с помощью свойств 9) и 10);
2) применяя законы де-Моргана, дистрибутивности и двойного отрицания (свойства 7), 4), 6)), приводим формулу к ДНФ;
3) от ДНФ к СДНФ переходим, добавляя в каждую элементарную конъюнкцию F недостающие переменные x_i, используя следствие упоминавшихся свойств:

$$(F \wedge x_i) \vee (F \wedge \overline{x_i}) = F,$$

при необходимости с помощью закона идемпотентности (свойство 1)) добиваемся, чтобы все элементарные конъюнкции в формуле были попарно различны.

Пример. Эквивалентными преобразованиями приведем формулу $(x_1 \leftrightarrow x_2) \to x_3$ к СДНФ. Реализуем алгоритм пошагово, подписывая номера использованных свойств.
1) $(x_1 \leftrightarrow x_2) \to x_3 \overset{10}{=} (x_1 \to x_2) \wedge (x_2 \to x_1) \to x_3 \overset{9}{=} \overline{((\overline{x_1} \vee x_2) \wedge (\overline{x_2} \vee x_1))} \vee x_3 =$
2) $\overset{7,6}{=} (x_1 \wedge \overline{x_2}) \vee (x_2 \wedge \overline{x_1}) \vee x_3 =$
3) $= (x_1 \wedge \overline{x_2} \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (x_2 \wedge \overline{x_1} \wedge x_3) \vee (x_2 \wedge \overline{x_1} \wedge \overline{x_3}) \vee (x_3 \wedge x_1) \vee (x_3 \wedge \overline{x_1}) =$
$= \underbrace{(x_1 \wedge \overline{x_2} \wedge x_3)} \vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee \underbrace{(x_2 \wedge \overline{x_1} \wedge x_3)} \vee (x_2 \wedge \overline{x_1} \wedge \overline{x_3}) \vee$
$\vee (x_3 \wedge x_1 \wedge x_2) \vee \underbrace{(x_3 \wedge x_1 \wedge \overline{x_2})} \vee \underbrace{(x_3 \wedge \overline{x_1} \wedge x_2)} \vee (x_3 \wedge \overline{x_1} \wedge \overline{x_2}) =$

$\overset{1,2}{=} (x_1 \wedge \overline{x_2} \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge \overline{x_3}) \vee (x_1 \wedge x_2 \wedge x_3) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_3)$.
Задача решена.

1.3.3. *Принцип двойственности*

Определение 1.3.6. *Пусть $f(x_1, x_2, \ldots, x_n)$ – булева функция. Тогда функция $f^*(x_1, x_2, \ldots, x_n)$, определенная следующим образом*

$$f^*(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$$

называется **двойственной** *к f.*

Если в табличном задании функции f инвертировать все значения, то получим таблицу функции f^* :

x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

.

x_1	x_2	$(x_1 \wedge x_2)^* = x_1 \vee x_2$
1	1	1
1	0	1
0	1	1
0	0	0

.

Выпишем двойственные к элементарным булевым функциям:

f	x	$\neg x$	$x_1 \wedge x_2$	$x_1 \vee x_2$	1	0
f^*	x	$\neg x$	$x_1 \vee x_2$	$x_1 \wedge x_2$	0	1

.

Замечание. 1. Не нужно путать двойственную формулу с отрицанием. Например:

$$(x_1 \wedge x_2)^* = x_1 \vee x_2 \neq \neg(x_1 \wedge x_2) = \neg x_1 \vee \neg x_2.$$

2. Как видно из приведенной таблицы, конъюнкция не *самодвойственная* функция, т. е. $f \neq f^*$. Тождественная функция и отрицание являются самодвойственными, т. е. $f = f^*$.
3. Для всякой булевой функции $f = (f^*)^*$.

Теорема 1.3.4 (теорема о реализации двойственной функции). *Если функция $\varphi(x_1, \ldots, x_n)$ реализована формулой*

$$f(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)),$$

то формула

$$f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_k^*(x_1, \ldots, x_n)),$$

реализует функцию $\varphi^*(x_1, \ldots, x_n)$.

Доказательство. Для упрощения записи примем обозначение: $\overline{f(\ldots)} = \overline{f}(\ldots)$. Тогда по определению двойственной функции имеем:

$$\varphi^*(x_1,\ldots,x_n) = \overline{\varphi}(\overline{x_1},\ldots,\overline{x_n}) = \overline{f}(f_1(\overline{x_1},\ldots,\overline{x_n}),\ldots,f_k(\overline{x_1},\ldots,\overline{x_n})) =$$

$$= \overline{f}(\overline{f_1}(\overline{x_1},\ldots,\overline{x_n}),\ldots,\overline{f_k}(\overline{x_1},\ldots,\overline{x_n})) =$$

$$= \overline{f}(\overline{f_1^*}(x_1,\ldots,x_n),\ldots,\overline{f_k^*}(x_1,\ldots,x_n)) = f^*(f_1^*(x_1,\ldots,x_n),\ldots,f_k^*(x_1,\ldots,x_n)).$$

Теорема доказана.

Следующая теорема является следствием доказанной теоремы.

Теорема 1.3.5 (принцип двойственности). *Пусть $F = \{f_1,\ldots,f_m\}$ – система булевых функций, а $F^* = \{f_1^*,\ldots,f_m^*\}$ – система двойственных функций. Тогда если формула $\mathcal{F}$ реализует функцию f над базисом F, то формула $\mathcal{F}^*$, полученная заменой в $\mathcal{F}$ функций f_i на f_i^*, реализует функцию f^* над базисом F^*.*

Определение 1.3.7. *Реализация булевой функции формулой называется конъюнктивной нормальной формой –* **КНФ**, *если эта формула является конъюнкцией одной или нескольких элементарных дизъюнкций. Если КНФ состоит из элементарных дизъюнкций, зависящих от одного и того же набора переменных, то она называется совершенной –* **СКНФ**.

Из принципа двойственности вытекает следующая теорема.

Теорема 1.3.6 (теорема о СКНФ). *Всякая булева функция, тождественно не равная 1, реализуется СКНФ, которая определяется по набору переменных однозначно с точностью до перестановки элементарных дизъюнкций. СКНФ вычисляется по формуле*

$$f(x_1;\ldots;x_n) = \bigwedge_{f^*(a_1;\ldots;a_n)=1} \left(x_1^{\sigma(a_1)} \vee \ldots \vee x_n^{\sigma(a_n)}\right).$$

Пример. Проиллюстрируем теорему, вычислив СКНФ функции $f(x_1,x_2) = x_1 \wedge x_2$ через СДНФ двойственной функции $f^*(x_1,x_2) = x_1 \vee x_2$. Действительно, имеем

$$f^*(x_1,x_2) = x_1 \vee x_2 = (x_1 \wedge x_2) \vee (x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \text{ – СДНФ}$$

Поскольку $f(x_1,x_2) = \overline{f^*(\overline{x_1},\overline{x_2})}$, получим

$f(x_1,x_2) = \overline{(\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge \overline{\overline{x_2}}) \vee (\overline{\overline{x_1}} \wedge \overline{x_2})} = (x_1 \vee x_2) \wedge (x_1 \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_2)$ – СКНФ.

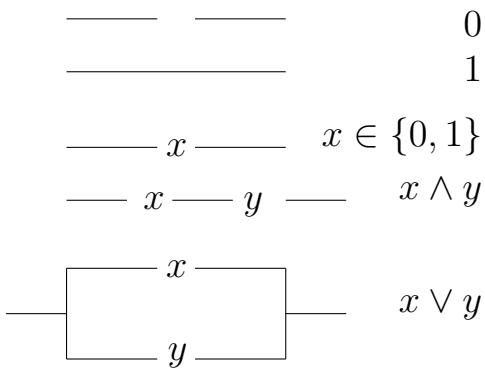

Рис. 1.4. Элементарные контактные схемы

1.3.4. *Контактные схемы*

Применение булевых функций (логики высказываний) не ограничивается изучением корректности рассуждений. Есть и технические приложения этой теории: например, в электротехнике (в контактно-релейных схемах), в химии (описание химического синтеза), в вычислительной технике и т. д.

Назовем **контактом** устройство, которое может находиться в двух состояниях: замкнутом (состояние 1) или разомкнутом (состояние 0). Обозначать контакты будем также как переменные булевых функций: $x, y, \ldots$. Если два контакта всегда находятся в одинаковом состоянии, то мы обозначаем их одной и той же буквой. Если контакт y замкнут тогда и только тогда, когда контакт x разомкнут, то пишем: $y = \overline{x}$. Если контакт всегда замкнут, то обозначаем его 1, если контакт всегда разомкнут, то обозначаем его 0. Контакты x и y, соединенные последовательно обозначим: $x \wedge y$; контакты x и y, соединенные параллельно обозначим: $x \vee y$.

Назовем **элементарными контактными схемами** элементы списка (см. рис. 1.4):

$$1,\ 0,\ x,\ \overline{x},\ x \wedge y,\ x \vee y.$$

Понятно, что это список элементарных булевых функций, причем контактная схема замкнута (проводит ток) тогда и только тогда, когда соответствующая булева функция принимает значение 1.

Теперь индуктивно определим произвольную **контактную схему** S:
1) S – элементарная контактная схема; 2) если S_1 и S_2 – контактные схемы, то их последовательное соединение (обозначение $S_1 \wedge S_2 = S$) или параллельное соединение (обозначение $S_1 \vee S_2 = S$) тоже контактные схемы.

Пример контактной схемы приведен на рисунке 1.5 *b*). Состояние каждой контактной схемы S зависит от состояния ее контактов $x, y, \ldots$ точно также как

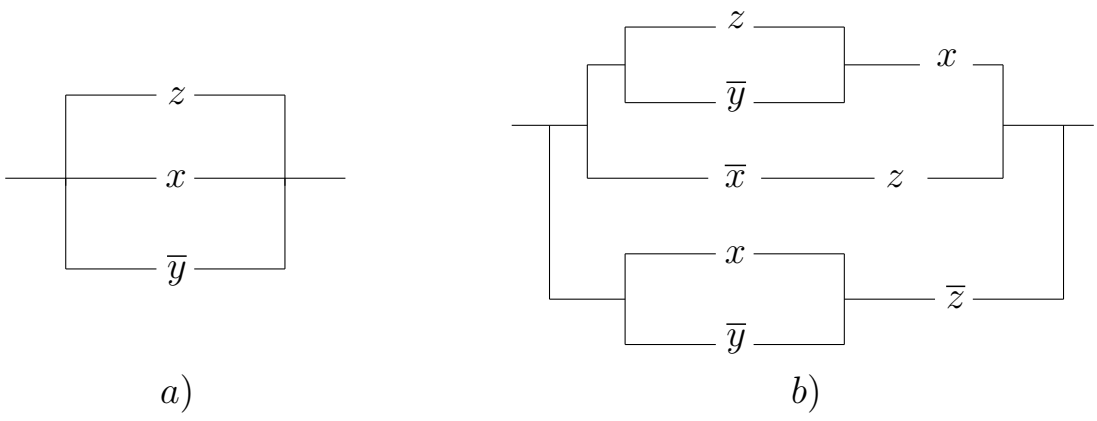

Рис. 1.5. Эквивалентные контактные схемы

значение булевой функции зависит от значения ее аргументов. Для каждой контактной схемы можно построить формулу соответствующей булевой функции. Например, для схемы на рисунке 1.5 *b*) формула имеет вид:

$$(x \wedge (z \vee \overline{y})) \vee (\overline{x} \wedge z) \vee ((x \vee \overline{y}) \wedge \overline{z}).$$

Верно и обратное: если $f(x_1, x_2, \ldots, x_k)$ – булева функция, реализуемая формулой, в которой $\overline{(\ )}$ (т. е. «не») относится только к переменным x_i, то по формуле легко восстановить контактную схему. Каждому набору состояний контактов для данной схемы взаимно-однозначно сопоставляется набор значений булевых переменных $x_i \in \{0, 1\}$.

Две схемы называются **эквивалентными**, если они имеют один набор контактов и при одинаковых значениях контактов схемы либо одновременно замкнуты либо одновременно разомкнуты. Это означает, что соответствующие эквивалентным схемам булевы функции одинаковы. Однако, формулы, соответствующие разным схемам – разные, т. е. представляют собой различные реализации одной функции.

Задача упрощения контактной схемы заключается в построении схемы, эквивалентной первоначальной, но, по возможности, с меньшим числом контактов. На языке булевых функций, это означает упрощение формулы, реализующей данную функцию (или нахождение одной из минимальных форм).

Пример. Упростить контактную схему, изображенную на рис. 1.5 *b*). Воспользуемся свойствами логических операций (элементарных булевых функций):

$$(x \wedge (z \vee \overline{y})) \vee (\overline{x} \wedge z) \vee ((x \vee \overline{y}) \wedge \overline{z}) = (x \wedge z) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge z) \vee ((x \vee \overline{y}) \wedge \overline{z}) =$$

$$= z \vee (x \wedge \overline{y}) \vee ((x \vee \overline{y}) \wedge \overline{z}) = ((z \vee x \vee \overline{y}) \wedge (z \vee \overline{z}) \vee (x \wedge \overline{y}) =$$

$$= z \vee x \vee \overline{y} \vee (x \wedge \overline{y}) = z \vee x \vee \overline{y}.$$

Соответствующая схема изображена на рисунке 1.5 *a*).

1.4. Отношения

1.4.1. *n*-местные отношения

Определение 1.4.1. ***n*-местным отношением** *на множестве A называется произвольное подмножество* $\mathbf{P}$ *множества* A^n.

Если $\mathbf{P} = A^n$, отношение $\mathbf{P}$ называется **универсальным отношением**.

Соответствие между предикатами и отношениями

Предикату P на множестве A будем ставить в соответствие отношение $\mathbf{P} \subseteq A^n$, определенное формулой: $\mathbf{P} = \left\{(a_1, a_2, \ldots, a_n) \,\middle|\, P(a_1, a_2, \ldots, a_n)\right\} = I_P$ и совпадающее с областью истинности предиката P. В частности, если φ – функция истинности предиката, то этому предикату соответствует отношение

$$\mathbf{P}_{(\varphi=1)} = \left\{(a_1, a_2, \ldots, a_n) \,\middle|\, \varphi(a_1, a_2, \ldots, a_n) = 1\right\}. \tag{1.1}$$

Переход от отношения $\mathbf{P}$ к предикату P осуществляется с помощью формулы:

$$P(a_1, a_2, \ldots, a_n) \quad \Leftrightarrow \quad (a_1, a_2, \ldots, a_n) \in \mathbf{P}. \tag{1.2}$$

Таким образом, отношения можно задавать на языке теории множеств и на языке логики предикатов.

Пример. На множестве $A = \{-1, 0, 1, 2, 3\}$ зададим отношения $\mathbf{Q}$ и $\mathbf{P}$.

1. $(x, y) \in \mathbf{Q} \Leftrightarrow x < y^2$. Предикат Q, задающий бинарное (двухместное) отношение $\mathbf{Q}$, формулируется так: $((x, y) \in A^2)\&(x < y^2)$. Областью истинности I_Q этого предиката является множество пар:
$\mathbf{Q} = \{(-1, 0), (-1, 1), (-1, 2), (-1, 3), (0, 1)(0, 2), (0, 3), (0, -1)(1, 2), (1, 3)(2, 3)\}$.
2. $(x, y, z) \in \mathbf{P} \Leftrightarrow z = \text{ОД}(x, y)$. Предикат P, задающий тернарное (трехместное) отношение $\mathbf{P}$, формулируется так: $((x, y, z) \in A^3)\&(z = \text{ОД}(x, y))$, где ОД - общий делитель чисел x и y. Областью истинности I_P этого предиката является множество троек:
$\mathbf{P} = \{(-1, 0, -1), (-1, 0, 1), (0, -1, 1), (0, -1, -1), (0, 1, 1), (0, 1, -1), (1, 0, -1),$
$(1, 0, 1), (1, 2, 1), (2, 1, 1), (1, 2, -1), (2, 1, -1,)(2, 3, 1), (3, 2, 1), (2, 3, -1), (3, 2, -1)\}$.

Алгебра отношений

Поскольку отношения – множества, то на них определены теоретико-множественные операции. Этим операциям соответствуют логические операции на предикатах, для которых отношения являются областями истинности. Операции на отношениях носят обычно логические названия. Все свойства логических (теоретико-множественных) операций выполнены (см. стр. 13).

1.4.2. *Бинарные отношения*

Определение 1.4.2. Бинарным (двухместным) отношением *на множестве A называется произвольное подмножество* $\mathbf{P}$ *множества* A^2.

Бинарные отношения хорошо известны и привычны в математике. Это, например, отношение меньше на множестве действительных чисел, отношение равенства, отношение быть подмножеством на множестве подмножеств и т. п. Привычные обозначения в этом случае имеют вид: $x < y$, $x = y$, $x \subset y$. Значок отношения при этом находится между компонентами пары, входящей в данное отношение. Поэтому введем для бинарного отношения p *специальное обозначение*: xpy. Таким образом, $(I_P = \mathbf{P} = \{(x,y)\big|\ P(x,y)\} \subset A^2) \Leftrightarrow (xpy)$. Здесь $P(x.y)$ – некоторый предикат.

Пример. 1. Универсальное отношение: $x\omega y \Leftrightarrow I_\omega = A^2$.

Пустое отношение: $x\nu y \Leftrightarrow I_\nu = \emptyset$.

Равенство (диагональ): $x\delta y \Leftrightarrow I_\delta = \{(x,x)|x \in A\}$.

2. График функции $\varphi(a)$ на множестве A есть бинарное отношение $\Gamma_\varphi = \{(a, \varphi(a))|a \in A\}$.

Пример. Рассмотрим отношение делимости p на множестве $A = \{1,2,3,4,5,6\}$, т. е. xpy, если x делит y. Зададим p на языке предикатов и теории множеств:

Язык предикатов	Язык теории множеств
P : (x делит y) $\Leftrightarrow (x\|y)$	$\mathbf{P} = \{(1,2),(1,3),(1,4),(1,5),(1,6),$ $(2,2),(1,1),(2,4),(3,6),(3,3),(4,4),(5,5),(6,6)\} = I_P$

Для описания бинарных отношений используются также и графы. Однако, отметим, что сейчас мы действуем вне поля строгого определения графа, используя лишь изображение (диаграмму) графа.

Язык ориентированных графов

Пусть бинарное отношение r определено на множестве A, состоящем из небольшого числа элементов. Каждому элементу a множества A взаимно однозначным образом поставим в соответствие точку плоскости $g(a)$, называемую **вершиной графа**, и из точки $g(a)$ в точку $g(b)$ будет идти стрелка (называемая **дугой графа**) тогда и только тогда, когда arb. Если дуга идет из $g(a)$ в эту же точку, то есть ara, то такая дуга называется **петлей**. Полученное изображение на плоскости назовем **графом бинарного отношения** r и будем обозначать $\Gamma(r)$.

Алгебра бинарных отношений

Если p и q бинарные отношения, тогда

Операция	Язык предикатов	Язык теории множеств
пересечение (конъюнкция) $p \cap q = p \wedge q$	$P \wedge Q$	$\mathbf{P} \cap \mathbf{Q} = I_P \cap I_Q$
объединение (дизъюнкция) $p \cup q = p \vee q$	$P \vee Q$	$\mathbf{P} \cup \mathbf{Q} = I_P \cup I_Q$
дополнение (отрицание) $\neg p = \overline{p}$	$\neg P$	$\overline{\mathbf{P}} = \overline{I_P}$
обращение p^{-1}	$P^{-1} \equiv (x,y) \in \mathbf{P^{-1}}$	$\mathbf{P^{-1}} = I_{P^{-1}} = = \{(x,y) \mid (y,x) \in \mathbf{P}\}$
произведение $r = pq$	$R \equiv (x,y) \in \mathbf{R}$	$\mathbf{R} = I_R = \{(x,y) \mid \exists z : (x,z) \in \mathbf{P} \& (z,y) \in \mathbf{Q}\}$

Замечание. 1. Если p – бинарное отношение, ν – пустое отношение, δ – диагональ, то $\delta p = p\delta = p, \quad \nu p = p\nu = \nu$.

2. Если ω – универсальное отношение, то найдется отношение p для которого равенство $p\omega = \omega p = \omega$ нарушается.

Пример. 1. Дополнение отношения меньше или равно «$\leq$» на числовом множестве A есть отношение « $>$ » – строго больше.

2. Если Γ_{φ_1} и Γ_{φ_2} – графики функций φ_1 и φ_2 на множестве A (т. е. области определения есть A, множества значений из A), то произведение отношений $\gamma_{\varphi_1}\gamma_{\varphi_2}$ совпадает с графиком суперпозиции функций: $\varphi_2\varphi_1(a) = \varphi_2(\varphi_1(a)), a \in A$.

Свойства операций

I. Свойства теоретико-множественных операций переносятся (см. стр. 13).

II. Свойства умножения и обращения сформулируем в виде теорем.

Теорема 1.4.1 (ассоциативность умножения). *Для любых бинарных отношений p, q, r, заданных на множестве A, имеем $p(qr) = (pq)r$.*

Доказательство. На языке множеств: требуется доказать совпадение подмножеств из A^2, определенных левой и правой частями равенств: $I_{p(qr)} = I_{(pq)r}$.

Пусть $(x,y) \in I_{p(qr)}$. Тогда $\exists z : xpz \ \& \ z(qr)y$. Снова по определению произведения: $\exists t : zqt \ \& \ try$.

Итак $(\exists t \exists z : xpz \ \& \ zqt) \Rightarrow x(pq)t$ и try, т. е. $x(pq)ry \Leftrightarrow (x,y) \in I_{(pq)r}$.

Получено включение $I_{p(qr)} \subseteq I_{(pq)r}$. Прочитав цепочку рассуждений справа налево, получим обратное включение. Теорема доказана.

Теорема 1.4.2 (свойства обращения). *Если p и q – бинарные отношения на множестве A, тогда*

$$(p \cup q)^{-1} = p^{-1} \cup q^{-1}, \quad (p \cap q)^{-1} = p^{-1} \cap q^{-1}, \quad (\overline{p})^{-1} = \overline{p^{-1}}$$

Доказательство. Докажем первое равенство по определению (на языке теории множеств): $I_{(p\cup q)^{-1}} = I_{p^{-1}\cup q^{-1}}$. Пусть $(x, y) \in I_{(p\cup q)^{-1}}$, тогда
$(y, x) \in I_{p\cup q} \Rightarrow ((y, x) \in I_p \vee (y, x) \in I_q) \Rightarrow ((x, y) \in I_{p^{-1}} \vee (x, y) \in I_{q^{-1}}) \Rightarrow$

$$\Rightarrow (x, y) \in I_{p^{-1}\cup q^{-1}}$$

Итак, $I_{(p\cup q)^{-1}} \subseteq I_{p^{-1}\cup q^{-1}}$. Обратное включение доказывается обращением стрелок в рассуждении. Теорема доказана.

Теорема 1.4.3 (связь обращения и произведения). *Если p и q – бинарные отношения на множестве A, то*

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

Теорема 1.4.4 (связь объединения и произведения). *Если p, q и r – бинарные отношения на множестве A, то*

$$(p \cup q)r = (pr) \cup (qr), \quad r(p \cup q) = (rp) \cup (rq).$$

Две последние теоремы доказываются также на основании определений.

Замечание. Аналогичное свойство для пересечения неверно. Можно привести пример отношения p, для которого $(p \cap \overline{p})\omega = \omega(p \cap \overline{p}) = \nu$ – пустое отношение (ω – универсальное отношение), но $(p\omega) \cap (\overline{p}\omega) \neq \nu$.

Определение 1.4.3. *Бинарное отношение p, определенное на множестве A* **индуцирует** *бинарное отношение p_B на подмножестве B множества A, если $I_{P_B} = I_P \cap (B \times B)$.*

В таблице приведены определения некоторых важных свойств бинарного отношения p, заданного на множестве A.

Свойство p	Язык предикатов	Язык множеств	Язык графов
рефлексивность	$\forall a \in A\ apa$	$I_\delta \subseteq I_P$	всякая вершина снабжена петлей
симметричность	$apb \Rightarrow bpa$	$I_P = I_{P^{-1}}$	всякая дуга имеет обратную
транзитивность	$(apb\ \&\ bpc) \Rightarrow apc$	$I_{P^2} \subseteq I_P$	все треугольники замкнуты
антисимметричность	$(apb\ \&\ bpa) \Rightarrow a = b$	$I_P \cap I_{P^{-1}} \subseteq I_\delta$	обратная дуга есть только у петли

1.4.3. *Отношения и матрицы*

Рассмотрим числовое множество $\mathbb{K} = \{0, 1\}$, на котором зададим операции булева сложения и булева умножения (см. стр. 28):

$+ = \vee$	0	1
0	0	1
1	1	1

$\bullet = \wedge$	0	1
0	0	0
1	0	1

.

Теперь рассмотрим все квадратные матрицы размерности $n \times n$ над множеством $\mathbb{K}$, т. е. матрицы из нулей и единиц. Используя обычные определения матричных операций и правила действий в $\mathbb{K}$, мы можем любые две матрицы складывать, умножать, транспонировать. Добавим к этому списку операции *инвертирование* и *вычитание*. Выпишем определения всех операций.
Пусть $R = (R_{ij}),\ Q = (Q_{ij}),\ 1 \le i, j \le n$, тогда
булево сложение матриц $R + Q = (R_{ij} + Q_{ij} = R_{ij} \vee Q_{ij})$;
булево умножение матриц $R \cdot Q = (\sum\limits_{k=1}^{n} R_{ik} \cdot Q_{kj} = \bigvee\limits_{k=1}^{n} R_{ik} \wedge Q_{kj})$;
транспонирование $R^T = (R_{ji})$;
инвертирование $\overline{R} = (1 - R_{ij} = \overline{R}_{ij})$;
вычитание $R - Q = (R_{ij} \cdot (1 - Q_{ij}) = R_{ij} \wedge \overline{Q}_{ij})$.

Полученное множество квадратных матриц размерности $n \times n$ над множеством $\mathbb{K}$, называют **булевы матрицы**.

Опишем бинарные отношения на языке матриц. Пусть множество A – конечно и содержит n элементов. Перенумеруем их: $A = \{a_1, a_2, \ldots, a_n\}$. Если на множестве A задано бинарное отношение r, то сопоставим ему матрицу R из нулей и единиц:

$$R_{ij} = 1 \Leftrightarrow a_i r a_j;\ R = (R_{ij}),\ 1 \le i, j \le n.$$

Теперь установим связь между операциями на бинарных отношениях и операциями на булевых матрицах, представляющих эти отношения.

Теорема 1.4.5. *Пусть на конечном множестве $A = \{a_1, a_2, \ldots, a_n\}$ заданы бинарные отношения r, q. Пусть $R = (R_{ij}),\ Q = (Q_{ij}),\ 1 \le i, j \le n$ – матрицы, представляющие эти отношения, тогда верны следующие утверждения:*

1) если $p = r^{-1}$, то $P = R^T$;

2) если $p = \overline{r}$, то $P = \overline{R}$;

3) если $p = rq$, то $P = R \cdot Q$, в частности, если $p = r^k$, то $P = R^k$;

4) если $p = r \vee q$, то $P = R + Q$,
где матрица P представляет отношение p.

Доказательство. Утверждения 1) и 2) – очевидные следствия определений. Докажем утверждение 3).

$$(a_i, a_j) \in rq \Leftrightarrow \exists a_k \in A(a_i r a_k \& a_k q a_j) \Leftrightarrow$$

$$\Leftrightarrow \exists k(R_{ik} = 1 \& Q_{kj} = 1) \Leftrightarrow \exists k(R_{ik} \cdot Q_{kj} = 1) \Leftrightarrow \sum_{s=1}^{n} R_{is} \cdot Q_{sj} = 1 \Leftrightarrow (R \cdot Q)_{ij} = 1.$$

Докажем утверждение 4).

$$(a_i, a_j) \in r \vee q \Leftrightarrow a_i r a_j \vee a_i q a_j \Leftrightarrow$$

$$\Leftrightarrow R_{ij} = 1 \vee Q_{ij} = 1 \Leftrightarrow R_{ij} + Q_{ij} = 1 \Leftrightarrow (R + Q)_{ij} = 1.$$

Теорема доказана.

Пример. На множестве $A = \{1, 2, 3\}$ задано бинарное отношение r : $I_r = \{(1, 2), (2, 2), (3, 2), (2, 1)\}$. Сопоставить r матрицу. Найти отношение r^3.

Запишем матрицу R отношения r и вычислим ее степени, учитывая, что $1 + 1 = 1$:

$$R = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, R^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 & 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 & 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 \\ 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 & 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 \\ 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 & 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 & 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

$$R^3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} = R^3$$

Заметим, что матрица R^3 совпадает с матрицей R^2. Более того, $R^k = R^2$ и, соответственно, $r^k = r^2$ для любой степени $k \geq 3$. Элементы множества $I_{r^k} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}$ описывают искомые отношения на теоретико-множественном языке. Можно проверить, что отношение r^2 является транзитивным, в отличае от первоначального отношения r.

1.4.4. *Рефлексивное, симметричное, транзитивное замыкания*

Определение 1.4.4. *Если p – бинарное отношение на множестве A, то его* **рефлексивным замыканием** *p_1 называется наименьшее рефлексивное бинарное отношение на множестве A, содержащее p.*

Определение 1.4.5. *Если p – бинарное отношение на множестве A, то его* **симметричным замыканием** *p_2 называется наименьшее симметричное бинарное отношение на множестве A, содержащее p.*

Определение 1.4.6. *Если p – бинарное отношение на множестве A, то его* **транзитивным замыканием** *p_3 называется наименьшее транзитивное бинарное отношение на множестве A, содержащее p.*

Используя операции на бинарных отношениях, можно записать очевидные равенства: $p_1 = p \cup \delta$, $p_2 = p \cup p^{-1}$. Что касается транзитивного замыкания, то очевидным является лишь включение $p \cup p^2 \subseteq p_3$. Обратное включение, вообще говоря, неверно. Строение транзитивного замыкания раскрывают лемма и теорема.

Лемма 1.4.1 (Свойства степеней бинарных отношений). *Если p – бинарное отношение на множестве A, тога*

1) если $xp^k y$, $k \geq 1$, то существуют элементы $c_1, \ldots, c_{k-1}$ (т. н. посредники) такие, что $xpc_1 \& c_1 pc_2 \& \ldots \& c_{k-1} py$, (на языке графов: граф отношения p содержит направленную ломаную, состоящую из $k-1$ дуги и соединяющую вершины x и y);

2) для любых натуральных чисел m, n имеет место равенство: $p^n p^m = p^{n+m}$;

3) если p транзитивно, то оно содержит любую свою натуральную степень: $p^n \subseteq p$, (на языке графов: замкнуты не только направленные ломаные из двух звеньев (треугольники), но и направленные ломаные любой длины).

Теорема 1.4.6. *Если p – бинарное отношение на множестве A, то его транзитивное замыкание t выражается формулой*

$$t = \bigcup_{k=1}^{\infty} p^k.$$

Доказательство. Сначала покажем, что $\bigcup_{k=1}^{\infty} p^k \subseteq t$. Рассуждая индукцией по k получим $p^k \subseteq t$. Действительно, если для $(x, y) \in A^2$ $xp^k y$, то $\exists z : xp^{k-1}z \ \& \ zpy$. По предположению индукции $p^{k-1} \subseteq t$, т. е. xtz и $p \subseteq t$ поэтому zty. Тогда, в силу транзитивности t, xty.

Для доказательства обратного включения $t \subseteq \bigcup_{k=1}^{\infty} p^k$, в силу минимальности t, нужно проверить, что отношение $\bigcup_{k=1}^{\infty} p^k$ транзитивно. Пусть $x(\bigcup_{k=1}^{\infty} p^k)z \;\&\; z(\bigcup_{k=1}^{\infty} p^k)y$. Тогда найдутся натуральные показатели m, n такие, что $xp^n z \;\&\; zp^m y$. По определению произведения отношений, получим $xp^{n+m}y$ а значит $x(\bigcup_{k=1}^{\infty} p^k)y$.

Следствие. Если $A = \{a_1, a_2, \ldots, a_n\}$ – конечное множество из n элементов,на котором задано отношение p. Тогда транзитивное замыкание p вычисляется по формуле

$$t = \bigcup_{k=1}^{n-1} p^k.$$

Доказательство. Пусть atb для некоторых элементов $a, b \in A$. Докажем, что найдется показатель $k < n$ такой, что $ap^k b$. Поскольку $t = \bigcup_{k=1}^{\infty} p^k$, найдется показатель m (необязательно меньше, чем n) такой, что $ap^m b$. Тогда

$$ap^m b \Rightarrow \exists c_1, \ldots, c_{m-1} \in A : a = c_0 p c_1 p c_2 \ldots p c_{m-1} p c_m = b.$$

Если $m \geq n$, то в списке $c_0, c_1, \ldots, c_{m-1}, c_m$ по крайней мере $n+1$ элемент. Но тогда найдутся два одинаковых элемента $c_i = c_j$. Отбросив посредников между равными элементами, получим

$$a = c_0 p c_1 p c_2 \ldots c_{i-1} p c_i = c_j p c_{j+1} \ldots p c_{m-1} p c_m = b \Rightarrow ap^{m-(j-i)}b.$$

Продолжая таким же образом, получим цепочку из различных элементов c_i, но тогда количество k «соединений» p меньше, чем n, т. е. $ap^k b,\ k < n$. Следствие доказано.

Алгоритм Уоршелла[1]

Для нахождения транзитивного замыкания бинарного отношения p, заданного на множестве A, состоящем из n элементов существует алгоритм Уоршелла. Используя описание бинарных отношений на языке булевых матриц и используя формулу транзитивного замыкания, получим следующий алгоритм. Строим матрицу отношения p – $P = (p_{ij})$. Тогда матрица транзитивного замыкания имеет вид

$$T = \sum_{k=1}^{n-1} P^k.$$

На языке теории графов суть алгоритма заключается в том, что замыкаются все направленные ломаные в орграфе отношения p.

Программная реализация матричной формулы выглядит так:

[1] Стивен Уоршелл (р. 1935)

На входе: матрица отношения p – $p_{ij} \in \{0,1\}$
На выходе: матрица отношения t – $t_{ij} \in \{0,1\}$ – транзитивного замыкания p
Цикл по i от 1 до n
Цикл по j от 1 до n
Цикл по k от 1 до n
$t_{jk} := p_{jk} \vee p_{ji} \& p_{ik}$
Конец цикла
Конец цикла
$p := t$
Конец цикла

1.4.5. *Отношение эквивалентности*

Определение 1.4.7. *Бинарное отношение p, определенне на множестве A и удовлетворяющее свойствам рефлексивности, симметричности и транзитивности называется* **эквивалентностью.**

Пример. На множестве целых чисел $\mathbb{Z}$ отношение $p : xpy \Leftrightarrow 3 \Big| (x-y)$ (т. е. $x-y$ делится на 3) является эквивалентностью.

Определение 1.4.8. Разбиением множества *A называется выбор такой системы непустых подмножеств (классов разбиения), когда каждый элемент из A принадлежит точно одному подмножеству (классу).*

Определение 1.4.9. *Пусть p – отношение эквивалентности, определенное на множестве A . Тогда назовем p* **-классом элемента** *a(классом эквивалентности) множество*

$$a^p = \{b \mid apb,\ b \in A\}.$$

Лемма 1.4.2 (о свойствах классов эквивалентности). *Если p – отношение эквивалентности, то*
1) все элементы из a^p находятся в отношении p друг с другом;
2)для любого x из a^p имеем $x^p = a^p$;
3)ни один элемент из A, не входящий в a^p, не находится в отношении p ни с одним элементом из a^p.

Доказательство.
1. Докажем: $\forall y, z \in a^p \ \ ypz$.

Пусть $y, z \in a^p$. Тогда, используя симметричность и транзитивность p, получим

$$apy \ \& \ apz \ \Rightarrow \ ypa \ \& \ apz \ \Rightarrow \ ypz,$$

что и требовалось.

2. Докажем: $\forall x \in a^p \ \ x^p = a^p$.

Из соображений симметрии, достаточно доказать включение $x^p \subseteq a^p$. Возьмем $z \in x^p$.

$$z \in x^p \ \& \ a \in x^p \ \Rightarrow \ xpz \ \& \ xpa \ \Rightarrow \ zpx \ \& \ xpa \ \Rightarrow \ zpa \ \Rightarrow \ z \in a^p.$$

3. Докажем: $\forall x \notin a^p \ \ x^p \cap a^p = \emptyset$.

Будем рассуждать «от противного»:

$$\exists y \notin a^p : \ \exists z \in y^p \cap a^p \ \Rightarrow \ ypz \ \& \ apz$$

Тогда, по свойству 2),

$$y^p = z^p = a^p$$

Следовательно, $y \in a^p$, противоречие.

Лемма доказана.

Теорема 1.4.7 (критерий отношения эквивалентности). *Отношение p является отношением эквивалентности на множестве A тогда и только тогда, когда p определяет на A разбиение такое, что любые два элемента, находящиеся в отношении p, принадлежат одному классу разбиения, а любые два элемента, не находящиеся в отношении p, не принадлежат одному классу.*

Доказательство. 1. Пусть p является отношением эквивалентности на множестве A. Рассмотрим систему различных p - классов элементов множества A. Отметим два свойства такой системы подмножеств:

$$1)\forall a \in A \ \ a \in a^p \ \Rightarrow \ A = \bigcup_{a \in A} a^p; \ \ 2) \ a^p \cap b^p \neq \emptyset \ \Rightarrow \ a^p = b^p.$$

Первое утверждение очевидно. Второе – логически эквивалентно свойству 3) классов эквивалентности (см. лемму).

Таким образом, множество различных p - классов эквивалентных элементов образует множество классов разбиения множества A, причем любые два элемента множества A находятся в отношении p тогда и только тогда, когда принадлежат одному классу разбиения (лемма, свойства 2) и 3)). Необходимость доказана.

2. Докажем достаточность. Пусть имеется некоторое разбиение множества A:

$$A = \bigcup_{i \in I} A_i.$$

Определим бинарное отношение p на A:

$$apb \Leftrightarrow a \in A_i \ \& \ b \in A_i.$$

Очевидно, что отношение p обладает свойствами рефлексивности, симметричности и транзитивности, т. е. является эквивалентностью. Осталось показать, что p - классы эквивалентности совпадают с классами разбиения:

$$\forall a \in A \ \exists i \in I : a^p = A_i.$$

Понятно, что каждый элемент $a \in A$ содержится в некотором A_i. Но тогда $a^p \subseteq A_i$ и $A_i \subseteq a^p$ по определению p. Теорема доказана.

Пример. Классами эквивалентных элементов для отношения p делимости на три ($xpy \Leftrightarrow 3 \Big| (x - y)$) являются множества, состоящие из целых чисел с одинаковыми остатками от деления на три (классы вычетов по модулю 3).

Замечание. Теорема полностью описывает все эквивалентности на множестве A и дает инструмент задания эквивалентности как некоторого разбиения множества A.

Определение 1.4.10. *Если p – отношение эквивалентности на множестве A, то множество p - классов эквивалентности называется* **фактор-множеством** *A/p множества A по отношению p.*

1.4.6. *Упорядоченные множества*

Определение 1.4.11. *Бинарное отношение p, определенное на множестве A и удовлетворяющее свойствам рефлексивности, антисимметричности и транзитивности называется* **отношением частичного порядка.** *Множество A с заданным на нем отношением частичного порядка называется* **частично упорядоченным множеством** *(ЧУМ).*

Пример. На множестве всех подмножеств множества A (на булеане 2^A) отношение включения как подмножества «$\subseteq$» является частичным порядком. На множестве действительных чисел $\mathbb{R}$ отношение меньше или равно «$\leq$» также частичный порядок.

Определение 1.4.12. *Если на множестве A задано отношение частичного порядка p и xpy, то элементы x, y называются* **сравнимыми.**

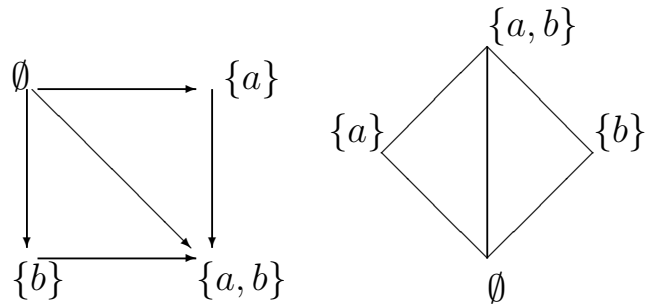

Рис. 1.6. Диаграммы ЧУМ

Определение 1.4.13. *Если на множестве A задано отношение частичного порядка p, то такой элемент $m \in A$, что для каждого $x \in A$ либо mpx либо m и x несравнимы, называется* **минимальным в множестве** A.

Частично упорядоченные множества (особенно конечные) удобно изображать с помощью диаграммы. Диаграмма – это неориентированный граф бинарного отношения, в котором направление каждой дуги однозначно восстанавливается по расположению вершин (ниже-выше).

Пример. На булеане $2^A = \Big\{\emptyset, \{a\}, \{b\}, \{a, b\}\Big\}$ двухэлементного множества $A = \{a, b\}$ рассмотрим отношение частичного порядка «$\subseteq$». Изобразим ориентированный граф этого отношения и диаграмму на рис. 1.6. Элемент $\emptyset$ является минимальным (и наименьшим), а элементы $\{a\}$ и $\{b\}$ несравнимы.

Определение 1.4.14. *Отношение частичного порядка p называется* **отношением линейного порядка**, *если в A нет несравнимых элементов, т. е.*

$$\forall x, y \in A \quad xpy \vee ypx.$$

Соответственно множество A называется **линейно упорядоченным множеством** *(ЛУМ) или цепью.*

Определение 1.4.15. *Если на множестве A задано отношение частичного порядка p, то такой элемент $M \in A$, что*

$$\forall x \in A \quad Mpx \ (xpM)$$

называется **наименьшим (наибольшим) в множестве** A

Определение 1.4.16. *Отношение частичного порядка p называется* **отношением полного порядка** *на множестве A, если в любом подмножестве $B \subseteq A$ найдется наименьший элемент.*

Заметим, что минимальных элементов может быть много, а наименьшего элемента при этом нет.

Теорема 1.4.8 (об отношении полного порядка). *Если r – отношение полного порядка на множестве A, то справедливы следующие утверждения:*

1) r является отношением линейного порядка;

2) Если элемент x из A не является наибольшим в A, то среди элементов множества A, «больших» чем x, существует наименьший элемент, то есть такой элемент $y \in A$, что

- $x \neq y$;
- xry;
- $\forall z \in A(xrz \;\&\; x \neq z) \;\Rightarrow\; yrz$.

Доказательство. 1. Если $x, y \in A$, то, по определению полного порядка, во множестве $\{x, y\}$ имеется наименьший элемент. Это либо x, тогда xry, либо y, тогда yrx, т. е. r – линейный порядок.

2. Пусть $x \in A$. Рассмотрим множество

$$B = \left\{ z \,\middle|\, z \in A \;\&\; z \neq x \;\&\; xrz \right\}.$$

Тогда, по определению отношения полного порядка, в B найдется наименьший элемент y. Тогда, так как $y \in B$, то, во-первых, $x \neq y$, во-вторых, xry, и, в-третьих,

$$\forall z \in A \quad (xrz \;\&\; x \neq z) \;\Rightarrow\; (z \in B) \;\Rightarrow\; yrz,$$

что и требовалось доказать.

Сформулируем без докавзательства следующие теоремы.

Теорема 1.4.9. *К вполне упорядоченным множествам и только к ним применим принцип математической индукции.*

Теорема 1.4.10 (Цермело). [2] *Всякое множество можно вполне упорядочить.*

Эти теоремы позволяют обобщить метод математической индукции для ЧУМ натуральных чисел с отношением «$\leq$» на множество произвольной мощности с соответствующим отношением линейного порядка. Таким образом, есть возможность использовать для доказательства теорем «обобщенную индукцию».

[2] Эрнст Фридрих Фердинанд Цермело (1871–1953) - немецкий математик, внесший значительный вклад в теорию множеств и создание аксиоматических оснований математики.

ГЛАВА 2

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

2.1. Универсальные алгебры

2.1.1. *Алгебраические операции, определение алгебры*

Определение 2.1.1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется функция с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Пример. 1. Бинарная операция сложения целых чисел отображает $\mathbb{Z} \times \mathbb{Z}$ в $\mathbb{Z}$, она *паре* целых чисел a, b ставит в соответствие целое число $a + b$.

2. Унарная операция обращения целых чисел отображает $\mathbb{Z}$ в $\mathbb{Z}$, она *одному* целому числу a ставит в соответствие целое число $-a$.

3. Особую роль играют 0-арные операции, то есть константы. Например, числа 1 и 0 играют особую роль в теории целых чисел, их можно рассматривать как значения соответствующих 0-арных операций.

Обычно образ элемента x относительно операции f обозначают через $f(x)$. Для бинарных алгебраических операций обычно используют другой способ обозначения образа: вместо $f(x, y)$ его обозначают через $x * y$, где $*$ – обозначение алгебраической операции. Например, мы пишем $x + y$, $x \cdot y$, $x - y$ и т. п.

Определение 2.1.2. Алгеброй (универсальной алгеброй) *называется упорядоченная пара $\mathcal{A} = \langle A, \mathcal{F} \rangle$, где A – некоторое непустое множество, называемое* **носителем** *алгебры $\mathcal{A}$, и $\mathcal{F}$ – множество операций , определенных на A, называемое* **сигнатурой** *алгебры $\mathcal{A}$.*

Пример. На одном и том же непустом множестве можно определить различные алгебры. Например, на множестве натуральных чисел можно определить алгебру $\langle \mathbb{N}, \{+\} \rangle$, а можно – алгебру $\langle \mathbb{N}, \{\cdot, 1\} \rangle$. Можно рассмотреть и «более богатую» (в смысле множества операций) алгебру $\langle \mathbb{N}, \{+, \cdot, 1\} \rangle$.

Определение 2.1.3. *Если в алгебре* $\mathcal{A} = \langle A, \mathcal{F} \rangle$ *подмножество* $B \subseteq A$, *замкнуто относительно любой* n*-арной операции из* $\mathcal{F}$*:*

$$\forall f \in \mathcal{F}\ \forall a_1, \ldots, a_n,\ a_i \in B, f(a_1, \ldots, a_n) \in B,$$

то $\mathcal{B} = \langle B, \mathcal{F}^1 \rangle$ *называется* **подалгеброй** *алгебры* $\mathcal{A}$. *Обозначение:* $\mathcal{B} \leq \mathcal{A}$.

Пример. 1. В алгебре $\langle \mathbb{R}, +, \cdot \rangle$ среди конечных подмножеств относительно обеих операций замкнуто только множество $\{0\}$. Однако бесконечными подалгебрами являются $\langle \mathbb{Q}, +, \cdot \rangle$ и $\langle \mathbb{Z}, +, \cdot \rangle$.

2. Алгебра подмножеств множества M: $\langle 2^M, \cup, \cap, ^- \rangle$ в качестве подалгебры содержит алгебру подмножеств $\langle 2^X, \cup, \cap, ^- \rangle$ любого множества $X \subseteq M$.

3. Алгебра дифференцируемых функций $\langle \{f | f : \mathbb{R} \to \mathbb{R}\}, \frac{d}{dx} \rangle$ содержит алгебру полиномов $\mathbb{R}[x]$.

Теорема 2.1.1. *Непустое пересечение подалгебр некоторой алгебры образует подалгебру этой же алгебры.*

Доказательство. Пусть $\mathcal{B}_i \leq \mathcal{A} = \langle A, \mathcal{F} \rangle,\ i \in I$ и $a_k \in \bigcap_{i \in I} B_i,\ 1 \leq k \leq n$. Тогда поскольку алгебры $\mathcal{B}_i$ замкнуты относительно любой операции f_j из $\mathcal{F}$,

$$\forall i (\forall f_j \in \mathcal{F},\ f(a_1, \ldots, a_n) \in B_i) \Rightarrow\ \forall j\ f(a_1, \ldots, a_n) \in \bigcap_{i \in I} B_i.$$

Что и требовалось доказать.

Определение 2.1.4. *Говорят, что* **множество** M **порождает алгебру** $\mathcal{A}$ *(соответственно* $\mathcal{A}$ *является* **замыканием** M *относительно сигнатуры* $\mathcal{F}$*), если каждый элемент из* $\mathcal{A}$ *есть результат применения конечного числа операций из* $\mathcal{F}$ *к элементам из* M. *Обозначение:* $< M >= \mathcal{A}$.

Определение 2.1.5. *Множество* $M \subseteq A$ *называется* **системой образующих** *алгебры* $\mathcal{A} = \langle A, \mathcal{F} \rangle$, *если* $< M >= \mathcal{A}$. *Если алгебра имеет конечную систему образующих, то она называется* **конечнопорожденной.** *Если система образующих состоит из одного элемента, то алгебра называется* **циклической.**

Пример. 1. Циклической алгеброй является $\langle \mathbb{N}, + \rangle =< 1 >$.

2. Замыкание множества $M = \{x\}$ относительно сигнатуры $\mathcal{F} = \{+, \cdot\}$ состоит из всех выражений, которые можно построить из переменной x с помощью операций сложения и умножения. Эти выражения есть полиномы от x с натуральными коэффициентами любой степени и без свободных членов. Таким образом,

$$\mathbb{N}[x] \setminus \mathbb{N} =< x >, \quad \mathcal{F} = \{+, \cdot\}.$$

[1] строго говоря, *ограничения* операций f на подмножестве B

2.1.2. *Некоторые классические алгебры*

Пусть $*$ и $\circ$ – некоторые бинарные операции из множества $\mathcal{F}$ алгебры $\mathcal{A} = \langle A, \mathcal{F}\rangle$, и $a, b, c \in A$. Отметим некоторые часто встречающиеся **свойства бинарных операций.**

1. *Ассоциативность* $*$: $\forall a, b, c \in A \;\; (a * b) * c = a * (b * c)$.

2. Коммутативность $*$: $\forall a, b, \in A \;\; a * b = b * a$.

3. Дистрибутивность $\circ$ *относительно* $*$ *слева:*
$\forall a, b, c \in A \;\; a \circ (b * c) = (a \circ b) * (a \circ c)$

4. Дистрибутивность $\circ$ *относительно* $*$ *справа:*
$\forall a, b, c \in A \;\; (a * b) \circ c = (a \circ c) * (b \circ c)$

5. Поглощение ($\circ$ *поглощает* $*$): $(a * b) \circ a = a$.

Пример. 1. Ассоциативные и коммутативные операции: сложение и умножение чисел, объединение и пересечение множеств. Неассоциативная (и некоммутативная)– вычитание чисел.

2. Объединение множеств поглощает пересечение, а пересечение поглощает объединение.

Различные типы алгебр определяются набором операций и их свойств (другими словами – аксиомами).

Определение 2.1.6. *Пусть A – некоторое непустое множество, $*$ – бинарная операция на этом множестве. Тогда алгебра $\langle A, \{*\}\rangle$ называется* **группоидом**.

Пример.Группоидами являются алгебры $\langle \mathbb{N}, \{+\}\rangle$, $\langle \mathbb{Z}, \{\cdot\}\rangle$, $\langle \mathbb{N}, \{-\}\rangle$, $\langle \mathbb{Q}, \{\max\}\rangle$, где max – бинарная операция, выбирающая из элементов x, y максимальный, и т. п.

Определение 2.1.7. *Группоид $\langle A, \{*\}\rangle$ называется* **полугруппой**, *если $*$ – ассоциативная операция, то есть выполняется тождество $(x * y) * z = x * (y * z)$.*

Определение 2.1.8. *Пусть A – некоторое непустое множество, $*$ – бинарная операция, определенная на этом множестве, e – 0-местная операция на A, то есть e – некоторый элемент из A, называемый* **нейтральным (единичным)**. *Алгебра $\langle A, \{*, e\}\rangle$ называется* **группой**, *если выполняются следующие утверждения (аксиомы группы):*
1) $\forall x, y, z \in A \;\; (x * y) * z = x * (y * z)$ *– аксиома ассоциативности;*
2) $\forall x \in A \; x * e = e * x = x$ *– аксиома существования нейтрального элемента;*
3) $\forall x \in A \; \exists \tilde{x} : \; x * \tilde{x} = \tilde{x} * x = e$ *– аксиома существования обратного элемента.*

Пример. Группой является алгебра $\langle \mathbb{Z}, \{+, 0\}\rangle$, т. к. ассоциативность сложения и свойства нейтрального элемента 0 очевидно выполнены.

Пример. Зададим на множестве $A = \{a, b, c\}$ операции таблицами:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Выяснить, какие из этих операций являются коммутативными и какие из группоидов $\langle A, \{+\}\rangle$, $\langle A, \{*\}\rangle$, $\langle A, \{\ominus\}\rangle$, $\langle A, \{\odot\}\rangle$, являются полугруппами. Выяснить, в каких из этих группоидов имеются нейтральные элементы и какие из них становятся группами после добавления во множество операций соответствующего нейтрального элемента.

Решение. Таблицы, задающие операции называются **таблицы Кэли**. Изучим свойства для каждой из заданных операций.

Как нетрудно увидеть, коммутативными являются операции $+, *, \ominus$, а операция $\odot$ коммутативной не является, так как, например, $a \odot b = c$, но $b \odot a = b$.

Непосредственная проверка ассоциативности операции дает: операции $+, *, \ominus$ ассоциативны, а операция $\odot$ – не ассоциативная.

Таким образом, группоиды $\langle A, \{+\}\rangle$, $\langle A, \{*\}\rangle$ и $\langle A, \{\ominus\}\rangle$, являются полугруппами. Группоид $\langle A, \{\odot\}\rangle$ полугруппой не является, так как, например, $(a \odot b) \odot b = c \odot b = b$, но $a \odot (b \odot b) = a \odot a = a$, то есть $(a \odot b) \odot b \neq a \odot (b \odot b)$.

Очевидно, что в группоиде $\langle A, \{+\}\rangle$ элемент a является нейтральным. В группоиде $\langle A, \{*\}\rangle$ также имеется нейтральный элемент: это b. А вот в группоидах $\langle A, \{\ominus\}\rangle$ и $\langle A, \{\odot\}\rangle$ нет ни одного нейтрального элемента (легко показать, что если в полугруппе нейтральный элемент существует, то он единственный).

Из рассмотренных четырех группоидов только $\langle A, \{+\}\rangle$ является группой. Обратные элементы задаются следующей таблицей:

x	a	b	c
$\tilde{x}$	a	c	b

Определение 2.1.9. *Группа с коммутативной групповой операцией называется* **коммутативной группой** *или* **абелевой группой**.

Не все группы коммутативны.

Определение 2.1.10. Кольцом *или* **ассоциативным кольцом** *называется алгебра $\langle K, \{+, \cdot, 0\}\rangle$ для которой выполняются следующие утверждения (***аксиомы кольца***):*

1) $x + y = y + x$ *(коммутативность «сложения»);*

2) $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*

3) в K *существует элемент, который мы обозначим* 0*, такой, что* $\forall x \in K \quad x + 0 = x$*;*

4) $\forall x \in K \ \exists(-x) : (-x) + x = 0$ *(элемент, обратный относительно* $+$*);*

5) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(ассоциативность «умножения»);*

6) $x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x$ *(левая и правая дистрибутивности).*

Определение 2.1.11. *Пусть* A *– непустое множество,* $+, \cdot$ *– операции на множестве* A*, и* $\mathbf{0}, \mathbf{1}$ *– элементы множества* A*. Тогда алгебра* $\langle A, \{+, \cdot, \mathbf{0}, \mathbf{1}\}\rangle$ *называется* **полем** *тогда и только тогда, когда выполняются следующие утверждения (аксиомы поля):*

1) $\langle A, \{+, \mathbf{0}\}\rangle$ *– абелева (коммутативная) группа;*

2) $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ *– абелева (коммутативная) группа;*

3) $a \cdot (b + c) = a \cdot b + a \cdot c$ *и* $(b + c) \cdot a = b \cdot a + c \cdot a$ *– дистрибутивность.*

При этом группа $\langle A, \{+, \mathbf{0}\}\rangle$ *называется* **аддитивной группой поля.** $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ *называется* **мультипликативной группой поля**.

Обобщением понятия универсальной алгебры является понятие алгебраической системы.

Определение 2.1.12. Алгебраической системой *называется тройка* $\mathcal{A} = \langle A, \mathcal{F}, \mathcal{P}\rangle$*, где* A *–* **носитель алгебраической системы**$, \mathcal{F}$ *– множество операций, заданных на множестве* A*,* $\mathcal{P}$ *– множество предикатов, заданных на множестве* A*. При этом множество* $\mathcal{F} \cup \mathcal{P}$ *называется* **сигнатурой алгебраической системы** $\mathcal{A}$*.*

Определение 2.1.13. Реляционной системой *или* **системой отношений**$,$ *или* **моделью** *называется упорядоченная пара* $\mathcal{A} = \langle A, \mathcal{P}\rangle$*, где* A *–* **носитель реляционной системы**$, \mathcal{P}$ *– множество предикатов, определенных на этой реляционной системе.*

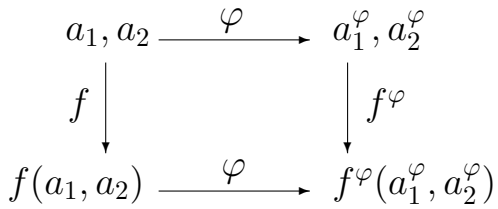

Рис. 2.1. К определению 2.1.14

2.1.3. *Гомоморфизмы*

Определение 2.1.14. *Функция* $\varphi : \begin{cases} A & \to & B \\ \mathrm{F} & \to & \mathrm{G} \end{cases}$ *называется* **гомоморфизмом** *алгебры* $\mathcal{A} = \langle A, \mathrm{F} \rangle$ *в алгебру* $\mathcal{B} = \langle B, \mathrm{G} \rangle$*, если для любой* n*-арной операции* f *из* F *и любого набора* $a_1, a_2, \ldots, a_n$ *из* A *имеем равенство*

$$(f(a_1, a_2, \ldots, a_n))^\varphi = f^\varphi(a_1^\varphi, a_2^\varphi, \ldots, a_n^\varphi)$$

(в частности, «арность» операций f *и* f^φ *совпадает).*

Для случая бинарной операции на рисунке 2.1 схематично представлено определение гомоморфизма.

Чтобы обозначения были менее громоздкими здесь обозначаем «внутренние» функции – операции, традиционно: $f(a_1, a_2, \ldots, a_n)$, а для «внешнего» отображения используем запись: a_i^φ, f^φ.

Определение 2.1.15. *Алгебры* $\mathcal{A} = \langle A, \mathcal{F} \rangle$ *и* $\mathcal{B} = \langle B, \mathcal{G} \rangle$ *называются* **однотипными,** *если можно установить взаимно однозначное соответствие из множества* $\mathcal{F}$ *на* $\mathcal{G}$*, сохраняющее «арность» операций.*

Заметим, что отображение φ не обязано быть взаимно однозначным как на множестве A так и на множестве F. Однако чаще рассматриваются гомоморфизмы, взаимно однозначные на множестве F, т. е. отображения в однотипную алгебру, «сохраняющие» все операции.

Пример. 1. Отображение $\mathcal{A} = \langle \mathbb{N}, + \rangle$ на $\mathcal{B} = \langle A/(3), +_3 \rangle$ – гомоморфизм.

2. Отображение φ из $\mathcal{A} = \langle \mathbb{N}, + \rangle$ на $\mathcal{B} = \langle \mathbb{N}_2 = \{2k | k \in \mathbb{N}\}, + \rangle$, заданное формулой $k^\varphi = 2k$ сохраняет операцию:

$$(k_1 + k_2)^\varphi = 2(k_1 + k_2) = 2k_1 + 2k_2 = k_1^\varphi + k_2^\varphi.$$

Следовательно, алгебра четных чисел с операцией сложения есть гомоморфный образ алгебры натуральных чисел с той же операцией.

Теорема 2.1.2. *Если φ – гомоморфизм алгебры $\mathcal{A} = \langle A, \mathcal{F} \rangle$ в алгебру $\mathcal{B} = \langle B, \mathcal{G} \rangle$, то подмножество $A^\varphi \subseteq B$ относительно операций из $\mathcal{F}^\varphi$ является алгеброй.*

Доказательство. В силу определения 2.1.14 подмножество $B^\varphi \subseteq B$ является замкнутым относительно любой операции из $\mathcal{F}^\varphi$:

$$\left.\begin{array}{c} \forall g \in \mathcal{F}^\varphi \subseteq \mathcal{G} \;\; \exists f \in \mathcal{F} : f^\varphi = g \\ \forall b_1, \ldots, b_n, \;\; b_i \in A^\varphi \;\; \exists a_1, \ldots, a_n, \;\; a_i \in A : a_i^\varphi = b_i \end{array}\right\} \Rightarrow$$

$$g(b_1, \ldots, b_n) = f^\varphi(a_1^\varphi, \ldots, a_n^\varphi) = (f(a_1, \ldots, a_n))^\varphi \in A^\varphi.$$

Что доказывает утверждение теоремы.

Определение 2.1.16. *Если φ – гомоморфизм алгебры $\mathcal{A} = \langle A, \mathcal{F} \rangle$ в алгебру $\mathcal{B} = \langle B, \mathcal{G} \rangle$, то алгебра $\mathcal{A}^\varphi = \langle A^\varphi, \mathcal{F}^\varphi \rangle$ называется* **гомоморфным образом** *алгебры $\mathcal{A}$ при отображении φ.*

Замечание. 1. Гомоморфный образ группоида – группоид, полугруппы – полугруппа. Гомоморфизм сохраняет ассоциативность и коммутативность бинарной операции.

2. Гомоморфный образ группы – группа. Образ нейтрального (единичного) элемента есть нейтральный в образе; образом обратного элемента является обратный.

3. Образ кольца – кольцо.

Определение 2.1.17. *Взаимно однозначный гомоморфизм алгебры $\mathcal{A}$ <u>на</u> однотипную алгебру $\mathcal{B}$ называется* **изоморфизмом.** *Обозначение: $\mathcal{A} \sim \mathcal{B}$.*

Теорема 2.1.3. *Если φ – изоморфизм алгебры $\mathcal{A} = \langle A, \mathcal{F} \rangle$ в алгебру $\mathcal{B} = \langle B, \mathcal{G} \rangle$, то φ^{-1} – изоморфизм из $\mathcal{B}$ в $\mathcal{A}$.*

Доказательство. Поскольку φ – взаимно однозначное соответствие на множествах A и $\mathcal{F}$, причем $A^\varphi = B$ и $\mathcal{F}^\varphi = \mathcal{G}$, то φ^{-1} – тоже взаимно однозначное отображение на B и $\mathcal{G}$. Проверим сохранение операций отображением φ^{-1}:

$$\left.\begin{array}{c} \forall g \in \mathcal{F}^\varphi = \mathcal{G} \;\; \exists f \in \mathcal{F} : f^\varphi = g \leftrightarrow g^{\varphi^{-1}} = f \\ \forall b_1, \ldots, b_n, \;\; b_i \in A^\varphi = B \;\; \exists a_1, \ldots, a_n, \;\; a_i \in A : a_i^\varphi = b_i \leftrightarrow b_i^{\varphi^{-1}} = a_i \end{array}\right\} \Rightarrow$$

$$(g(b_1, \ldots, b_n))^{\varphi^{-1}} = (f^\varphi(a_1^\varphi, \ldots, a_n^\varphi))^{\varphi^{-1}} = ((f(a_1, \ldots, a_n))^\varphi)^{\varphi^{-1}} =$$

$$= f(a_1, \ldots, a_n) = g^{\varphi^{-1}}(b_1^{\varphi^{-1}}, \ldots, b_n^{\varphi^{-1}}).$$

Таким образом φ^{-1} – изоморфизм из $\mathcal{B}$ в $\mathcal{A}$.

Теорема 2.1.4. *На множестве однотипных алгебр $\mathcal{M}$ изоморфизм – отношение эквивалентности.*

Доказательство. Проверим свойства эквивалентности.

1. Рефлексивность: $\forall \mathcal{A} \in \mathcal{M} \;\; \mathcal{A} \sim \mathcal{A}$, т. к. тождественное отображение $\varphi(a) = a, \;\; a \in A$, является изоморфизмом.

2. Симметричность: $\forall \mathcal{A}, \mathcal{B} \in \mathcal{M}$ если $\mathcal{A} \sim \mathcal{B}$, т. к. существует изоморфизм φ из $\mathcal{A}$ в $\mathcal{B}$, то $\mathcal{B} \sim \mathcal{A}$, т. к. φ^{-1} – изоморфизм из $\mathcal{B}$ в $\mathcal{A}$ (теорема 2.1.3).

3. Транзитивность: если $\mathcal{A} \sim \mathcal{B}$, т. к. существует изоморфизм φ из $\mathcal{A}$ в $\mathcal{B}$ и $\mathcal{B} \sim \mathcal{C}$, т. к. существует изоморфизм ψ из $\mathcal{B}$ в $\mathcal{C}$, то $\mathcal{A} \sim \mathcal{C}$, т. к. существует изоморфизм $a^{\phi} = (a^{\varphi})^{\psi}, a \in A$ из $\mathcal{A}$ в $\mathcal{C}$. Теорема доказана.

Пример. Приведем примеры изоморфных алгебр.

1. $\langle \mathbb{N}, + \rangle \sim \langle \mathbb{N}_2 = \{2k | k \in \mathbb{N}\}, + \rangle$, $k^{\varphi} = 2k, k \in \mathbb{N}$.
2. $\langle 2^M, \cap, \cup \rangle \sim \langle 2^M, \cup, \cap \rangle, \;\; X^{\varphi} = \overline{X}, \;\; X \subseteq M$.
3. $\langle \mathbb{R}_+, \cdot \rangle \sim \langle \mathbb{R}, + \rangle, \;\; x^{\varphi} = \ln x, x \in \mathbb{R}_+$.

Изоморфные алгебры с точки зрения свойств операций на равномощных носителях устроены одинаково вне зависимости от природы элементов носителей. В частности, если есть равенство формул $\Phi_1 = \Phi_2$ в алгебре $\langle A, \mathcal{F} \rangle$, то в изоморфной алгебре $\langle B, \mathcal{G} \rangle$ будет иметь место равенство формул $\Psi_1 = \Psi_2$, где формулы $\Psi_1, \;\; \Psi_2$ получены заменой операций сигнатуры $\mathcal{F}$ на соответствующие операции сигнатуры $\mathcal{G}$. Все алгебраические структуры изучаются с точностью до изоморфизма.

Определение 2.1.18. *Функция* $\varphi : \begin{cases} A & \to & B \\ \mathcal{F} & \to & \mathcal{G} \\ \mathcal{P} & \to & \mathcal{Q} \end{cases}$ *называется* **сильным гомоморфизмом** *алгебраической системы $\mathcal{A} = \langle A, \mathcal{F}, \mathcal{P} \rangle$ в алгебраическую систему $\mathcal{B} = \langle B, \mathcal{G}, \mathcal{Q} \rangle$, если*

1) φ – гомоморфизм алгебры $\langle A, \mathcal{F} \rangle$ в алгебру $\langle B, \mathcal{G} \rangle$;

2) для любого предиката $p \in \mathcal{P}$ p^{φ} совпадает с индуцированным отношением, т.е из $p^{\varphi}(b_1, b_2, \ldots, b_n)$ истинно следует, что в A найдутся такие элементы $a_1, a_2, \ldots, a_n$, что, во-первых,

$$a_1^{\varphi} = b_1, \quad a_2^{\varphi} = b_2, \quad \ldots, \quad a_n^{\varphi} = b_n,$$

и, во-вторых, $p(a_1, a_2, \ldots, a_n)$ – истинно.

Определение 2.1.19. *Алгебраические системы $\mathcal{A} = \langle A, \mathcal{F}, \mathcal{P} \rangle$ и $\mathcal{B} = \langle B, \mathcal{G}, \mathcal{Q} \rangle$ называются изоморфными, если существует взаимно однозначное соответствие из $\mathcal{A}$ на $\mathcal{B}$ которое является сильным гомоморфизмом (***изоморфизм алгебраических систем***).*

2.1.4. *Конгруэнции*

Определение 2.1.20. Конгруенцией *алгебры* $\mathcal{A} = \langle A, \mathcal{F}\rangle$ *называется отношение эквивалентности* π *на множестве* A *такое, что для любой* n*-местной операции* f *из* $\mathcal{F}$ *и любых двух наборов* $x_1, x_2, \ldots, x_n$ *и* $y_1, y_2, \ldots, y_n$ *из* A *истинна импликация*

$$\left.\begin{array}{l} x_1 \pi y_1 \\ x_2 \pi y_2 \\ \ldots \\ x_n \pi y_n \end{array}\right\} \Rightarrow\ f(x_1, x_2, \ldots, x_n)\, \pi f(y_1, y_2, \ldots, y_n). \tag{2.1}$$

Пример. Конгруэнцией на множестве целых чисел $\mathbb{Z}$ является отношение $\pi : x\pi y \Leftrightarrow 3|(x-y)$. Ранее было показано, что это отношение делимости на 3 является эквивалентностью. Проверим, что относительно операции сложения $f(x,y) = x + y$ отношение π есть конгруэнция. Действительно,

$$\left.\begin{array}{l} x_1 \pi y_1 \Leftrightarrow 3|(x_1 - y_1) \\ x_2 \pi y_2 \Leftrightarrow 3|(x_2 - y_2) \end{array}\right\} \Rightarrow\ 3 \Big| ((x_1 - y_1) + (x_2 - y_2)) \Leftrightarrow 3 \Big| ((x_1 + x_2) - (y_1 + y_2))$$

Но это и означает

$$(x_1 + x_2) = f(x_1, x_2)\, \pi f(y_1, y_2) = (y_1 + y_2).$$

Лемма 2.1.1. *Если* π *– конгруэнция на алгебре* $\mathcal{A} = \langle A, \mathcal{F}\rangle$*, то на фактормножестве* A/π *порождается однотипная* $\mathcal{A}$ *алгебра* $\mathcal{A}/\pi = \langle A/\pi, \mathcal{F}\rangle$.

Доказательство. Напомним, что в качестве элементов фактор-множества A/π выступают классы эквивалентных элементов (см. теорему 1.4.7): $A/\pi = \{a^\pi = \overline{a} = \{x \in A | x\pi a\}\}$. На этом множестве определим операции из сигнатуры $\mathcal{F}$ алгебры $\mathcal{A}$: если $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}$ – некоторые классы из множества A/π и f – n-местная операция из $\mathcal{F}$, то

$$f(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) = \overline{f(a_1, a_2, \ldots, a_n)}. \tag{2.2}$$

Введенное определение операции на множестве A/π корректно, т. к. результат не зависит от выбора представителей классов эквивалентности: если выбрать другой набор представителей $a'_1, a'_2, \ldots, a'_n$ в тех же классах, т. е.

$$\overline{a'_1} = \overline{a_1}, \overline{a'_2} = \overline{a_2}, \ldots, \overline{a'_n} = \overline{a_n},$$

то по определению конгруэнции 2.1.20 имеем

$$\left.\begin{array}{l} a_1 \pi a'_1 \\ a_2 \pi a'_2 \\ \ldots \\ a_n \pi a'_n \end{array}\right\} \Rightarrow\ f(a_1, a_2, \ldots, a_n)\, \pi f(a'_1, a'_2, \ldots, a'_n) \quad \Leftrightarrow$$

$$\overline{f\left(a_1, a_2, \ldots, a_n\right)} = \overline{f\left(a'_1, a'_2, \ldots, a'_n\right)}.$$

Таким образом на множестве A/π определены операции сигнатуры $\mathcal{F}$ и конгруэнция π порождает алгебру $\mathcal{A}/\pi = \langle A/\pi, \mathcal{F}\rangle$.

Определение 2.1.21. *Если π – конгруэнция алгебры $\mathcal{A} = \langle A, \mathcal{F}\rangle$, то алгебра $\mathcal{A}/\pi = \langle A/\pi, \mathcal{F}\rangle$ с операциями, определенными по формуле (2.2) на классах эквивалентности $\overline{a} \in A/\pi$, называется* **фактор-алгеброй**, *порожденной конгруэнцией π.*

Лемма 2.1.2. *Если π – конгруэнция на алгебре $\mathcal{A} = \langle A, \mathcal{F}\rangle$, то отображение φ из $\mathcal{A}$ на фактор-алгебру $\mathcal{A}/\pi$, ставящее в соответствие каждому элементу $a \in A$ класс эквивалентности, порожденный этим элементом: $a^\varphi = \overline{a}$, является гомоморфизмом, который называется* **естественным**.

Доказательство. По определению гомоморфизма 2.1.14 нужно проверить: для любой n-арной операции $f \in \mathcal{F}$ и любого набора $a_1, a_2, \ldots, a_n$ из A имеем равенство

$$(f(a_1, a_2, \ldots, a_n))^\varphi = f^\varphi(a_1^\varphi, a_2^\varphi, \ldots, a_n^\varphi).$$

Действительно, заметим, что $f^\varphi = f$, $a_i^\varphi = \overline{a_i}$ и π – конгруэнция (см. (2.2)), тогда

$$f^\varphi(a_1^\varphi, a_2^\varphi, \ldots, a_n^\varphi) = f(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) = \overline{f(a_1, a_2, \ldots, a_n)} = (f(a_1, a_2, \ldots, a_n))^\varphi.$$

Лемма доказана.

Заметим, что из леммы следует, что фактор-алгебра группы – группа, фактор-алгебра кольца – кольцо и т. д.

Теорема 2.1.5 (о гомоморфизмах). *Если φ – гомоморфизм из алгебры $\mathcal{A} = \langle A, \mathcal{F}\rangle$ <u>на</u> однотипную алгебру $\mathcal{B} = \langle B, \mathcal{F}\rangle$, тогда существует конгруэнция π алгебры $\mathcal{A}$, такая, что $\mathcal{B}$ изоморфна $\mathcal{A}/\pi$.*

Доказательство. Определим бинарное отношение π на множестве A следующим образом:

$$a\pi b \quad \Leftrightarrow \quad a^\varphi = b^\varphi.$$

Очевидно, что это отношение эквивалентности. Покажем, что π – конгруэнция $f \in \mathcal{F}$, $f^\varphi = f$:

$$\left.\begin{array}{l} a_1\pi b_1 \leftrightarrow a_1^\varphi = b_1^\varphi \\ a_2\pi b_2 \leftrightarrow a_2^\varphi = b_2^\varphi \\ \ldots \\ a_n\pi b_n \leftrightarrow a_n^\varphi = b_n^\varphi \\ f^\varphi\left(a_1^\varphi, a_2^\varphi, \ldots, a_n^\varphi\right) = \left(f\left(a_1, a_2, \ldots, a_n\right)\right)^\varphi \end{array}\right\} \Rightarrow \begin{array}{c} f\left(a_1^\varphi, a_2^\varphi, \ldots, a_n^\varphi\right) = f\left(b_1^\varphi, b_2^\varphi, \ldots, b_n^\varphi\right) \\ || \qquad\qquad\qquad\qquad || \\ \left(f\left(a_1, \ldots, a_n\right)\right)^\varphi = \left(f\left(b_1, \ldots, b_n\right)\right)^\varphi \\ f\left(a_1, a_2, \ldots, a_n\right) \pi f\left(b_1, b_2, \ldots, b_n\right) \end{array}$$

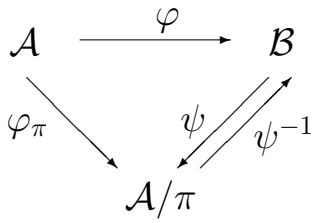

Рис. 2.2. К теореме 2.1.5

Осталось построить изоморфизм из алгебры $\mathcal{B}$ в фактор-алгебру $\mathcal{A}/\pi$. Определим отображение ψ :

$$\forall y \in B \quad \psi(y) = a^\pi = \overline{a}, \quad \text{если} \quad a^\varphi = y.$$

Напомним, что $a^\pi = \overline{a} = \{x \in A | x\pi a \ \leftrightarrow \ x^\varphi = a^\varphi\}$ – класс эквивалентных a элеменов посредством отношения π. Определение корректно, т. к. из $a_1^\varphi = a_2^\varphi = y$ следует, что $\overline{a_1} = \overline{a_2} = \psi(y)$.

Проверим по определению, что ψ – изоморфизм. Во-первых ψ – взаимно однозначное отображение на. Пусть

$$y_1, y_2 \in B : y_1 \neq y_2 \quad \psi(y_1) = \overline{a_1} \quad \psi(y_2) = \overline{a_2},$$

тогда если $\psi(y_1) = \psi(y_2)$, то $\overline{a_1} = \overline{a_2} \leftrightarrow \ y_1 = a_1^\varphi = a_2^\varphi = y_2$ – противоречие.

Доказана взаимная однозначность. Проверим, что ψ – отображение на:

$$\forall \overline{a} \in \mathcal{A}/\pi \ \exists y \in B : \ a^\varphi = y, \ \text{т. к. } \varphi \text{ – отображение на, поэтому } \psi(y) = \overline{a}.$$

Во-вторых ψ сохраняет операции:

$$f(y_1^\psi, y_2^\psi, \ldots, y_n^\psi) = f(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) = \overline{f(a_1, a_2, \ldots, a_n)} = f(a_1, a_2, \ldots, a_n)^\psi.$$

Таким образом ψ – изоморфизм. Теорема доказана.

Замечание. 1. Если φ – гомоморфизм из алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$ и φ_π – естественный гомоморфизм (см. лемму 2.1.2) из $\mathcal{A}$ на фактор-алгебру $\mathcal{A}/\pi$, где π – конгруэнция, порожденная гомоморфизмом φ, то для подходящего (см. теорему 2.1.5) изоморфизма ψ диаграмма рис. 2.2 коммутативна.

2. Собирая утверждения леммы 2.1.2 и теоремы 2.1.5, получим, что существует взаимно однозначное соответствие между множеством конгруэнций (или фактор-алгебр) на алгебре $\mathcal{A}$ и всеми ее гомоморфизмами (или гомоморфными образами). Конгруэнция, порожденная данным гомоморфизмом, называется **ядром гомоморфизма**.

Для алгебраических систем $\mathcal{A} = \langle A, \mathcal{F}, \mathcal{P} \rangle$ существует своя теорема о гомоморфизмах.

Теорема 2.1.6 (о гомоморфизмах алгебраических систем). *Если φ – сильный гомоморфизм из алгебраической системы $\mathcal{A} = \langle A, \mathcal{F}, \mathcal{P} \rangle$ на однотипную алгебраическую систему $\mathcal{B} = \langle B, \mathcal{F}, \mathcal{P} \rangle$, тогда существует конгруэнция π системы $\mathcal{A}$, такая, что $\mathcal{B}$ изоморфна $\mathcal{A}/\pi$.*

2.2. Булевы алгебры

2.2.1. *Определение и свойства*

Примерами алгебр являются уже рассмотренные нами алгебра множеств, алгебра высказываний и алгебра булевых функций. Легко заметить, что теоретико-множественные и логические операции обладают набором одинаковых свойств. Но свойства операций определяют тип алгебры, в данном случае приведены примеры булевой алгебры.

Определение 2.2.1. Булевой алгеброй *называется универсальная алгебра $\langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\} \rangle$ с носителем B, в котором выделены два элемента $\mathbf{1}$ и $\mathbf{0}$, и на котором определены двуместные операции «+» и «*» и одноместная операция «$\overline{}$», причем выполняются следующие аксиомы:*

A1.	*а)*	$x + y = y + x;$	*б)*	$x * y = y * x;$
A2.	*а)*	$(x + y) + z = x + (y + z);$	*б)*	$(x * y) * z = x * (y * z);$
A3.	*а)*	$(x + y) * z = x * z + y * z;$	*б)*	$(x * y) + z = (x + z) * (y + z);$
A4.	*а)*	$x + x = x;$	*б)*	$x * x = x;$
A5	*свойство совместимости:* $x + y = x \Leftrightarrow x * y = y;$			
A6.	*а)*	$x + \mathbf{1} = \mathbf{1};$	*б)*	$x * \mathbf{1} = x;$
A7.	*а)*	$x + \mathbf{0} = x;$	*б)*	$x * \mathbf{0} = \mathbf{0};$
A8.	*а)*	$x + \overline{x} = \mathbf{1};$	*б)*	$x * \overline{x} = \mathbf{0}.$

Пример. Алгебра

$$\langle \{\emptyset, \{0\}, \{1\}, \{0,1\}\}, \{\{0,1\}, \emptyset\}, \{\cup, \cap, \overline{}\} \rangle$$

является булевой алгеброй. Для доказательства достаточно проверить аксиомы A1-A8, полагая, что

$$\emptyset = \mathbf{0}, \{0,1\} = \mathbf{1}, \cup = +, \cap = *, \overline{} \text{ – дополнение множеств.}$$

В следующей теореме формулируются свойства операций, которые являются следствиями определения.

Теорема 2.2.1 (свойства булевых операций). *В любой булевой алгебре* $\langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\}\rangle$ *верны утверждения:*

1) $y = \overline{x} \Leftrightarrow \begin{cases} y + x = \mathbf{1}, \\ y * x = \mathbf{0} \end{cases}$, *в частности,* $\overline{\mathbf{0}} = \mathbf{1}$ *и* $\overline{\mathbf{1}} = \mathbf{0}$;

2) $\overline{\overline{x}} = x$;

3) $\overline{x} = \overline{y} \Leftrightarrow x = y$;

4) законы поглощения: $x * (x + y) = x$, $x * (x + y) = x$;

5) $x + y = x + \overline{x} * y$;

6) законы де-Моргана: $\overline{x + y} = \overline{x} * \overline{y}$, $\overline{x * y} = \overline{x} + \overline{y}$;

7) $x * y = \mathbf{0} \Leftrightarrow x + \overline{y} = \overline{y}$;

8) $x * y = x \Leftrightarrow x * \overline{y} = \mathbf{0}$.

Доказательство. Приведем доказательство свойств 1), 2) и законов де-Моргана.

Свойство 1). Пусть $x + y = \mathbf{1}$ и $x * y = \mathbf{0}$. Тогда, используя (см. определение 2.2.1) аксиомы A1-A8, имеем

$$\overline{x} = \overline{x} + \mathbf{0} = \overline{x} + x * y = \overline{x} * \mathbf{1} + x * y = \overline{x} * (x + y) + x * y = (\overline{x} * x + \overline{x} * y) + x * y =$$

$$= (\mathbf{0} + \overline{x} * y) + x * y = \overline{x} * y + x * y = (\overline{x} + x) * y = \mathbf{1} * y = y,$$

что и требовалось доказать. Обратное: если $y = \overline{x}$, то $x + y = \mathbf{1}$ и $x * y = \mathbf{0}$ очевидно следует из аксиомы A8.

Свойство 2). В свойстве 1) в качестве x возьмем $\overline{x}$, а в качестве y – элемент x. Тогда $x + y = \mathbf{1}$ и $x * y = \mathbf{0}$ по аксиоме A8. Откуда по свойству 1) заключаем $\overline{\overline{x}} = x$.

6). Законы де-Моргана.

Проверим, что элемент $\overline{x} * \overline{y}$ является «обратным» к $x + y$. Для этого, естественно, воспользуемся свойством 1). Итак, надо проверить, что

$$(x + y) + \overline{x} * \overline{y} = \mathbf{1}, \qquad (x + y) * \overline{x} * \overline{y} = \mathbf{0}.$$

Первое равенство – это следствие законов поглощения:

$$(x + y) + \overline{x} * \overline{y} = x + (y + \overline{x} * \overline{y}) = x + y + \overline{x} = y + \mathbf{1} = \mathbf{1}.$$

Второе равенство является следствием аксиом A1-A8:

$$(x + y) * \overline{x} * \overline{y} = x * \overline{x} * \overline{y} + y * \overline{x} * \overline{y} = \mathbf{0} * \overline{y} + \mathbf{0} * \overline{x} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Второй закон де-Моргана доказывается аналогично. Доказательство закончено.

2.2.2. *Двойственность и частичный порядок*

Поскольку аксиомы булевой алгебры симметричны относительно операций «$*$» и «$+$», то они останутся неизменными, если поменять обозначения операций а также взять в качестве «нового нуля» «старую единицу» и наоборот.

Определение 2.2.2. *Если* $\mathcal{B} = \langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\}\rangle$ *– булева алгебра, то алгебраическая система* $\mathcal{B}' = \langle B, \{\mathbf{0}, \mathbf{1}, *, +, \overline{}\}\rangle$ *называется алгеброй,* **двойственной** *к булевой алгебре* $\mathcal{B}$.

Пример. Алгебра

$$\mathcal{B} = \langle \{\emptyset, \{0\}, \{1\}, \{0,1\}\}, \{\{0,1\}, \emptyset\}, \{\cup, \cap, {}^-\}\rangle$$

является булевой алгеброй, в которой

$$\emptyset = \mathbf{0}, \{0,1\} = \mathbf{1}, \cup = +, \cap = *, {}^- \text{ – дополнение множеств.}$$

Алгебра

$$\mathcal{B}' = \langle \{\emptyset, \{0\}, \{1\}, \{0,1\}\}, \{\emptyset, \{0,1\}\}, \{\cap, \cup, {}^-\}\rangle$$

в которой

$$\{0,1\} = \mathbf{0}, \emptyset = \mathbf{1}, \cap = +, \cup = *, {}^- \text{ – дополнение множеств}$$

является двойственной булевой алгеброй к $\mathcal{B}$.

Теорема 2.2.2. *Если булева алгебра* $\mathcal{B} = \langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\}\rangle$ *двойственна алгебре* $\mathcal{B}' = \langle B, \{\mathbf{0}, \mathbf{1}, *, +, \overline{}\}\rangle$, *то отображение* φ, *заданное правилом*

$$\forall b \in B\ \varphi(b) = \overline{b};\quad \varphi(+) = *;\quad \varphi(*) = +;\quad \varphi(\mathbf{1}) = \mathbf{0};\quad \varphi(\mathbf{0}) = \mathbf{1};\quad \varphi(\overline{}) = \overline{},$$

является изоморфизмом.

Доказательство. Очевидно, что отображение φ является взаимно однозначным. Покажем, что оно сохраняет операции:
1) $\varphi(\overline{b}) = \overline{\overline{b}} = b = \overline{\varphi(b)}$;
2) $\varphi(b_1 + b_2) = \overline{b_1 + b_2} = \overline{b_1} * \overline{b_2} = \varphi(b_1)\varphi(+)\varphi(b_2)$;
3) $\varphi(b_1 * b_2) = \overline{b_1 * b_2} = \overline{b_1} + \overline{b_2} = \varphi(b_1)\varphi(*)\varphi(b_2)$.
В приведенных равенствах использовалось свойство инволютивности и законы де Моргана. Таким образом, φ – взаимно однозначный гомоморфизм, что и требовалось доказать.

Замечание. Каждой формуле Ψ в булевой алгебре $\mathcal{B}$ можно сопоставить двойственную $\varphi(\Psi)$, полученную по правилу, указанному в теореме. В частности, в алгебре булевых функций получаем двойственные формулы, задающие двойственные функции (см. теорему 1.3.4).

Рассмотрим отношение «$\leq$», введенное на булевой алгебре правилом:

$$x \leq y \;\Leftrightarrow\; x * y = x.$$

В силу аксиомы А5

$$x \leq y \;\Leftrightarrow\; x * y = x \Leftrightarrow\; x + y = y.$$

Проверим свойства этого бинарного отношения.
Рефлексивность :

$$x * x = x \;\Rightarrow\; x \leq x.$$

Антисимметричность:

$$\left\{ \begin{array}{l} x \leq y, \\ y \leq x \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x * y = x, \\ y * x = y \end{array} \right. \Rightarrow\; x = x * y = y * x = y.$$

Транзитивность:

$$\left\{ \begin{array}{l} x \leq y, \\ y \leq z \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x * y = x, \\ y * z = y \end{array} \right. \Rightarrow\; x * z = (x * y) * z = x * y = x \;\Rightarrow\; x \leq z.$$

Таким образом, доказана следующая теорема.

Теорема 2.2.3 (о частичном порядке на булевой алгебре). *Отношение «$\leq$», определенное на носителе булевой алгебры правилом $x \leq y \;\Leftrightarrow\; x * y = x$, является частичным порядком.*

Пример. В булевой алгебре $\mathcal{A}$ подмножеств множества M :

$$\mathcal{A} = \langle A; \{M, \emptyset\}; \{\cup, \cap, \bar{}\} \rangle \text{, где } A = 2^M = \{X \mid X \subseteq M\}$$

индуцированный порядок совпадает с отношением $\subseteq$. Действительно,

$$X \leq Y \;\Leftrightarrow X * Y = X \;\Leftrightarrow\; X \cap Y = Y \;\Leftrightarrow\; X \subseteq Y.$$

2.2.3. *Строение конечных булевых алгебр*

Определение 2.2.3. *Отличный от* $\mathbf{0}$ *элемент x булевой алгебры $\langle B, \{\mathbf{1}, \mathbf{0}, +, *, \bar{}\}\rangle$ называется* **атомом**, *если для любого элемента y из B, отличного от* $\mathbf{0}$, *справедлива альтернатива: либо $x * y = x$, либо $x * y = \mathbf{0}$.*

Пример. В булевой алгебре $\mathcal{A}$ подмножеств множества M :

$$\mathcal{A} = \langle A; \{M, \emptyset\}; \{\cup, \cap, \bar{}\} \rangle \text{, где } A = 2^M = \{X \mid X \subseteq M\}$$

атомами являются одноэлементные подмножества.

Теорема 2.2.4 (о свойствах атомов). *Для любых различных атомов x и y справедливо*
1) $x * y = \mathbf{0}$;
2) $x + \overline{y} = \overline{y}$;
3) x атом тогда и только тогда, когда x —минимальный (среди ненулевых) элемент относительно частичного порядка $\leq$, где $x \leq y \Leftrightarrow x * y = y$.

Доказательство.
1. По определению $x * y \in \{\mathbf{0}, x\} \cap \{\mathbf{0}, y\} = \{\mathbf{0}\}$, поэтому $x * y = \mathbf{0}$.
2. По закону де-Моргана $\overline{x + \overline{y}} = \overline{\overline{y}} \Leftrightarrow \overline{x} * y = y$, поэтому достаточно доказать равенство $\overline{x} * y = y$. Так как y – атом, то достаточно доказать, что $\overline{x} * y \neq \mathbf{0}$. От противного: пусть $\overline{x} * y = \mathbf{0}$. По свойству 1) получаем, что $x * y = \mathbf{0}$. Следовательно, с одной стороны, $\overline{x} * y + x * y = \mathbf{0} + \mathbf{0} = \mathbf{0}$. С другой стороны, по аксиомам булевой алгебры, $\overline{x} * y + x * y = (\overline{x} + x) * y = \mathbf{1} * y = y$. Значит, $y = \mathbf{0}$, что противоречит определению атома.
3. Очевидное следствие определения атома. Теорема доказана.

Теорема 2.2.5 (об атомах конечной булевой алгебры). *Если булева алгебра $\langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\}\rangle$ имеет конечное число элементов в носителе B, и $\mathbf{Б} = \{a, b, \ldots, c\}$ – множество всех ее атомов, то $\mathbf{1} = a + b + \ldots + c$.*

Доказательство. Пусть $h = a + b + \ldots + c$. По закону де-Моргана $\overline{h} = \overline{a} * \overline{b} * \ldots * \overline{c}$. Достаточно доказать, что $\overline{h} = \mathbf{0}$.

От противного: пусть $\overline{h} \neq \mathbf{0}$. Среди всех элементов, не превосходящих $\overline{h}$, выберем произвольный минимальный элемент $x \neq \mathbf{0}$ (он существует в силу конечности B).

Пусть найдется такой ненулевой элемент $y \neq x$, что $y \leq x$. Имеем $y \leq x \leq \overline{h}$, откуда в силу транзитивности отношения частичного порядка, $y \leq \overline{h}$, что противоречит минимальности x. Значит, такого элемента y не найдется, то есть x– минимальный относительно $\leq$ элемент.

Мы доказали, что если $\overline{h} \neq \mathbf{0}$,то элемент x, являющийся минимальным среди всех элементов, не превосходящих $\overline{h}$, является минимальным ненулевым элементом. Тогда по критерию атома (пункт 3) теоремы 2.2.4), x – атом: $x \in \mathbf{Б}$ $x \leq \overline{h}$. С другой стороны, имеем

$$\forall x \in \mathbf{Б}\ x * \overline{h} = \mathbf{0} \Leftrightarrow x \not\leq \overline{h}.$$

Получено противоречие. Теорема доказана.

Без доказательства сформулируем следующее следствие.

Следствие. *Пусть булева алгебра* $\langle B, \{\mathbf{1}, \mathbf{0}, +, *, \overline{}\}\rangle$ *имеет конечный носитель* B. *Тогда любой ненулевой элемент* a *может быть представлен в виде* $a = x_1 + x_2 + \ldots + x_k$, *где* $\{x_1,\ x_2,\ \ldots,\ x_k\}$ – *множество всех атомов, сравнимых с* a (*т. е.* $x_i * a = a,\ 1 \le i \le k$).

Теорема 2.2.6 (о классификации конечных булевых алгебр). *Всякая конечная булева алгебра* $\mathcal{B}$ *изоморфна алгебре подмножеств множества ее атомов. В частности,* $|\mathcal{B}| = 2^n$, *где* n – *количество атомов алгебры* $\mathcal{B}$.

Доказательство. Построим изоморфизм φ из $\mathcal{B}$ в алгебру подмножеств, состоящих из атомов. Положим $\varphi(\mathbf{1})$ равным множеству всех атомов исходной булевой алгебры:
$\varphi(\mathbf{1}) = \{x_1,\ x_2,\ \ldots,\ x_n\}$, а также
$\varphi(\mathbf{0}) = \emptyset,\quad \varphi(+) = \cup, \varphi(*) = \cap,\quad \varphi(\overline{}) = \overline{}$ (в последнем случае под $\overline{}$ понимается дополнение).

Согласно следствию из теоремы 2.2.6, всякий элемент x алгебры $\mathcal{B}$ является суммой некоторых ее атомов: $x = a + b + \ldots + c$. Положим

$$\varphi(x) = \varphi(a + b + \ldots + c) = \{a, b, \ldots, c\}.$$

Нетрудно проверить, что φ – требуемый изоморфизм. Теорема доказана.

2.3. Группы

2.3.1. *Определение и примеры*

Универсальная алгебра с одной бинарной операцией и одной 0-арной операцией (выделение нейтрального элемента), которые удовлетворяют групповым аксиомам (ассоциативности, существования нейтрального элемента, существования обратного элемента) из определения 2.1.8, называется группой. В теории групп обычно используют мультипликативную запись и групповую операцию обозначают «$\cdot$», а обратный элемент $\tilde{g} = g^{-1}$. Нейтральный элемент, играющий роль единицы, будем обозначать e. В следующей лемме отметим некоторые следствия определения группы.

Теорема 2.3.1 (о свойствах обращения в группе). *Пусть алгебра* $\langle G,\ \cdot, e\ \rangle$ *является группой. Тогда*

1) если $\exists g \in G:\ g \cdot x = g$ (*или* $x \cdot g = g$),*то*
$\forall g \in G\ \ g \cdot x = x \cdot g = g$, *т. е.* $x = e$ (*признак единичного элемента);*

2) если $x \cdot g = e$ (*или* $g \cdot x = e$),*то*
$x = g^{-1}$(*однозначность обратного элемента);*

3) $\forall g \in G\ (g^{-1})^{-1} = g$ *(инволютивность обращения);*
4) $\forall g, h \in G\ (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ *(обращение произведения).*

Доказательство. Заметим для начала, что в силу однозначности некоторой бинарной операции $f(x, y)$ (как функции), равенство элементов $y_1 = y_2$ эквивалентно $f(x, y_1) = f(x, y_2)$. Для мультипликативной группы это записывается так:

$$\forall x \in G\ \ (y_1 = y_2\ \Leftrightarrow\ x \cdot y_1 = x \cdot y_2),$$

что выглядит как «домножение» первого равенства на x слева. То же можно сказать и о «домножении» справа. В дальнейшем будем использовать эту терминологию.

1. Пусть $g \cdot x = g$. Домножим слева это равенство на g^{-1} :

$$\left.\begin{array}{l} g^{-1} \cdot (g \cdot x) = g^{-1} \cdot g = e \\ g^{-1} \cdot g = e \text{ (аксиома существования обратного элемента)} \\ g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = e \cdot x = x \text{ (аксиома ассоциативности)} \end{array}\right\} \Rightarrow\ x = e.$$

2. Пусть $x \cdot g = e$. Домножим справа это равенство на g^{-1} и используем аксиомы группы:

$$\left.\begin{array}{l} (x \cdot g) \cdot g^{-1} = x \cdot (g \cdot g^{-1}) = x \cdot e = x \\ \quad || \\ e \cdot g^{-1} = g^{-1} \end{array}\right\} \Rightarrow\ x = g^{-1}.$$

3. Имеем аксиому существования обратного элемента: $g \cdot g^{-1} = e$ и единственность обратного, в силу доказанного пункта 2). Тогда g – единственный обратный к g^{-1}, т. е. $(g^{-1})^{-1} = g$.

4. Проверим, что $g \cdot h$ и $h^{-1} \cdot g^{-1}$ – взаимно обратные элемены:

$$(g \cdot h) \cdot (h^{-1} \cdot g^{-1}) = g \cdot ((h \cdot h^{-1}) \cdot g^{-1}) = g \cdot (e \cdot g^{-1}) = g \cdot g^{-1} = e.$$

Теорема доказана.

Следствие. 1. Доказанные свойства групповой операции позволяют применять в мультипликативной группе свойства возведения в степень :

если $\underbrace{g \cdot \ldots \cdot g}_{n \text{ раз}} = g^n$, то $\forall g \in G,\ \forall n, m \in \mathbb{N}\ (g^n)^m = g^{nm},\ (g^{-1})^n = (g^n)^{-1} = g^{-n}$.

2. Группу можно рассматривать как алгебру с тремя операциями: бинарная групповая операция, 0-арная операция выделения единичного элемента и унарная операция обращения. В силу доказанной единственности обратного элемента обращение является функцией одной переменной, т. е. унарной операцией.

Заметим, что при мультипликативной записи обозначение операции «$\cdot$» обычно опускают: $g \cdot h = gh$.

Пример. Рассмотрим все взаимно однозначные функции $g(x)$ (подстановки) из множества X на X. Относительно операции суперпозиции функций «$\circ$»: $(g \circ h)(x) = g(h(x))$ множество функций будет группой. В качестве единичного элемента «e» здесь выступает тождественное преобразование: $\forall x \in X \;\; e(x) = x$, а в качестве обратного – обратная функция: $g^{-1}(x) = y \leftrightarrow \;\; g(y) = x$. Такая группа называется *группой подстановок (или симметрической группой)* и обозначается Σ_X.

Определение 2.3.1. *Алгебра* $\mathcal{A}$ **изоморфно вкладывается** *в однотипную алгебру* $\mathcal{B}$*, если* $\mathcal{A}$ *изоморфна некоторой подалгебре* $\mathcal{B}'$ *алгебры* $\mathcal{B}$*.*

Теорема 2.3.2 (Кэли). *Всякая группа* G *изоморфно вкладывается в симметрическую группу* Σ_G*.*

Доказательство. Определим функцию $\varphi : G \to \Sigma_G$ правилом: каждому элементу $g \in G$ сопоставим правый сдвиг $\sigma_g \in \Sigma_G$. При этом $\sigma_g(x) = xg$ и есть подстановка на множестве G. Действительно, если $x \neq y$, то $xg \neq yg$ и σ_g взаимно однозначная функция. Кроме того для любого $y \in G$ найдется $x = (yg)^{-1}$ такой, что $\sigma_g(x) = \sigma_g((yg)^{-1}) = (yg)^{-1}g = y$. Т. е. σ_g функция из G на G.

Далее, φ – взаимно однозначный гомоморфизм:

$$x, y \in G : \;\; x \neq y \Rightarrow \;\; \sigma_x \neq \sigma_y; \quad \varphi(xy) = \sigma_{xy} = \sigma_x \circ \sigma_y = \varphi(x) \circ \varphi(y).$$

Гомоморфный образ G^φ изоморфен G и является подалгеброй, а конкретно – подгруппой в Σ_G. Теорема доказана.

2.3.2. *Подгруппы*

Определение 2.3.2. *Подмножество* H *группы* $\langle G, \cdot \rangle$ *называется* **подгруппой** *группы* G *тогда и только тогда, когда* $\langle H, \cdot \rangle$ *также является группой.*

Тот факт, что H – подгруппа группы G, обозначается как $H \leq G$.

Заметим, что подгруппа является подалгеброй (см. определение 2.1.3), т. е. замкнутось подгруппы относительно групповой операции необходима, но не достаточна. Например в группе $\langle \mathbb{Z}, + \rangle$ $\langle \mathbb{N}, + \rangle$ – продалгебра, но не подгруппа. Если же рассмотреть расширенную сигнатуру группы, состоящую из групповой операции, обращения и выделения нейтрального элемента, то в группе $\langle \mathbb{Z}, +, (-1)\cdot, 0 \rangle$ $\langle \mathbb{N}, + \rangle$ – не подалгебра. Сформулируем признак подгруппы.

Теорема 2.3.3 (критерий подгруппы). *Непустое подмножество H группы $\langle G, \cdot \rangle$ является подгруппой тогда и только тогда, когда*

$$\begin{cases} x \in H, \\ y \in H \end{cases} \Rightarrow \begin{cases} x \cdot y \in H, \\ x^{-1} \in H \end{cases}$$

Доказательство. Необходимость очевидна.

Достаточность. Если $x \cdot y$ принадлежит H для любых x, y из H, то это означает, что на H определена операция «$\cdot$». Проверим выполнение свойств групповой операции.

Ассоциативность выполняется во всем G, а тем более в H.

Аксиома существования обратного элемента выполняется если $e \in H$ и $\forall h \in H \ \exists h^{-1} \in H$. Действительно, в H содержится хотя бы один элемент h, тогда, по условию теоремы, $h^{-1} \in H$. Следовательно, поскольку произведение элементов из H снова в H, то $h \cdot h^{-1} = e \in H$. Теорема доказана.

Определение 2.3.3. *Для подгруппы H из $\langle G, \cdot \rangle$ и элемента g из G множество $gH = \left\{ gh \,\middle|\, h \in H \right\}$, называется* **левым смежным классом** *группы G по подгруппе H. Количество левых смежных классов группы G по подгруппе H называется* **индексом подгруппы** *H в группе G, и обозначается $|G : H|$.*

Лемма 2.3.1 (критерий совпадения левых смежных классов). *Для подгруппы $H \leq G$ равенство $xH = yH$ выполняется тогда и только тогда, когда элемент $x^{-1}y$ (или $y^{-1}x$) содержится в H.*

Доказательство. Необходимость. Пусть $xH = yH$. Тогда

$$\exists h \in H : \quad x = yh \ \Rightarrow \ y^{-1}x \in H.$$

Одновременно можно получить, что $x^{-1}y \in H$, т. к.

$$xH = yH \ \Rightarrow \ \exists h_1 \in H : \quad y = xh_1 \ \Rightarrow \ x^{-1}y \in H.$$

Достаточность. Пусть $x^{-1}y = h \in H$. Тогда $y = xh$ и $x = yh^{-1}$. Докажем равенство множеств $xH = yH$:

$$\text{пусть } g \in xH \ \Rightarrow \ g = xh_1 = y(h^{-1}h_1) \in yH \ \Rightarrow \ xH \subseteq yH.$$

Обратное включение $xH \subseteq yH$ доказывается также. Значит $xH = yH$.

Лемма доказана.

Замечание. Можно определить правые смежные классы по подгруппе: $Hg = \left\{ hg \,\middle|\, h \in H \right\}$ и сформулировать аналогичную лемму.

Определение 2.3.4. *Группа называется* **конечной**, *если она состоит из конечного числа элементов.* **Порядком конечной группы**, *обозначаемым* $|G|$, *называется количество элементов этой группы.*

Теорема 2.3.4 (Лагранжа). *Для всякой подгруппы H конечной группы G справедливо равенство* $|G| = |H| \cdot |G : H|$.

Доказательство. Достаточно доказать, что различные левые смежные классы группы G по H не пересекаются, равномощны и всякий элемент группы G содержится в некотором смежном классе.

Рассмотрим различные левые смежные классы: $xH \neq yH$. Предположим, что их пересечение не пусто и $z \in xH \cap yH$. Тогда $\exists h_1, h_2 \in H$:

$$z = xh_1 = yh_2 \Rightarrow \left\{ \begin{array}{l} zx^{-1} \in H, \\ zy^{-1} \in H \end{array} \right. \underbrace{\Rightarrow}_{\text{лемма 2.3.1}} \left\{ \begin{array}{l} zH = xH, \\ zH = yH \end{array} \right. \Rightarrow xH = yH,$$

что противоречит предположению $xH \neq yH$.

Покажем, что $|xH| = |yH|$ для любых $x, y \in G$. Установим соответствие между множествами xH и yH: $xh \to yh,\ h \in H$. Оно является взаимно однозначным, т. к.

$$xh_1 \neq xh_2 \Rightarrow h_1 \neq h_2 \Rightarrow yh_1 \neq yh_2.$$

Но верны и обратные импликации. Следовательно $|xH| = |yH| = |H|$.

Рассмотрим теперь произвольный элемент $g \in G$. Но тогда $e \in H$ поэтому $g \in gH$, т. е. $G = \bigcup_{g \in G} gH$ Итак,

$$\left. \begin{array}{l} xH \neq yH \to xH \cap yH = \emptyset \\ |xH| = |yH| = |H| \\ G = \bigcup_{g \in G} gH \end{array} \right\} \Rightarrow |G| = |H| \cdot |G : H|$$

Теорема доказана.

Следствие. 1. Порядок любой подгруппы конечной группы делит нацело порядок самой группы.

2. Число левых и правых смежных классов по одной и той же подгруппе совпадает.

2.3.3. *Циклические группы*

Группа G называется циклической в смысле определения 2.1.5, если она, как алгебра, порождается одним элементом в сигнатере из трех операций: бинарная групповая операция, 0-арная операция выделения нейтрального элемента и унарная операция обращения. Сформулируем это определение подробнее.

Определение 2.3.5. *Группа G называется* **циклической**, *если для некоторого элемента g из G имеем*

$$G = \left\{ g^n,\ \left(g^{-1}\right)^n, e \,\middle|\, n \in \mathbb{N} \right\}.$$

Пример. 1. $\langle \mathbb{Z}, + \rangle =< 1 >= \{ n \cdot 1, n \cdot (-1) = (-n) \cdot 1, 0 \,; n \in \mathbb{N} \}$ – бесконечная циклическая группа в аддитивной записи.

2. $\langle \mathbb{Z}/(n), + \rangle =< \overline{1} >= \left\{ k \cdot \overline{1},\ k \cdot \overline{-1},\ \overline{0} \,; k \in \mathbb{N} \right\} = \left\{ k \cdot \overline{1};\ k = 0, 1, \ldots, n-1 \right\}$ – конечная циклическая группа порядка n в аддитивной записи.

3. $\langle \mathbb{C}_n, \cdot \rangle =< \omega_1 >= \left\{ \omega_1^k,\ (\omega_1^{-1})^k,\ 1 \,; k \in \mathbb{N} \right\} =$

$= \left\{ \omega_1^k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n};\ k = 0, 1, \ldots, n-1 \right\}$ – конечная циклическая группа комплексных корней из единицы порядка n в мультипликативной записи. Заметим, что $\mathbb{Z}/(n) \sim \mathbb{C}_n$ – изоморфные группы.

Лемма 2.3.2. *Всякая бесконечная циклическая группа изоморфна $\langle \mathbb{Z}, + \rangle$.*

Доказательство. Пусть G – бесконечная циклическая группа, тогда по определению 2.3.5

$$G =< g >= \left\{ g^n,\ \left(g^{-1}\right)^n = g^{-n}, e = g^0 \,\middle|\, n \in \mathbb{N} \right\}.$$

Определим функцию $\varphi : G \to \mathbb{Z}$ правилом: $\varphi(g^n) = n,\ n \in \mathbb{Z}$. Это отображение является взаимно однозначным отображением на множество $\mathbb{Z}$. Его гомоморфность доказывает формула:

$$\varphi(g^n \cdot g^k) = \varphi(g^{n+k}) = n + k = \varphi(g^n) + \varphi(g^k).$$

Следовательно φ – изоморфизм и лемма доказана.

Из леммы следует, что других (с точностью до изоморфизма) бесконечных циклических групп кроме $\langle \mathbb{Z}, + \rangle$ нет. Но и всякая подгруппа $\langle \mathbb{Z}, + \rangle$ – бесконечная циклическая, что докажем в следующей лемме.

Лемма 2.3.3. *Всякая подгруппа циклической группы (конечной или бесконечной) является циклической.*

Доказательство. Пусть $H \leq\!< g >$. В доказательстве используем мультипликативную запись. Выберем наименьшее натуральное число n такое, что $g^n \in H$. Тогда для любого $h \in H$ найдется $k \in \mathbb{Z}$ такого, что $h = g^k \in H$. Используя алгоритм деления с остатком, получим $k = nm + r,\ 0 \leq r \leq n-1$. Тогда

$$\left.\begin{array}{l} g^k \in H \\ g^n \in H \\ g^r = g^{k-nm} = g^k (g^n)^{-m} \ \Rightarrow\ g^r \in H,\ r < n \end{array}\right\} \Rightarrow \begin{array}{l} r = 0 \text{ по выбору } n, \\ k = nm, g^k = (g^n)^m. \end{array}$$

Таким образом, $H =< g^n >$ – циклическая.

Следствие. Все подгруппы бесконечной циклической группы – бесконечные циклические.

В доказательстве леммы 2.3.3 показано, что всякая подгруппа H группы $< g >$ порождается степенью элемента g: $H =< g^n >$. В группе $\langle \mathbb{Z}, + \rangle$, изоморфной любой бесконечной циклической по лемме 2.3.2, это записывается так: $< n >= \{n, 2n, 3n, \dots, \}$, т. к. $g = 1$. Но $< n >$ – бесконечная циклическая группа. Следствие доказано.

В леммах 2.3.2 и 2.3.3 описаны (с точностью до изоморфизма) все бесконечные циклические группы и их подгруппы. Заметим, что фактор-группы циклической группы – циклические, но могут быть конечными ($\langle \mathbb{Z}/(n), + \rangle$).

Определение 2.3.6. *Говорят, что* g – **элемент конечного порядка** *в группе* $\langle G, \cdot \rangle$, *если существует такое число* n, *для которого* $g^n = e$. *В противном случае* g – **элемент бесконечного порядка**. *Если* g – *элемент конечного порядка, то наименьшее такое натуральное число* n, *что* $g^n = e$, *называется* **порядком элемента**, *и обозначается* $|g|$. *В этом случае говорят, что* g – **элемент порядка** n.

Лемма 2.3.4 (о порядке элемента группы). *Порядок любого элемента конечной группы* G *равен порядку циклической группы, порожденной этим элементом и делит нацело порядок самой группы.*

Доказательство. Пусть $g \in G$. Рассмотрим все степени g^k, $k \in \mathbb{N}$. Поскольку число элеменов в G – конечно, то для некоторых натуральных чисел k_1 и k_2 имеем $g^{k_1} = g^{k_2}$. Но тогда $g^{k_1} g^{-k_2} = g^{k_1 - k_2} = e$. Рассмотрим наименьшее натуральное n такое, что $g^n = e$, тогда $< g >= \{g, g^2, g^3, \dots, g^{n-1}, g^n = e\}$. Получили $| < g > | = |g|$, по теореме Лагранжа 2.3.4 порядок подгруппы $| < g > | = |g|$ делит порядок группы G, что и требовалось доказать.

Лемма 2.3.5. *В любой конечной циклической группе* $G =< g >$ *порядка* n *верны утверждения:*

1) $|g| = n$;

2) если $g^k = e$, *то* k *делится на* $|g|$;

3) если $|g| = lm$, *то* $|g^l| = m$;

4) порождающими элементами группы G *являются те и только те степени* g^k *для которых* k *взаимно просто с* n.

Лемма 2.3.6. *Любая конечная циклическая группа* $G =< g >$ *порядка* n *изоморфна* $\langle \mathbb{Z}/(n), + \rangle$ – *аддитивной группе вычетов по модулю* n.

2.4. Поля

2.4.1. *Определение и примеры*

Напомним определение 2.1.8 (см. стр. 52): универсальная алгебра $\langle G, \{*, e\}\rangle$ называется **группой**, если двуместная операция «$*$» и элемент e из G удовлетворяют следующим трем условиям (аксиомам группы):
1) $(x * y) * z = x * (y * z)$ (ассоциативность);
2) $\forall g \in G \;\; g * e = e * g = g$ (существование нейтрального элемента);
3) $\forall g \in G \; \exists \tilde{g} : \;\; g * \tilde{g} = e$ (существование обратного элемента).

Коммутативные группы называются абелевыми.

Сформулируем также определение поля 2.1.11 (см. стр. 54): универсальная алгебра $\langle F, \{\cdot, +, 0, 1\}\rangle$ называется **полем**, если выполнены условия:
1) $\langle F, \{+, 0\}\rangle$ – абелева аддитивная группа поля;
2) $\langle F \setminus \{0\}, \{\cdot, 1\}\rangle$ – абелева мультипликативная группа поля;
3) $\forall x, y, z \in F \quad x \cdot (y + z) = x \cdot y + x \cdot z$ (дистрибутивность).

Пример. 1. Алгебра $\langle \mathbb{Q}, \{+, \cdot, 0, 1\}\rangle$ является полем рациональных чисел.

2. Алгебра $\langle \mathbb{R}, \{+, \cdot, 0, 1\}\rangle$ является полем действительных чисел.

3. Алгебра $\langle \mathbb{C}, \{+, \cdot, 0, 1\}\rangle$ является полем комплексных чисел.

4. Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0 + 0 = 0, \quad 0 + 1 = 1 = 1 + 0$. Чему равно $1 + 1$?

Так как относительно сложения поле есть группа, то у 1 должен быть обратный элемент: $1 + (-1) = 0$. Но (-1) – это элемент поля, т. е. это либо 0, либо 1. Значит, $(-1) = 1$, т. е. $1 + 1 = 0$.

Разберемся с умножением. Ясно, что $1 \cdot 1 = 1$, так как 1 – нейтральный элемент e группы.

Чему равно $1 \cdot 0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только свойство дистрибутивности:
$x \cdot (y + z) = x \cdot y + x \cdot z$. Тогда

$$1 = 1 \cdot 1 = 1 \cdot (1 + 0) = 1 \cdot 1 + 1 \cdot 0 \;\Rightarrow\; 1 = 1 + 1 \cdot 0.$$

По критерию нейтрального элемента (пункт 1) теоремы 2.3.1) $1 \cdot 0 = 0$.

Чему равно $0 \cdot 0$?

$0 \cdot 0 = 0 \cdot (1 + 1) = 0 \cdot 1 + 0 \cdot 1 = 0 + 0 = 0$. Значит, $0 \cdot 0 = 0$.

Полем является алгебра $GF(2) = \langle \{0; 1\}, \; \{+, \cdot, 0, 1\}\rangle$, где бинарные опера-

ции «+»,«·» заданы следующими таблицами Кэли:

$x+y$		
$y\backslash x$	0	1
0	0	1
1	1	0

,

$x\cdot y$		
$y\backslash x$	0	1
0	0	0
1	0	1

.

Это поле имеет наименьшее число элементов в носителе.

Простые следствия из аксиом поля сформулируем в следующей теореме.

Теорема 2.4.1. *Если F – поле, тогда*

1) $\forall x \in F \quad x \cdot 0 = 0$;

2) $\forall x, y \in F \quad x \cdot y = 0 \;\Leftrightarrow\; x = 0$ *или* $y = 0$.

Доказательство. 1. Пусть $x \in F$, тогда, используя дистрибутивность и свойства нейтральных элементов 1 и 0, имеем

$$x = x \cdot 1 = x \cdot (1+0) = x \cdot 1 + x \cdot 0 = x + x \cdot 0 \;\Rightarrow\; x \cdot 0 = 0 \quad \text{(теорема 2.3.1 1))}.$$

2. Докажем необходимость от противного. Если бы $x \neq 0 \neq y$, то элемент $x \cdot y$ принадлежал бы мультипликативной группе поля, носитель которой не содержит нуля, противоречие. Достаточность следует из доказанного пункта 1). Теорема доказана.

Замечание. Утверждение 2) теоремы называют *отсутствием делителей нуля* в поле.

Если n – натуральное число и x – элемент поля F, то через nx будем обозначать сумму n штук элементов x:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

nx – это не умножение, а кратное сложение, точнее аддитивная степень элемента x с показателем n.

Определение 2.4.1. *Если существует такое натуральное число n, что $n1 = 0$, то наименьшее такое число n называется* **характеристикой поля** *F. Если, такое n не существует, т. е. для любого n в F найдется такой x, что $nx \neq 0$, то характеристику поля считают равной 0. Характеристика поля F обозначается через* $\mathrm{char}F$.

Теорема 2.4.2 (о характеристике поля). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n – ненулевая характеристика поля F и $n = p \cdot q$, где $n > p > 1, n > q > 1$. Рассмотрим произведение *ненулевых* (по определению характеристики как *минимального* натурального n со свойством $n1 = 0$) элементов поля $(p1) \cdot (q1)$. Тогда $(p1) \cdot (q1) = (pq)1 = n1 = 0$, что противоречит отсутствию делителей нуля в любом поле (теорема 2.4.1). Теорема доказана.

Теорема 2.4.3 (критерий характеристики поля).

1. Если F – поле ненулевой характеристики p, тогда $\forall x \in F \;\; px = 0$.

2. Если для некоторого ненулеувого элемента x поля F выполнено $nx = 0$, то $n = \mathrm{char}F$, где n —наименьшее натуральное число со свойством $nx = 0$.

Доказательство. 1. Рассмотрим $x \in F$, тогда

$$px = \underbrace{x + x + \ldots + x}_{p \text{ слагаемых}} = \underbrace{1 \cdot x + 1 \cdot x + \ldots + 1 \cdot x}_{p \text{ слагаемых}} =$$

$$= (\underbrace{1 + 1 + \ldots + 1 + 1}_{p \text{ слагаемых}}) \cdot x = (p1) \cdot x = 0 \cdot x = 0.$$

2. Пусть $x \neq 0$ и $nx = 0$. Тогда повторяя выкладки из 1), имеем

$$0 = nx = (\underbrace{1 + 1 + \ldots + 1 + 1}_{n \text{ слагаемых}}) \cdot x = (n1) \cdot x.$$

Так как $x \neq 0$, по теореме 2.4.1, получим, что $n1 = 0$. Далее, если n – наименьшее натуральное число со свойством $nx = 0$, то n одновременно наименьшее натуральное число со свойством $n1 = 0$ (достаточно прочесть приведенные равенства справа налево). Таким образом $n = \mathrm{char}F$. Теорема доказана.

2.4.2. *Конечные поля*

Определение 2.4.2. *Поле, имеющее конечное число элементов, называется* **полем Галуа.**

Теорема 2.4.4 (о цикличности мультипликативной группы поля Галуа). *Мультипликативная группа поля Галуа циклическая.*

Доказательство. Пусть порядок поля F равен $n + 1 : F = \{0, a_1, a_2, \ldots, a_n\}$. Пусть в мультипликативной группе поля $\langle F \setminus \{0\}, \{\cdot, 1\}\rangle$ a_1 – элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$.

Пусть элемент y из $F\setminus\{0\}$ не является корнем этого многочлена. Тогда $y^m \neq 1$. Так как m не делится на $|y|$, то для некоторого простого числа q имеем $m = uq^s, \quad |y| = vq^t, \quad s < t$, числа u и q взаимно просты. Обозначим через z элемент y^v. В частности,

$$z^{q^t} = y^{uq^t} = y^{|y|} = e \;\Rightarrow\; |z| = q^t.$$

Пусть $|a_1 \cdot z| = k$.

$$(a_1 \cdot z)^k = \underbrace{(a_1 \cdot z) \cdot (a_1 \cdot z) \cdot \ldots \cdot (a_1 \cdot z)}_{k \text{ раз}} \underbrace{=}_{\text{«}\cdot\text{» коммутативна}} a_1^k \cdot z^k = e$$

Тогда $a_1^k = (z^{(-1)})^k$. Следовательно, поскольку $|z| = |z^{(-1)}| = q^t$ – степень простого число, то порядок любой степени как делитель $|z|$ есть степень простого q и, в частности, $(z^{(-1)})^k$ равен q^r. Значит,

$$|a_1^k| = q^r \Big| \;\; |a_1| = m = uq^s \;\Rightarrow\; u \Big| \; k :$$

k делится на u: $k = uw$.

С другой стороны,

$$((a_1 \cdot z)^{(q^s)})^{uq^{(t-s)}} = (a_1 \cdot z)^{uq^t} = e$$

поэтому $\left|(a_1 \cdot z)^{(q^s)}\right| = uq^{(t-s)}$, поэтому рассуждением «от противного» легко получить, что k делится и на q^t.Таким образом, k делится на число uq^t, большее m, что противоречит максимальности m.

$|P| = n + 1, \quad P = \{0, a_1, a_2, \ldots, a_n\}, \quad a_1$ – элемент наибольшего порядка m. Доказано, что каждый ненулевой элемент поля P является корнем многочлена $x^m - 1$. Но количество ненулевых элементов $n \geq m$, т. е. количество корней многочлена больше либо равно его степени, следовательно $n = m$. Поскольку $| < a_1 > | = m$, то все элементы a_i исчерпываются степенями a_1, т. е. мультипликативная группа поляявляется циклической. Теорема доказана.

Определение 2.4.3. *Если элемент ϑ является порождающим мультипликативной группы конечного поля P т. е. $< \vartheta >= \{P \setminus \{0\}\}$, тогда он называется* **примитивным.**

Примитивные элементы имеют важное значение в строении конечного поля. Поскольку каждый ненулевой элемент есть степень примитивного, как порождающего циклической группы, вычисление произведений в конечных полях сводится к арифметике целых чисел – показателей степеней элемента ϑ:

$$\vartheta^m \cdot \vartheta^n = \vartheta^{m+n}.$$

Как в любой алгебре, в полях можно рассматривать подалгебры – подполя (см. определение 2.1.3).

Определение 2.4.4. *Если поле P содержится в поле F, то P является* **подполем в** F, *а F называется* **расширением** *поля P.*

Определение 2.4.5. *Подполе P из поля F, называется* **собственным подполем в** F, *если оно отлично от F. Поле, не содержащее собственных подполей, называется* **простым полем.**

Теорема 2.4.5 (о порядке простого конечного поля). *Конечное поле является простым тогда и только тогда, когда количество элементов поля F равно простому числу.*

Доказательство. Необходимость. Пусть F – простое конечное поле характеристики p. Тогда очевидно, что множество $P = \{1, 1+1, \ldots, p1 = 0\}$ замкнуто относительно операций «+» и «·». Следовательно, P – подполе в F. В силу простоты поля F имеем $F = P$, в частности, его порядок равен p. Необходимость доказана, так как, в силу теоремы о характеристике поля 2.4.2, p – простое число.

Достаточность. Пусть $|F| = p$ – простое число. Аддитивная группа любого подполя Q поля F является подгруппой аддитивной группы поля F. По теореме Лагранжа 2.3.4 ее порядок $|Q|$ делит $|P| = p$, но у простого числа нет неединичных собственных делителей. Следовательно, $|Q| = |F|$, откуда следует, что $F = Q$, что и требовалось доказать.

Пример. Простым полем порядка p является кольцо классов вычетов по модулю простого числа p. Это поле строится как фактор-кольцо целых чисел $\mathbb{Z}$ по конгруэнции $\pi : x\pi y \Leftrightarrow p \Big| (x - y)$. Заметим, что всякое конечное простое поле характеристики p изоморфно полю классов вычетов по модулю p, т. е. фактор-кольцу $\mathbb{Z}/\pi$.

Дальнейшей нашей целью будет доказательство того, что порядок любого конечного поля равен p^t для некоторого простого числа p. В частности, будет обосновано стандартное обозначение полей Галуа: $GF(p^t)$. Для этого потребуются некоторые факты теории расширения полей, изложенные в следующем разделе.

2.4.3. *Расширения полей*

Теорема 2.4.6 (о надполе, как линейном пространстве). *Пусть F – расширение поля P. В поле F определена операция сложения элементов,*

и операция умножения на элементы поля P. Относительно этих операций поле F является линейным пространством над полем P.

Доказательство сводится к легкой проверке выполнения аксиом линейного пространства.

Определение 2.4.6. *Если расширение F поля P имеет конечную размерность d, как линейное пространство над P, то поле F называется* **конечным расширением поля** *P, и число d называется* **степенью расширения** *F поля P. В противном случае говорят, что F - расширение поля P* **бесконечной степени**. *Обозначение: $d = |F : P|$.* [1]

Пример. Каждое комплексное число имеет вид $z = x + iy$, где $x, y \in \mathbb{R}$, а $i \notin \mathbb{R}$. Поэтому можно интерпретировать алгебраическую форму записи числа z, как разложение по базису $1, i$ с коэффициентами из $\mathbb{R}$. Другими словами, поле комплексных чисел $\mathbb{C}$ есть линейное пространство размерности 2 над числовым полем $\mathbb{R}$ и является его расширением. Поэтому $|\mathbb{C} : \mathbb{R}| = 2$.

Теорема 2.4.7 (о порядке конечного поля). *Конечное поле содержит p^t элементов, где p – простое число, t – неотрицательное целое число.*

Доказательство. Пусть характеристика поля F равна p – простое число (теорема 2.4.2). По теореме 2.4.5 либо F простое и тогда $|F| = p$ либо F содержит простое подполе P порядка p. Пусть поле F – расширение поля P степени $t = |F : P|$. По теореме 2.4.6 F – линейное пространство над P размерности t. Если $\{s_1, \ldots, s_t\}$ – некоторый базис этого пространства, то каждый элемент x поля F имеет вид:

$$x = \alpha_1 \cdot s_1 + \ldots + \alpha_t \cdot s_t, \quad \alpha_i \in P.$$

Но тогда количество всех таких элементов равно p^t, что и требовалось доказать.

Определение 2.4.7. *Говорят, что поле F получено* **присоединением элементов** *$s_1, s_2, \ldots, s_n$ к полю P (пишут $F = P(s_1, s_2, \ldots, s_n)$), если F – наименьшее поле*[2]*, содержащее как P так и все элементы $s_1, s_2, \ldots, s_n$. Если $F = P(s)$, то поле F называется* **простым расширением поля** *P.*

Пример. Строение комплексных чисел позволяет заключить, что $\mathbb{C} = \mathbb{R}(i)$. Легко показать, что множество чисел $\mathbb{Q}(\sqrt{2}) = \{x + \sqrt{2}y | x, y \in \mathbb{Q}\}$ является полем и , следовательно, $\mathbb{Q} < \mathbb{Q}(\sqrt{2}) < \mathbb{R}$.

[1] Не стоит путать с индексом группы F по подгруппе P с тем же обозначением (с.69).

[2] F наименьшее поле, т. е. в F нет собственных подполей, содержащих одновременно все элементы поля P и элементы $s_1, s_2, \ldots, s_n$.

Заметим, что конечное расширение (конечной степени) получено присоединением конечного числа элементов, но обратное неверно поскольку присоединение конечного числа элементов может иметь бесконечную степень.

Рассмотрим простые расширения полей, т. е. полученные присоединением одного элемента.

Теорема 2.4.8. *$m = |P(s) : P|$ – степень расширения поля P, полученного присоединением элемента s тогда и только тогда, когда s является корнем многочлена $f(x)$ минимальной степени m с коэффициентами из P:*

$$f(x) = a_0\mathbf{1} + a_1x + a_2x^2 + \ldots + a_mx^m,\ a_i \in P,\ f(s) = 0,$$

и каждый элемент $P(s)$ есть линейная комбинация степеней s:

$$P(s) = \left\{\alpha_1 s^0 + \alpha_2 s + \ldots + \alpha_m s^{m-1} \middle| \alpha_i \in P\right\}.$$

Доказательство. Докажем здесь лишь необходимость. Пусть s является алгебраическим над полем P. Обозначим через m размерность линейного пространства $P(s)$ над полем P (теорема 2.4.6). Тогда система векторов $\left\{1, s, s^2, \ldots, s^m\right\}$ является линейно зависимой, так как в ней $m+1$ вектор. Следовательно, в P существуют такие элементы $a_0, \ldots a_m$, не все из которых равны 0, имеем

$$a_0\mathbf{1} + a_1s + a_2s^2 + \ldots + a_ms^m = \mathbf{0}.$$

Необходимость доказана.

Определение 2.4.8. *Пусть P – подполе в F. Элемент f поля F называется* **алгебраическим над полем** *P, если $|P(f) : P| < \infty$. В противном случае ($|P(f) : P| = \infty$) элемент f называется* **трансцендентным над полем** *P.*

Пример. Приведем примеры как алгебраических так и трансцендентных элементов над полем $\mathbb{Q}$. Действительно, $\sqrt{2}$ – алгебраический, т. к. корень многочлена $x^2 - 2$ с рациональными коэффициентами. Числа e, π – трансцендентные, т. к. нет многочлена с рациональными коэффициентами, корнями которых являются эти числа. В частности $\mathbb{R}$ есть бесконечное расширение $\mathbb{Q}$.

Соберем все доказанные факты теории конечных полей воедино.

Строение конечного поля F

1. $\mathrm{char}F = p$, *p – простое число;* $|F| = p^t$, *обозначение конечного поля* $GF(p^t)$ *(теорема2.4.7 на стр. 78).*

2. $GF(p^t) = \{0, \vartheta^0 = 1 = \vartheta^{p^t-1}, \vartheta^1, \vartheta^2, \ldots, \vartheta^{p^t-2}\}$, *где ϑ – примитивный элемент (теорема2.4.4 на стр. 75).*

3. Если P – простое подполе $GF(p^t)$, то $|P| = p$ и
$GF(p^t) = P(\vartheta) = \left\{a_1 + a_2\vartheta + \ldots + a_t\vartheta^{t-1} \,\middle|\, a_i \in P\right\}$, *где ϑ – примитивный элемент либо*
$GF(p^t) = P(s) = \left\{a_1 + a_2 s + \ldots + a_t s^{t-1} \,\middle|\, a_i \in P\right\}$, *где $s = \vartheta^\beta$, $P(s) = P(\vartheta)$ и s может не быть примитивным (теорема2.4.8 на стр. 79).*

4. $GF(p^t) = P(s)$, $|GF(p^t) : P| = m$, тогда и только тогда, когда $f(s) = 0$, где $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$, $a_i \in P$ (теорема2.4.8 на стр. 79).

Дополним приведенные факты теоремой о подполях конечного поля.

Теорема 2.4.9 (о подполях конечного поля). *Если поле F конечно, т. е. $F = GF(p^t)$ и $P = GF(p^d)$ – подполе в F, тогда d делит t. Обратно: если $F = GF(p^t)$ и d делит t, тогда существут и единственное подполе P в F такое, что $P = GF(p^d)$.*

Вычисления в конечных полях используются, например, в теории кодов. Все приведенные теоремы являются основой этих вычислений. Также отметим, что конечные поля описываются на языке многочленов, что уже видно в теореме 2.4.8. Однако, необходимые сведения о делимости в кольце многочленов и их связи с конечными полями планируется изложить во второй части пособия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. **Ершов, Ю.Л.** Математическая логика / Ю.Л. Ершов, Е.А. Палютин. – СПб. : Лань, 2004. – 336 с.

2. **Мендельсон, Э.** Введение в математическую логику / Э. Мендельсон. – М. : Наука, 1984. – 320 с.

3. **Мельников, Ю.Б.** Алгебра и теория чисел. Изд-е 4-е, испр. и доп. [Электронный ресурс] / Ю.Б. Мельников. – Екатеринбург : Издательство УрГЭУ, 2010. – 70 уч.-изд.л. [режим доступа свободный] http : //lib.usue.ru/resource/free/12/MelnikovAlgebra4/index.html

4. **Новиков, Ф.А.** Дискретная математика / Ф.А. Новиков. – М.,СПб. : Питер, 2013. – 432 с.

5. **Яблонский, С.В.** Введение в дискретную математику / С.В. Яблонский. – М. : Высшая школа, 2001. – 384 с.

Электронный текстовый ресурс

Голикова Елена Александровна

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Подготовка к публикации – Овчинниковой А.В.
Компьютерная верстка – Голиковой Е.А.

Рекомендовано Методсоветом УрФУ
Разрешено к публикации 03.10.2017
Электронный формат – pdf
Объем 3,47 уч.-изд.л.

62002, Екатеринбург, ул. Мира, 19

Уральский федеральный университет

информационный портал УрФУ
http//www.urfu.ru