Глава 4

Группы, кольца, поля

4.1. Бинарная алгебраическая операция

Сложение, вычитание, умножение чисел — это примеры бинарных операций. Двум числам каждая их этих операций ставит в соответствие третье число. С другой стороны, функции $\sin x$ или $\ln x$ бинарными операциями не являются, так как ставят в соответствие число не паре, а только одному числу. Дадим строгое определение.

Пусть A — непустое множество. Правило, которое каждой упорядоченной паре элементов (*операндов*) из A ставит в соответствие элемент из A, называется *бинарной алгебраической операцией*[1] *на множестве* A (или *над* A). Иными словами, бинарная алгебраическая операция есть отображение

$$\circ : \ A^2 \to A.$$

Для обозначения результата бинарной операции используют *инфиксную* форму записи, помещая символ операции между операндами: $a \circ b$. В конкретных случаях операция может иметь специальные названия и обозначения, например, сложение «$+$», умножение «$\cdot$» и т. п. В этом случае результат обозначается соответственно $a + b$, $a \cdot b$ и т. д. Для умножения знак операции часто совсем опускается.

Результат операции может являться операндом для другой операции и т. д. Для указания порядка выполнения операций используют скобки. Например,

$$(a \circ b) \circ (c \circ d). \tag{4.1}$$

Здесь вначале вычисляются $a \circ b$ и $c \circ d$. Затем к результатам снова применяется операция $\circ$. Если скобки не стоят, то считаем, что операция действует слева направо. Заметим, что в общем случае результат зависит от того, как расставлены скобки.

Упражнение 4.1. Выписать все способы расстановки скобок в выражениях $a \circ b \circ c$, $a \circ b \circ c \circ d$.

Бинарная операция $\circ$ называется *ассоциативной*, если для любых a, b, c из A

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

Бинарная операция $\circ$ называется *коммутативной*, если для любых a, b из A

$$a \circ b = b \circ a.$$

[1] Иногда бинарную алгебраическую операцию называют просто алгебраической.

Элемент e из A называется *нейтральным* относительно бинарной операции $\circ$, если для любого a из A

$$a \circ e = e \circ a = a.$$

Элемент b из A называется *симметричным* к a относительно бинарной операции $\circ$, если

$$a \circ b = b \circ a = e.$$

Если $B \subseteq A$ и для любых a, b из B элемент $a \circ b$ также принадлежит B, то говорят, что B *замкнуто относительно операции* $\circ$. Очевидно, A замкнуто относительно любой бинарной алгебраической операции, заданной над A.

Пример 4.2. Рассмотрим операцию *сложения* чисел. Над $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ сложение — это бинарная алгебраическая операция, коммутативная и ассоциативная. Нейтральным элементом относительно этой операции является число 0. Для любого элемента a существует симметричный, называемый в данном случае *противоположным* и обозначамый $-a$.

Сложение над множеством $\mathbb{N}$ по-прежнему является бинарной алгебраической операцией, коммутативной и ассоциативной, но уже не обладает нейтральным элементом. Сложение над множеством $\mathbb{N} \cup \{0\}$ является бинарной алгебраической операцией и теперь обладает нейтральным элементом 0, но симметричный (противоположный) элемент существует здесь только для 0 и ни для какого другого элемента.

Пример 4.3. Теперь рассмотрим *умножение*. Над $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$ умножение — это бинарная алгебраическая операция, коммутативная и ассоциативная. Нейтральным элементом относительно этой операции является число 1. Над $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ для любого ненулевого элемента a относительно операции умножения существует симметричный a^{-1}, называемый в этом случае *обратным*. Над $\mathbb{Z}$ обратный элемент существует только для 1 и -1. Над $\mathbb{N}$ — только для 1.

Пример 4.4. *Вычитание* является бинарной алгебраической операцией, например, над каждым из следующих множеств: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Эта операция не является ни коммутативной, ни ассоциативной и не обладает нейтральным элементом. Над $\mathbb{N}$ вычитание не является бинарной алгебраической операцией, так как существуют натуральные числа a, b, такие, что $a - b \notin \mathbb{N}$.

Пример 4.5. *Деление* не является бинарной алгебраической операцией ни над одним из множеств $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, так как не определена операция деления на 0. Ситуацию можно «спасти», если из этих множеств исключить 0. Пусть A — некоторое (конечное или бесконечное) числовое множество. Обозначим через $A^* = A \setminus \{0\}$ множество его ненулевых чисел. Легко видеть, что деление является бинарной алгебраической операцией (некоммутативной и неассоциативной и без нейтрального элемента) над $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$. Однако не будет являться таковым для $\mathbb{Z}^*$, так как существуют целые ненулевые числа a, b, такие, что $a/b \notin \mathbb{Z}$. По той же причине деление не является бинарной алгебраической операцией над $\mathbb{N}$.

Пример 4.6. На множестве $\mathbf{V}_2$ геометрических векторов плоскости и множестве $\mathbf{V}_3$ геометрических векторов пространства сложение векторов является бинарной алгебраической операцией. Эта операция коммутативна, ассоциативна и обладает нейтральным элементом — нулевым вектором, причем для любого вектора существует симметричный (противоположный). Скалярное произведение бинарной алгебраической операцией не является, так как каждой паре векторов ставит в соответствие число, а не вектор.

Пример 4.7. На множестве классов вычетов $\mathbb{Z}_n$, где $n \geq 1$, определенные ранее операции сложения, вычитания и умножения являются алгебраическими бинарными операциями. Причем, легко видеть, что сложение и умножение — коммутативные и ассоциативные, а вычитание (при $n > 1$) не ассоциативно и не коммутативно.

Упражнение 4.8. Выяснить свойства операций НОД и НОК на множестве $\mathbb{N}$ (является ли бинарной алгебраической операцией, коммутативность, ассоциативность, наличие нейтрального элемента, симметричных элементов).

Если операция ассоциативна, то в выражениях вида (4.1) способ расстановок скобок не важен. Действительно, справедливо следующее.

Утверждение 4.9 (Обобщенная ассоциативность)**.** *Пусть $a_1, a_2, \ldots, a_n$ — элементы множества A, на котором задана ассоциативная операция $\circ$. Тогда*[2] *для любого k*

$$(a_1 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ a_n) = a_1 \circ a_2 \circ \ldots \circ a_n.$$

Доказательство. Докажем свойство индукцией по n. При $n \leq 3$ доказываемое равенство либо тривиально, либо представляет собой запись свойства ассоциативности. При $n > 3$ имеем

$$(a_1 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ a_n) = (a_1 \circ \ldots \circ a_k) \circ (a_{k+1} \circ \ldots \circ a_{n-1}) \circ a_n.$$

По предположению индукции

$$(a_1 \circ a_2 \circ \ldots \circ a_k) \circ (a_{k+1} \circ a_2 \circ \ldots \circ a_{n-1}) = a_1 \circ a_2 \circ \ldots \circ a_{n-1},$$

откуда получаем требуемое. ∎

Утверждение 4.10 (Обобщенная коммутативность)**.** *Пусть $j_1, j_2, \ldots, j_n$ — перестановка чисел $1, 2, \ldots, n$, и пусть $a_1, a_2, \ldots, a_n$ — элементы из множества A, на котором задана ассоциативная и коммутативная операция $\circ$. Тогда*

$$a_{j_1} \circ a_{j_2} \circ \ldots \circ a_{j_n} = a_1 \circ a_2 \circ \ldots \circ a_n.$$

Доказательство. Свойство докажем индукцией по n. При $n \leq 2$ доказываемое равенство либо тривиально, либо представляет собой запись свойства коммутативности. Пусть k такое, что $j_k = n$, тогда

$$a_{j_1} \circ a_{j_2} \circ \ldots \circ a_{j_n} = (a_{j_1} \circ \ldots \circ a_{j_{k-1}}) \circ a_n \circ (a_{j_{k+1}} \circ \ldots \circ a_{j_n}).$$

Два раза используя предположение индукции и применяя ассоциативность, выводим

$$(a_{j_1} \circ \ldots \circ a_{j_{k-1}}) \circ a_n \circ (a_{j_{k+1}} \circ \ldots \circ a_{j_n}) = (a_{j_1} \circ \ldots \circ a_{j_{k-1}}) \circ (a_{j_{k+1}} \circ \ldots \circ a_{j_n}) \circ a_n = (a_1 \circ \ldots \circ a_{n-1}) \circ a_n$$

откуда получаем требуемое. ∎

4.2. Полугруппа

Пусть бинарная алгебраическая операция $\circ$, заданная на A, ассоциативна, тогда A называется *полугруппой*. Если операция к тому же коммутативна, то полугруппа называется *коммутативной полугруппой*. Если множество A конечно, то $|A|$ (число элементов в A) называется *порядком* полугруппы A.

Пусть A — полугруппа относительно операции $\circ$, Тогда B называется *подполугруппой* полугруппы A, если $B \subseteq A$ и B является полугруппой относительно той же операции $\circ$. Легко видеть, что для того, чтобы B являлось подполугруппой группы A необходимо и достаточно, чтобы B было замкнуто относительно операции $\circ$.

Пример 4.11. Примеры коммутативных полугрупп:

1) $\mathbb{N}$ и $\mathbb{Z}$ относительно сложения, причем первая является подполугруппой второй;

2) $\mathbb{N}$ и $\mathbb{Z}$ относительно умножения, и также первая является подполугруппой второй;

[2] Напомним, что если скобки не расставлены, то порядок выполнения операции — слева направо.

3) $\mathbb{Z}_-$ (множество отрицательных целых чисел) относительно сложения.

Пример 4.12. Полугруппами *не* являются, например, $\mathbb{N}$ относительно вычитания (не бинарная алгебраическая операция), $\mathbb{N}$ относительно деления (не бинарная алгебраическая операция), $\mathbb{Z}$ относительно вычитания (отсутствие ассоциативности), $\mathbb{Z}$ относительно деления (не бинарная алгебраическая операция).

Приведем пример некоммутативной полугруппы. Пусть X — некоторое множество. Рассмотрим множество Φ_X всех отображений $X \to X$. Определим операцию *умножения* отображений (также используются названия «*композиция*» и «*суперпозиция*» отображений). Пусть $\varphi \in \Phi_X$, $\psi \in \Phi_X$. Под произведением отображений φ и ψ понимается отображение, обозначаемое $\varphi\psi$ и определенное по следующей формуле:

$$(\varphi\,\psi)\,x = \varphi\,(\psi x) \tag{4.2}$$

для любого $x \in X$. Таким образом, отображение $\varphi\psi$ получается в результате последовательного применения сначала отображения ψ, а затем — отображения φ. Обратите внимание, что, таким образом, результирующее преобразование вычисляется «справа налево». Очевидно, что операция умножения является алгебраической бинарной операцией на множестве Φ_X. Так как для любого $x \in X$

$$(\varphi(\psi\vartheta))x = \varphi((\psi\vartheta)x) = \varphi(\psi(\vartheta x)) = (\varphi\psi)(\vartheta x) = ((\varphi\psi)\vartheta)x,$$

то $\varphi\,(\psi\,\vartheta) = (\varphi\,\psi)\,\vartheta$, следовательно, эта операция ассоциативна, поэтому Φ_X — полугруппа. При $|X| \geq 2$, эта полугруппа некоммутативная. Она содержит нейтральный элемент — так называемое *тождественное* (или *единичное*) отображение ε, такое, что $\varepsilon x = x$. Однако при $|X| > 1$ не каждое отображение обладает обратным (симметричным). Обратимыми элементами (т. е. теми, для которых существует обратный) в Φ_X являются биекции (взаимно однозначные отображения) и только они.

Пусть $X = \{x_1, x_2, \ldots, x_n\}$ конечно. Тогда отображение φ удобно задавать в виде таблицы

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \varphi x_1 & \varphi x_2 & \ldots & \varphi x_n \end{pmatrix}. \tag{4.3}$$

Если множество X конечно, то, очевидно, $|\Phi_X| = n^n$.

Заметим, что разные таблицы вида (4.3) могут задавать одно и то же преобразование. Например, таблицы

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 2 & 4 & 1 & 3 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

задают одно и то же отображение множества $\{1, 2, 3, 4\}$ в себя.

Пример 4.13. Пусть $X = \{1, 2\}$. Построим множество Φ_X. Всего имеется 4 отображения:

$$\varepsilon = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Вычислим, например, произведения[3]:

$$ab = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ \downarrow & \downarrow \\ 1 & 1 \\ \downarrow & \downarrow \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = c,$$

[3]Внимание: уножение отображений не следует путать с матричнм умножением.

$$ba = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ \downarrow & \downarrow \\ 2 & 1 \\ \downarrow & \downarrow \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = b.$$

Тождественное отображение ε является нейтральным (единичным) элементом. Очевидно, это отображение само для себя является симметричным (обратным). Также обратным обладает еще элемент a. Он также является обратным сам для себя. Обратите внимание, что $ab \neq ba$, значит полугруппа некоммутативная. В следующей таблице (*таблице умножения*) сведены воедино результаты применения операции умножения к каждой паре элементов из Φ_X. Результат операции, примененной, например, к элементам a и b, нужно найти на пересечении строки с меткой a (первый операнд) и столбца с меткой b (второй операнд). Проверьте правильность таблицы.

	ε	a	b	c
ε	ε	a	b	c
a	a	ε	c	b
b	b	b	b	b
c	c	c	c	c

Обратите внимание, что, например, каждое из подмножеств $\{\varepsilon, a\}$ и $\{b, c\}$ образуют подполугруппу группы Φ_X.

Упражнение 4.14. В Φ_X из примера 4.13 найти все подполугруппы.

Упражнение 4.15. Рассмотрим множество линейных функций $\varphi : \mathbb{R} \to \mathbb{R}$, т. е. отображений вида $\varphi x = ax + b$, где a, b — произвольные числа из $\mathbb{R}$. Является ли это множество подполугруппой в $\Phi_{\mathbb{R}}$? Тот же вопрос для множества отображений вида $\varphi x = ax + b$, где $a \neq 0$.

Утверждение 4.16. *Если полугруппа обладает нейтральным элементом, то других нейтральных элементов в полугруппе нет.*

Доказательство. Пусть e_1 и e_2 — нейтральные элементы в M. Тогда

$$e_1 = e_1 \circ e_2 = e_2,$$

т. е. $e_1 = e_2$. ∎

Утверждение 4.17. *Пусть полугруппа содержит нейтральный элемент e. Если элемент a имеет симметричный элемент a', то других симметричных элементов у a нет.*

Доказательство. Пусть a' и a'' — симметричные элементы к a. Имеем

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a'',$$

т. е. $a' = a''$. ∎

4.3. Группа

Полугруппа G с нейтральным элементом, в которой для каждого элемента существует симметричный, называется *группой*. Если операция $\circ$ коммутативна, то группа называется *коммутативной* или *абелевой*. Если множество G конечно, то $|G|$ (число элементов в G) называется *порядком* группы G.

Согласно утверждению 4.16 нейтральный элемент группы единственен. Согласно утверждению 4.17 для любого элемента группы симметричный элемент единственен.

Если групповая операция называется сложением (и обозначается $+$), то группа называется *аддитивной*. В этом случае нейтральный элемент называют *нулем* (или *нулевым элементом*) и обозначают 0. Элемент b, симметричный к a, называют *противоположным* и обозначают $-a$. Если групповая операция называется умножением (и обозначается $\times$ или $\cdot$), то группа называется *мультипликативной*. В этом случае нейтральный элемент называют *единицей* (или *единичным элементом*) и обозначают e или 1. Элемент b, симметричный к a, называют *обратным* и обозначают a^{-1}. Часто значок операции в мультипликативных группах опускается, т. е. вместо $a \cdot b$ или $a \times b$ пишут ab.

Обратим внимание, что термины «аддитивный», «мультипликативный» говорят не о каких-то дополнительных свойствах групповой операции, а только о способе ее обозначения и названии. Пожалуй, единственным исключением является следующее: сложением называют всегда коммутативную операцию, поэтому аддитивные группы абелевы.

Пусть G — группа относительно операции $\circ$. Тогда G' называется *подгруппой* группы G, если $G' \subseteq G$ и G является группой относительно той же операции $\circ$. Легко видеть, что для того, чтобы G' являлось подгруппой группы G необходимо и достаточно, чтобы G' было замкнуто относительно операции $\circ$, в G' существовал единичный элемент и для любого элемента из G' нашелся бы симметричный в G'.

Пример 4.18. Примеры абелевых групп:

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ относительно сложения, причем $\mathbb{Z}$ — подгруппа в $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и т. д.;
2) $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ относительно умножения, где через F^* обозначено множество ненулевых элементов в F, причем $\mathbb{Q}^*$ — подгруппа в $\mathbb{R}^*$ и $\mathbb{C}^*$, а $\mathbb{R}^*$ — подгруппа в $\mathbb{C}^*$;
3) множество U_n всех значений корня n-й степени из 1 относительно умножения;
4) множество U всех комплексных чисел по модуля равных 1;
5) $\mathbf{V}_2$, $\mathbf{V}_3$ относительно сложения;
6) множество $\mathbb{Z}_n$ классов вычетов по модулю n относительно сложения; эта группа называется *группой вычетов по модулю n*.

Пример 4.19. Группами не являются, например, $\mathbb{N}$ относительно сложения, $\mathbb{Z}$ относительно вычитания, Φ_X при $|X| \geq 2$.

Далее, говоря об абстрактных группах мы будем использовать мультипликативные обозначения, а именно, групповую операцию будем называть умножением и обозначать $\cdot$ (а чаще опускать значок операции), нейтральный элемент будем называть единичным и обозначать e, симметричный к a элемент называть обратным и обозначать a^{-1}. Рассматривая конкретные примеры групп, мы разумеется будем оставлять принятые для этих групп обозначения.

Утверждение 4.20. *Пусть a, b — некоторые элементы из группы G. Тогда каждое из уравнений $ax = b$, $ya = b$ имеет, причем единственное, решение в G: $x = a^{-1}b$, $y = ba^{-1}$.*

Доказательство. Проверим, что $x = a^{-1}b$ является решением уравнения $ax = b$:

$$ax = a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Для доказательства единственности решения, предположим, что нашлось два решения: x и x'. Тогда $ax = b$, $ax' = b$, откуда

$$ax = ax'.$$

Умножая слева обе части этого тождества на a^{-1}, получаем

$$a^{-1}(ax) = a^{-1}(ax'),$$

пользуясь ассоциативностью, получаем

$$(a^{-1}a)x = (a^{-1}a)x',$$

откуда $ex = ex'$, т. е. $x = x'$.

Используя аналогичные рассуждения, легко проверить, что единственным решением уравнения $ya = b$ является $y = ba^{-1}$. ∎

Операция $\backslash$, определяемая формулой $a\backslash b = a^{-1}b$ называется *левым делением* (b *слева* делится на a). Операция $/$, определяемая формулой $b/a = ba^{-1}$ называется *правым делением* (b *справа* делится на a). Если группа G абелева, то это одна и та же операция (называемая просто *делением*).

Упражнение 4.21. Какие из следующих множеств чисел относительно сложения образуют полугруппу, а какие группу:

1) множество $\mathbb{N}$ натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $2\mathbb{Z}$ четных чисел;
6) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
7) множество $\mathbb{Q}$ рациональных чисел;
8) множество иррациональных чисел;
9) множество $\mathbb{R}$ вещественных чисел;
10) множество $\mathbb{C}$ комплексных чисел?

Упражнение 4.22. Какие из следующих множеств чисел относительно умножения образуют полугруппу, а какие группу:

1) множество $\mathbb{N}$ натуральных чисел;
2) множество целых неотрицательных чисел;
3) множество целых неположительных чисел;
4) множество $\mathbb{Z}$ целых чисел;
5) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
6) множество $\mathbb{Q}$ рациональных чисел;
7) множество $\mathbb{Q}^*$ ненулевых рациональных чисел;
8) множество $\mathbb{Q}_+$ положительных рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество $\mathbb{R}^*$ ненулевых вещественных чисел;
12) множество $\mathbb{R}_+$ положительных вещественных чисел;
13) множество $\mathbb{C}$ комплексных чисел;
14) множество $\mathbb{C}^*$ ненулевых комплексных чисел;
15) множество U_n всех значений корня n-й степени из 1;
16) множество всех корней натуральной степени из 1;
17) множество U всех комплексных чисел, по модулю равных 1;
18) множество H_n чисел вида

$$\rho\left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right),$$

где $\rho > 0$, $k = 0, 1, \ldots, n-1$?

Упражнение 4.23. Доказать, что мультипликативная группа всех значений корня n-й степени из 1 является единственной конечной мультипликативной группой с числовыми элементами порядка n, за исключением случая $n = 1$.

Упражнение 4.24. Пусть G — группа, a, b — ее произвольные элементы, e — единичный элемент, n — натуральное число. Доказать, что 1) $e^{-1} = e$; 2) $(a^{-1})^n = (a^n)^{-1}$; 3) $(a^{-1})^{-1} = a$; 4) $(ab)^{-1} = b^{-1}a^{-1}$.

Упражнение 4.25. Доказать, что если квадрат любого элемента группы равен единице, то группа абелева.

4.4. Симметрическая группа

Рассмотрим один из самых важных примеров группы.

Во множестве Φ_X всех преобразований некоторого непустого множества X рассмотрим подмножество S_X всех биекций. Легко видеть, что операция умножения преобразований замкнута на S_X, следовательно, S_X — подполугруппа. Далее, S_X обладает нейтральным элементом: его роль выполняет тождественное преобразование ε. Для любого элемента φ в S_X существует симметричный элемент — обратное преобразование ε^{-1}. Следовательно, S_X — группа. Эта группа при $|X| \geq 3$ абелевой не является.

Важную роль играет случай конечного множества X. Не нарушая общности, можем считать, что $X = \{1, 2, \ldots, n\}$. Тогда биекция φ множества X на себя называется *подстановкой* степени n, которую можно записать так:

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}, \tag{4.4}$$

где

$$(j_1,\ j_2,\ \ldots,\ j_n) \tag{4.5}$$

— *перестановка* чисел $1, 2, \ldots, n$, т. е. упорядоченный набор (кортеж), составленный из чисел $1, 2, \ldots, n$, записанных в некоторм порядке без повторений.

Заметим, что термины «подстановка» и «перестановка» тождественны. Действительно, кортеж длины n можно рассматривать как отображение, которое числу i ставит в соответствие i-й элемент кортежа. В этом случае перестановка $(j_1, j_2, \ldots, j_n)$ — это взаимно однозначное отображение множества $\{1, 2, \ldots, n\}$ на себя, которое числу i (номеру элемента в наборе) ставит в соответствие элемент j_i, т. е. подстановка. Мы будем использовать термины «подстановка» и «перестановка» как синонимы, обозначающие один и тот же объект. Разница обычно будет только в том, как мы будем *представлять* этот объект: в виде таблицы (4.4) или в виде кортежа (4.5).

Если $X = \{1, 2, \ldots, n\}$, то S_X называется *симметрической группой* или *группой подстановок* степени n и обозначается S_n. Порядок этой группы, очевидно, равен $n!$. Для подстановки φ, заданной таблицей (4.4), обратной, очевидно, является

$$\varphi^{-1} = \begin{pmatrix} j_1 & j_2 & \ldots & j_n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Пример 4.26. Рассмотрим группу S_3. В ней содержится 6 подстановок:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Таблица умножения для S_3 выглядит следующим образом:

	ε	a	b	c	d	f
ε	ε	a	b	c	d	f
a	a	ε	f	d	c	d
b	b	d	ε	f	a	c
c	c	f	d	ε	b	a
d	d	b	c	a	f	ε
f	f	c	a	b	ε	d

Подстановка

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k & i_{k+1} & \dots & i_n \\ i_2 & i_3 & \dots & i_k & i_1 & i_{k+1} & \dots & i_n \end{pmatrix} \tag{4.6}$$

называется *циклом*, причем k называется *длиной* цикла. Цикл длины 2 называется *транспозицией*. Кратко цикл (4.6) записывается так[4]: $(i_1\ i_2\ \dots\ i_{k-1}\ i_k)$. Разумеется, тот же цикл можно обозначить как $(i_2\ i_3\ \dots\ i_k\ i_1)$ или $(i_k\ i_1\ i_2\ \dots\ i_{k-2}\ i_{k-1})$ и т. п. Будем говорить, что этот цикл *составлен* из элементов $i_1, i_2, \dots, i_k)$. Для примера рассмотрим циклы

$$(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 \end{pmatrix},$$

$$(2\ 5\ 7\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 2 & 4 & 7 & 6 & 3 & 8 \end{pmatrix}.$$

Циклы $(i_1\ i_2\ \dots\ i_{k-1}\ i_k)$ и $(j_1\ j_2\ \dots\ j_{k-1}\ j_m)$ называются *независимыми*, если они составлены из разных наборов элементов, т. е. $i_p \neq j_q$ при $p \neq q$. Легко видеть, что независимые циклы коммутируют, т. е. если φ, ψ — независимые циклы, то $\varphi\psi = \psi\varphi$.

Почти очевидным является следующее

Утверждение 4.27. *Любая подстановка раскладывается в произведение независимых циклов. Такое представление единственно с точностью до порядка сомножителей.*

Пример 4.28. Разложим в произведение независимых циклов подстановку

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 5 & 2 & 7 \end{pmatrix} = (1\ 3\ 4)\,(2\ 6).$$

Для «полноты» к произведению $(1\ 3\ 4)\,(2\ 6)$ мы можем дописать циклы длины 1: $\varphi = (1\ 3\ 4)\,(2\ 6)\,(5)\,(7)$.

Утверждение 4.29. *Любую подстановку можно представить в виде произведения транспозиций.*

[4]Будьте внимательны: не перепутайте перестановку $(i_1, i_2\ \dots, i_{k-1}, i_k)$ и цикл $(i_1\ i_2\ \dots\ i_{k-1}\ i_k)$. Обычно в контексте всегда понятно, о чем идет речь, но для облегчения восприятия элементы, составляющие перестановку, мы всегда перечисляем, отделяя их запятыми, тогда как элементы, входящие в цикл, будем перечислять через пробел, не используя запятых.

Доказательство. В силу утверждения 4.27 достаточно представить в виде произведения транспозиций произвольный цикл. Легко проверить, что

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)\,(i_2\, i_k)\,(i_3\, i_k)\,(i_{k-1}\, i_k).$$

∎

Пусть φ — подстановка. Говорят, что пара $\varphi(i)$, $\varphi(j)$, где $i < j$, образует *инверсию* в подстановке φ, если $\varphi(i) > \varphi(j)$. Обозначим $\sigma(\varphi)$ общее число инверсий в подстановке φ. Если $\sigma(\varphi)$ четно, то подстановка называется *четной*. Если $\sigma(\varphi)$ нечетно, то подстановка называется *нечетной*.

Пример 4.30. Подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 5 & 2 & 7 \end{pmatrix}$$

содержит 9 инверсий: (3, 1), (3, 2), (6, 4), (6, 1), (6, 5), (6, 2), (4, 1), (4, 2), (5, 2). Подстановка нечетная.

Подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 7 & 4 & 6 \end{pmatrix}$$

содержит 4 инверсии: (2, 1), (5, 4), (7, 4), (7, 6). Подстановка четная.

Докажем, что транспозиция меняет четность подстановки.

Утверждение 4.31. *Пусть $\varphi = (p\, s)\psi$, где φ, ψ — подстановки, а $(p\, s)$ — транспозиция $(p \neq s)$. Тогда четности подстановок φ, ψ различны, т. е. одна из них четная, а другая нечетная.*

Доказательство. Если

$$\varphi = \begin{pmatrix} 1 & \ldots & p & \ldots & s & \ldots & n \\ i_1 & \ldots & i_p & \ldots & i_s & \ldots & i_n \end{pmatrix},$$

то

$$(p\, s)\varphi = \begin{pmatrix} 1 & \ldots & p & \ldots & s & \ldots & n \\ i_1 & \ldots & i_s & \ldots & i_p & \ldots & i_n \end{pmatrix},$$

Вначале рассмотрим транспозицию соседних элементов, т. е. $p = s + 1$:

$$(i_1, \ldots, i_{p-1}, i_p, i_{p+1}, i_{p+2}, \ldots, i_n) \to (i_1, \ldots, i_{p-1}, i_{p+1}, i_p, i_{p+2}, \ldots, i_n).$$

Легко видеть, что если $i_p < i_{p+1}$, то число инверсий увеличивается на 1 (появляется новая инверсия элементов i_p, i_{p+1}); если $i_p > i_{p+1}$, то число инверсий уменьшается на 1 (исчезает инверсия элементов i_p, i_{p+1}). Итак, транспозиция соседних элементов меняет четность.

Теперь рассмотрим транспозицию элементов i_p и i_s, где $s > p + 1$. Покажем, что такую инверсию можно осуществить с помощью серии транспозиций соседних элементов. Сначала

передвигаем i_p вправо на место элемента i_s:

$$\begin{array}{rll} & (i_1,\dots,i_{p-1},i_p,i_{p+1},i_{p+2},\dots,i_{s-2},i_{s-1},i_s,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_p,i_{p+2},\dots,i_{s-2},i_{s-1},i_s,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_p,\dots,i_{s-2},i_{s-1},i_s,i_{s+1},\dots i_n) & \to \\ & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_{p+3},\dots,i_p,i_{s-1},i_s,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_{p+3},\dots,i_{s-1},i_p,i_s,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_{p+3},\dots,i_{s-1},i_s,i_p,i_{s+1},\dots i_n) & \end{array}$$

Затем передвигаем элемент i_s влево:

$$\begin{array}{rll} & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_{p+3},\dots,i_{s-1},i_s,i_p,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_{p+3},\dots,i_s,i_{s-1},i_p,i_{s+1},\dots i_n) & \to \\ & \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_{p+2},i_s,\dots,i_{s-2},i_{s-1},i_p,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_{p+1},i_s,i_{p+2},\dots,i_{s-2},i_{s-1},i_p,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_s,i_{p+1},i_{p+2},\dots,i_{s-2},i_{s-1},i_p,i_{s+1},\dots i_n) & \to \\ \to & (i_1,\dots,i_{p-1},i_s,i_{p+1},i_{p+2},\dots,i_{s-2},i_{s-1},i_p,i_{s+1},\dots i_n). & \end{array}$$

Мы выполнили нечетное $(2(s-p)-1)$ число транспозиций соседних элементов. Каждая транспозиция меняет четность перестановки. В результате всей серии четность перестановки изменилась. ∎

Утверждение 4.32. *Четность подстановки равна четности числа транспозиций, входящих в ее представление.*

Доказательство. Пусть φ — произвольная подстановка. Согласно утверждению 4.29, φ можно представить в виде $\varphi = \tau_1\tau_2\dots\tau_s$, где $\tau_1,\tau_2,\dots,\tau_s$ — транспозиции, откуда $\varphi = \tau_1\tau_2\dots\tau_s\varepsilon$. Очевидно, что тождественная подстановка ε — четная. Теперь требуемое вытекает из утверждения 4.31. ∎

Утверждение 4.33. *Четность подстановки совпадает с четностью обратной подстановки.*

Доказательство. Разложим подстановку φ в произведение транспозиций: $\varphi = \tau_1\tau_2\dots\tau_s$. Очевидно, $\varphi^{-1} = \tau_s\tau_{s-1}\dots\tau_1$. Согласно утверждению 4.32, φ^{-1} имеет ту же четность, что и φ. ∎

Теорема 4.34. *Множество всех четных подстановок образуют подгруппу в S_n. При $n \geq 2$ ее порядок равен $n!/2$.*

Доказательство. Чтобы доказать замкнутость множества четных подстановок, рассмотрим две четные подстановки и разложим каждую в произведение транспозиций. Согласно утверждению 4.32, произведение этих подстановок также будет четным. Тождественная подстановка, разумеется, является четной. То, что подстановка, обратная четной, также является четной, следует из утверждения 4.33. ∎

Группа всех четных подстановок степени n называется *знакопеременной группой* и обозначается A_n.

Упражнение 4.35. Выписать транспозиции, с помощью которых можно перейти от перестановки $5, 2, 1, 3, 4$ к перестановке $1, 4, 2, 3, 5$.

Упражнение 4.36. Определить число инверсий в перестановках:
1) $1, 3, 5, 7, 2, 4, 8, 9, 6$;
2) $2, 1, 5, 4, 7, 6, 8, 9, 3$.

Упражнение 4.37. Определить число инверсий в перестановках:
1) $n, n-1, \ldots, 2, 1$;
2) $1, 3, 5, 7, \ldots, 2n-1, 2, 4, 6, 8, \ldots, 2n$;
3) $2, 4, 6, 8, \ldots, 2n, 1, 3, 5, 7, \ldots, 2n-1$.

Упражнение 4.38. В перестановке $i_1, i_2, \ldots, i_n$ имеется k инверсий. Сколько инверсий в перестановке $i_n, i_{n-1}, \ldots, i_1$?

Упражнение 4.39. Умножить подстановки:
1) $\begin{pmatrix} 1&2&3&4&5 \\ 2&4&3&1&5 \end{pmatrix} \cdot \begin{pmatrix} 1&2&3&4&5 \\ 4&1&2&5&3 \end{pmatrix}$; 2) $\begin{pmatrix} 1&2&3&4&5 \\ 3&2&4&5&1 \end{pmatrix} \cdot \begin{pmatrix} 1&2&3&4&5 \\ 4&1&3&2&5 \end{pmatrix}$.

Упражнение 4.40. Разложить подстановки на независимые циклы:
1) $\begin{pmatrix} 1&2&3&4&5 \\ 3&4&1&5&2 \end{pmatrix}$; 2) $\begin{pmatrix} 1&2&3&4&5 \\ 3&4&1&2&5 \end{pmatrix}$; 3) $\begin{pmatrix} 1&2&3&4&5 \\ 4&5&1&2&3 \end{pmatrix}$; 4) $(1\ 5)(1\ 4)(1\ 3)(1\ 2)$.

Упражнение 4.41. Вычислить $\begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 2&3&4&5&1&7&8&6&10&9 \end{pmatrix}^{100}$.

Упражнение 4.42. Доказать, что цикл длины k равен произведению $k-1$ транспозиций, поэтому цикл четной длины является нечетной подстановкой, а нечетной длины — четной подстановкой.

Пример 4.43.* Головоломка «15» представляет собой квадратную коробку 4×4, заполненную 15 квадратными фишками, на которых написаны числа от 1 до 15. Одно место в коробке, остается свободным. Фишки размещаются произвольным образом, например:

6	14	2	4
10	1		5
13	8	9	15
7	12	3	11

(4.7)

На свободное место можно передвигать любые соседние фишки. В позициии на рисунке выше на свободное место можно передвинуть 1, 2, 5, 9. Фишки запрещается вынимать из коробки. Задача состоит в том, чтобы прийти к состоянию:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(4.8)

(свободное место находится справа внизу). Покажем, что из начального положения, представленного ниже

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(4.9)

(фишки 14 и 15 поменяли свое положение) никакой последовательностью разрешенных ходов нельзя прийти в состояние (4.8).

Рассмотрим некоторое размещение фишек в коробке. Обходя *зигзагообразно* все фишки, начиная с левого верхнего угла, и записывая встречающиеся номера (на свободное место не обращаем внимания) составим перестановку $j_1, j_2, \dots j_{15}$. Например, для схемы (4.7) получим перестановку

$$6,\ 14,\ 2,\ 4,\ 5,\ 1,\ 10,\ 13,\ 8,\ 9,\ 15,\ 11,\ 3,\ 12,\ 7.$$

Перестановки, соответствующие схемам (4.8) и (4.9), имеют разную четность (так как перейти от одной к другой можно одной транспозицией). С другой стороны, покажем, что разрешенные ходы четности не меняют. Этим будет доказано, что из положения (4.9) нельзя перейти в (4.8).

Очевидно, горизонтальные перемещения фишек не меняют соответствующие им перестановки. Рассмотрим вертикальные перемещения. Так как четность прямой и обратной подстановки одинакова, то достаточно рассмотреть только перемещения из первого (верхнего) ряда во второй. Перемещение вниз фишки j_1 в ситуации

j_1	j_2	j_3	j_4
	j_7	j_6	j_5

переводит перестановку $j_1, j_2, j_3, j_4, j_5, j_6, j_7$ в $j_2, j_3, j_4, j_5, j_6, j_7, j_1$, что эквивалентно циклу $(j_1\, j_2\, j_3\, j_4\, j_5\, j_6\, j_7)$. Длина цикла равна 7, поэтому согласно упражнению 4.42 четность не изменилась.

Перемещение вниз фишки j_2 в ситуации

j_1	j_2	j_3	j_4
j_7		j_6	j_5

переводит перестановку $j_1, j_2, j_3, j_4, j_5, j_6, j_7$ в $j_1, j_3, j_4, j_5, j_6, j_2, j_7$, что эквивалентно циклу $(j_2\, j_3\, j_4\, j_5\, j_6)$. Длина цикла равна 5, поэтому четность не изменилась.

Перемещение вниз фишки j_3 в ситуации

j_1	j_2	j_3	j_4
j_7	j_6		j_5

переводит перестановку $j_1, j_2, j_3, j_4, j_5, j_6, j_7$ в $j_1, j_2, j_4, j_5, j_3, j_6, j_7$, что эквивалентно циклу $(j_3\, j_4\, j_5)$. Длина цикла равна 3, поэтому четность не изменилась.

Перемещение вниз фишки j_4 в ситуации

j_1	j_2	j_3	j_4
j_7	j_6	j_5	

не меняет соответствующей перестановки.

4.5. Кольцо

Понятия кольца и поля являются обобщениями понятий числового кольца и числового поля. Неформально говоря, кольцом называют некоторое множество, в котором можно складывать, вычитать и умножать, причем эти операции в целом обладают теми же свойствами, что и свойства обычных операций сложения, вычитания и умножения чисел.

Дадим строгое определение. *Кольцом* называется непустое множество K, на котором заданы две бинарные алгебраические операции, называемые сложением (обозначается «+») и умножением (обозначается «$\cdot$» или «$\times$», знак умножения может опускаться), причем относительно сложения K является абелевой группой (*аддитивная группа кольца*) и операции связаны законами *дистрибутивности*, т. е. для любых a, b, c из K

1) $(a+b)c = ac + bc$;

2) $a(b+c) = ab + ac$.

Из дистрибутивности следует обобщенная дистрибутивность.

Утверждение 4.44 (Обобщенная дистрибутивность)**.** *Пусть $a, b_1, b_2, \ldots, b_n$ — элементы кольца K. Тогда*

1) $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$;

2) $(b_1 + b_2 + \ldots + b_n)a = b_1a + b_2a + \ldots + b_na$.

Доказательство. Обе формулы доказываются индукцией по n. ∎

Нейтральный элемент в аддитивной группе кольца называется нулем и обозначается 0. Симметричный элемент к элементу a называется противоположным и обозначается $-a$.

Если операция умножения в кольце ассоциативная, то кольцо называется *ассоциативным*[5], если операция умножения коммутативная, то кольцо называется *коммутативным*. Если операция умножения обладает нейтральным элементом, то он называется *единицей* кольца и обычно обозначается 1 или e.

Пусть K — кольцо и $K' \subseteq K$, причем K' само является кольцом относительно тех же операций сложения и умножения. Тогда K' называется *подкольцом* кольца K. Любое кольцо K обладает по крайней мере двумя подкольцами: самим K и *нулевым* подкольцом $\{0\}$.

Пример 4.45. Примеры колец:

1) Числовые кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с обычными операциями сложения и умножения, причем $\mathbb{Z}$ — подкольцо в $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; кольцо $\mathbb{Q}$ является подкольцом в $\mathbb{R}$, $\mathbb{C}$; а $\mathbb{R}$ — подкольцом в $\mathbb{C}$. Все эти кольца ассоциативные и коммутативные с единицей. Кольца $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ являются полями (см. ниже). Множество $\mathbb{N}$ кольцом не является.

2) Кольцо $n\mathbb{Z}$ целых чисел, кратных заданному числу n, относительно обычных операций сложения и умножения. Кольцо $n\mathbb{Z}$ является подкольцом в $\mathbb{Z}$. Оно ассоциативное и коммутативное, при $n \geq 2$ — без единицы.

3) Кольцо $\mathbb{Z}_n$ вычетов по модулю n. Кольцо вычетов коммутативно и ассоциативно, обладает единицей.

4) Кольцо $\mathbf{V}_3$ геометрических векторов пространства с операциями сложения и векторного умножения. Это кольцо не ассоциативно и не коммутативно.

[5] Иногда ассоциативность умножения включают в определение кольца.

Выведем некоторые простейшие свойства колец.

Утверждение 4.46. *Пусть a, b, c — элементы кольца K и $a + b = a + c$, тогда $b = c$.*

Доказательство. Если $a + b = a + c$, то $(-a) + (a + b) = (-a) + (a + c)$, откуда, пользуясь ассоциативностью, $((-a) + a) + b = ((-a) + a) + c$, т. е. $b = c$. ∎

Утверждение 4.47. *Для любых элементов a, b кольца K уравнение $a+x = b$ имеет, причем единственное, решение $x = b + (-a)$.*

Доказательство. Вначале проверим, что $b + (-a)$ является решением уравнения $a + x = b$. Действительно,

$$a + (b + (-a)) = (a + (-a)) + b = 0 + b = b.$$

Теперь докажем, что других решений нет. Предположим, что x и x' — два решений уравнения $a + x = b$, тогда

$$a + x = a + x'.$$

Из утверждения 4.46 теперь следует, что $x = x'$. ∎

В кольце вводится операция *вычитания* по правилу

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

Утверждение 4.48 (Мультипликативные свойства нуля)**.** *Для любых элементов a, b, c кольца K верно $a0 = 0a = 0$.*

Доказательство. Имеем $aa + a0 = a(a + 0) = aa$, откуда из утверждения 4.47 получаем, что $a0 = aa - aa = 0$. Аналогично показывается, что $0a = 0$. ∎

Утверждение 4.49 («Правило знаков» при умножении)**.** *Для любых элементов a, b, c кольца K верно $(-a)b = a(-b) = -(ab)$; $(-a)(-b) = ab$.*

Доказательство. Докажем, например, что $(-a)b = -(ab)$. Остальные свойства доказываются аналогично. Имеем $ab + (-a)b = (a - a)b = 0b = 0$, т. е. $(-a)b$ противоположен элементу ab. ∎

Утверждение 4.50 (Дистрибутивность при вычитании)**.** *Для любых элементов a, b, c кольца K верно $(a - b)c = ac - bc$; $a(b - c) = ab - ac$.*

Доказательство. Имеем $(a - b)c = (a + (-b))c = ac + (-b)c = ac + (-bc) = ac - bc$. Второе равенство доказывается аналогично. ∎

Если в кольце K нашлись неравные нулю элементы a, b (возможно, $a = b$), такие, что $ab = 0$, то a называется *левым делителем нуля*, а b — *правым делителем нуля*. Если некоторый элемент является как левым, так и правым делителем нуля, то он называется просто *делителем нуля*. Очевидно, что в коммутативном кольце левый делителей нуля является также правым делителем нуля, и наоборот.

Пример 4.51. В кольце $\mathbb{Z}_4$ делителем нуля является $\overline{2}$, так как $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$. В кольце $\mathbb{Z}_6$ делителями нуля являются $\overline{2}$, $\overline{3}$, так как $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

Утверждение 4.52 (Лемма о сокращении)**.** *Пусть кольцо K не содержит делителей нуля. Если a, b, c — элементы кольца K, причем $a \neq 0$, то из каждого условия: $ab = ac$ и $ba = ca$ следует $b = c$.*

Доказательство. Если $ab = ac$, то $a(b - c) = 0$. Так как в кольце K нет делителей нуля и $a \neq 0$, то $b - c = 0$, откуда $b = c$. Если $ba = ca$, то рассуждения аналогичны. ∎

Введем операцию умножения элементов кольца на целые числа[6]. Пусть $a \in K$, а $n \in \mathbb{N}$, тогда под произведением $n \cdot a$ будем понимать $\underbrace{a + a + \ldots + a}_{n}$. Произведение $(-n) \cdot a$ означает $n \cdot (-a)$, а $0 \cdot a$ равно $0 \in K$.

Если K содержит единицу 1, то $n \cdot 1$ кратко будем записывать просто n. Таким образом, в частности, мы еще раз обосновали целесообразность записывать элементы $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ кольца $\mathbb{Z}_n$ как $0, 1, \ldots, n - 1$ соответственно.

4.6. Поле

Неформально говоря, полем называют некоторое множество, в котором можно складывать, вычитать, умножать и делить (деление на ноль запрещено), причем эти операции в целом обладают теми же свойствами, что и свойства обычных операций сложения, вычитания, умножения и деления чисел.

Дадим строгое определение. Кольцо F называется *полем*, если множество его ненулевых элементов, $F \setminus \{0\}$, непусто и образует абелеву группу. Эта группа называется *мультипликативной группой поля*. Из определения следует, что любое поле содержит по крайней мере 2 элемента: 0 и 1.

Если F — поле и $F' \subseteq F$, причем F' само является полем относительно тех же операций сложения и умножения, тогда F' называется *подполем* поля F.

Пример 4.53. Числовые кольца $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с обычными операциями сложения и умножения являются полями. Кольцо $\mathbb{Z}$ полем не является.

Упражнение 4.54. Какие из следующих множеств образуют кольцо, а какие поле:
1) множество $\{0\}$;
2) множество $\mathbb{N}$ натуральных чисел;
3) множество целых неотрицательных чисел;
4) множество целых неположительных чисел;
5) множество $\mathbb{Z}$ целых чисел;
6) множество $2\mathbb{Z}$ четных чисел;
7) множество $n\mathbb{Z}$ целых чисел, кратных заданному числу $n \neq 0$;
8) множество $\mathbb{Q}$ рациональных чисел;
9) множество иррациональных чисел;
10) множество $\mathbb{R}$ вещественных чисел;
11) множество $\mathbb{C}$ комплексных чисел;
12) множество $\mathbb{Z}[i]$ *целых гауссовых чисел*, т. е. комплексных чисел с целыми действительной и мнимой частями;
13) множество комплексных чисел с рациональными действительной и мнимой частями?

Упражнение 4.55. Какие из следующих множеств образуют кольцо, а какие поле:
1) множество чисел вида $a + b\sqrt{2}$, где a, b — целые;
2) множество чисел $a + b\sqrt{2}$, где a, b — рациональные;
3) множество чисел $a + b\sqrt[3]{2}$, где a, b — целые;

[6] В точности также определяется операция умножения элементов аддитивной группы на целые числа.

4) множество чисел $a + b\sqrt[3]{2}$, где a, b — рациональные;
5) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — целые;
6) множество чисел $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где a, b, c — рациональные?

Утверждение 4.56. *Поле не имеет делителей нуля.*

Доказательство. Пусть поле F обладает делителями нуля, т. е. $ab = 0$ для некоторого $a \neq 0$ и некоторого $b \neq 0$. Таким образом, $F \setminus \{0\}$ не замкнуто относительно операции умножения, следовательно, не образует группу, т. е. F полем не является. ∎

Теорема 4.57. *Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Доказательство. Необходимость. Пусть $\mathbb{Z}_n$ — поле. Покажем, что n — простое. Предположим противное. Значит найдутся a, b, такие, что $2 \leq a \leq n-1$, $2 \leq b \leq n-1$, $ab = n$, откуда $ab \equiv 0 \pmod{n}$, т. е. $\overline{a}\,\overline{b} = \overline{0}$. Итак, $\overline{a}$, $\overline{b}$ являются делителями нуля. Следовательно, по утверждению 4.56, $\mathbb{Z}_n$ полем не является.
Достаточность. Пусть n — простое число. Для того, чтобы доказать, что $\mathbb{Z}_n$ образует поле достаточно показать, что для любого $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ существует обратный. Не нарушая общности, можно считать, что $1 \leq a \leq n-1$. Тогда, так как n — простое, НОД $\{a, n\} = 1$. Поэтому найдутся целые u и v, такие, что

$$ua + vn = 1,$$

откуда

$$ua \equiv 1 \pmod{n},$$

т. е. $\overline{u}\,\overline{a} = \overline{1}$, поэтому $\overline{a} = \overline{u}^{-1}$. ∎

Пример 4.58. $\mathbb{Z}_2$ — наименьшее (по количеству элементов) поле. Оно состоит из элементов $\overline{0}$ (четные числа) и $\overline{1}$ (нечетные числа). То же самое поле (точнее, изоморфное — см. ниже раздел 4.7) из двух элементов 0, 1 — с булевыми операциями: «исключающее или» (сложение по модулю 2) и конъюнкция.

Упражнение 4.59. Является ли полем $\{0, 1\}$ относительно операций дизъюнкции (рассматриваемой в качестве сложения) и конъюнкции (рассматриваемой в качестве умножения).

Упражнение 4.60. Найти обратный к элементу 1) $\overline{24}$ в поле $\mathbb{Z}_{89}$; 2) $\overline{103}$ в поле $\mathbb{Z}_{691}$; 3) $\overline{35}$ в поле $\mathbb{Z}_{151}$.

Упражнение 4.61. Доказать, что для элемента $\overline{a}$ кольца $\mathbb{Z}_n$ обратный существует тогда и только тогда, когда НОД $\{a, n\} = 1$.

Упражнение 4.62. Существует ли в кольце $\mathbb{Z}_{1003}$ 1) обратный к $\overline{231}$; 2) обратный к $\overline{289}$? Если да, то найти его.

Итак, у нас есть метод построения полей из p элементов, где p — произвольное простое число. Приведем пример поля из 4 элементов.

Пример 4.63. Построим поле из 4 элементов. Поле должно содержать 0 и 1. Два других элемента обозначим a и b. Операции сложения и умножения зададим таблицами:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Теперь можно проверить, что все необходимые свойства операций выполнены.

4.7. Изоморфизм

Рассмотрим мультипликативную группу $U_4 = \{\pm 1, \pm i\}$ всех значений корня 4-й степени из 1 и аддитивную группу $\mathbb{Z}_4$ вычетов по модулю 4. Приведем таблицы их операций.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	$-i$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Мы видим, что эти группы отличаются только обозначениями: таблица сложения для группы $\mathbb{Z}_4$ получается из таблицы умножения для группы U_4 заменой 1, i, -1, $-i$ соответственно на $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ и заменой знака умножения на знак сложения. Это означает, что группы *изоморфны*. Дадим строгое определение.

Пусть G — группа с операцией $\circ$, а G' — группа с операцией $*$. Взаимно однозначное соответствие $\varphi: G \to G'$ называется *изоморфизмом*, если для любых a и b из G

$$\varphi(a \circ b) = \varphi(a) * \varphi(b), \tag{4.10}$$

т. е. результату операции с элементами группы G соответствует результат операции с образами этих элементов. Свойство (4.10), выполненное для всех элементов a и b из G, называется свойством *сохранения операции*.

Если между группами G и G' существует изоморфизм, то группы называются *изоморфными*.

Изоморфизм из G на G (изоморфизм на себя) называется *автоморфизмом*.

Пример 4.64. Обобщая пример с изоморфизмом групп U_4 и $\mathbb{Z}_4$, докажем, что для любого n изоморфны мультипликативная группа U_n и аддитивная группа $\mathbb{Z}_n$. Действительно, положим

$$\varphi(\omega^k) = \overline{k}, \quad \text{где} \quad \omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}, \quad k = 0, 1, \ldots, n-1.$$

В частности, $\varphi(1) = \overline{0}$, $\varphi(\omega) = \overline{1}$ и т. д. Имеем $U_4 = \{\omega^0,\ \omega^1,\ \ldots,\ \omega^{n-1}\}$. Очевидно, что φ — биекция. Проверим свойство (4.10):

$$\varphi(\omega^k \cdot \omega^\ell) = \varphi(\omega^{k+\ell}) = \varphi(\omega^{(k+\ell) \bmod n}) = \overline{(k+\ell) \bmod n} = \overline{k} + \overline{\ell} = \varphi(\omega^k) + \varphi(\omega^\ell).$$

Аналогично понятию изоморфизма групп вводится понятие изоморфизма колец и изоморфизма полей, но свойство сохранения нужно потребовать от обеих операций: сложения и умножения. Пусть K — кольцо (в частности, поле) с операцией сложения $+$ и операцией умножения $\cdot$, а K' — кольцо (в частности, поле) с операцией сложения $\oplus$ и операцией умножения $\odot$. Взаимно однозначное соответствие $\varphi: K \to K'$ называется *изоморфизмом*, если для любых a и b из K

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b), \qquad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b).$$

Если между кольцами (полями) K и K' существует изоморфизм, то они называются *изоморфными*.

Упражнение 4.65. Доказать, что кольца $\mathbb{Z}$ и $n\mathbb{Z}$ при $n \geq 2$ не изоморфны.

Упражнение 4.66. Доказать, что
1) поля $\mathbb{Q}$ и $\mathbb{R}$ не изоморфны;
2) поля $\mathbb{R}$ и $\mathbb{C}$ не изоморфны.

Упражнение 4.67.* Доказать, что
1) при любом изоморфизме числовых полей подполе $\mathbb{Q}$ отображается тождественно, следовательно, поле $\mathbb{Q}$ обладает только тождественным автоморфизмом;
2) поле $\mathbb{R}$ обладает только тождественным автоморфизмом.

Упражнение 4.68. Найти все автоморфизмы поля $\mathbb{C}$, переводящие действительные числа снова в действительные.

Упражнение 4.69. Изоморфны ли поля $\left\{a+b\sqrt{2}:\ a,b\in\mathbb{Q}\right\}$ и $\left\{a+b\sqrt{3}:\ a,b\in\mathbb{Q}\right\}$?

Ответы и решения

4.1. $(a\circ b)\circ c$, $a\circ(b\circ c)$; $((a\circ b)\circ c)\circ d$, $(a\circ(b\circ c))\circ d$, $(a\circ b)\circ(c\circ d)$, $a\circ(b\circ(c\circ d))$, $a\circ((b\circ c)\circ d)$.
4.8. НОД и НОК являются бинарными (коммутативными и ассоциативными) алгебраическими операциями на $\mathbb{N}$. Нейтрального элемента у НОД нет. У НОК есть нейтральный элемент 1. Симметричный элемент относительно операции НОК есть только у 1.
4.14. Всего 9 подполугрупп: $\{\varepsilon\}$, $\{b\}$, $\{c\}$, $\{\varepsilon,a\}$, $\{\varepsilon,b\}$, $\{\varepsilon,c\}$, $\{b,c\}$, $\{\varepsilon,b,c\}$, $\{\varepsilon,a,b,c\}$.
4.15. В обоих случаях является.
4.21. 1) Полугруппа, но не группа; 2) полугруппа, но не группа; 3) полугруппа, но не группа; 4) группа; 5) группа; 6) группа; 7) группа; 8) не является полугруппой; 9) группа; 10) группа.
4.22. 1) Полугруппа, но не группа; 2) полугруппа, но не группа; 3) не является полугруппой; 4) полугруппа, но не группа; 5) полугруппа, но не группа; 6) полугруппа, но не группа; 7) группа; 8) группа; 9) не является полугруппой; 10) полугруппа, но не группа; 11) группа; 12) группа; 13) полугруппа, но не группа; 14) группа; 15) группа; 16) группа; 17) группа; 18) группа.
4.23. *Указание:* Вначале показать, что для конечности необходимо, чтобы $|x|\in\{0,1\}$ для каждого элемента x группы.
4.25. Так как $(ab)^2=e$, то $ab=(ab)^{-1}=b^{-1}a^{-1}=ba$.
4.35. Например, $(1\,5)$, $(2\,5)$, $(5\,4)$. Число транспозиций нечетно.
4.36. 1) Инверсии образуют пары $(3,2)$, $(5,2)$, $(5,4)$, $(7,2)$, $(7,4)$, $(7,6)$, $(8,6)$, $(9,6)$. Всего 8 инверсий. Перестановка четная.
2) Инверсии образуют пары $(2,1)$, $(5,4)$, $(5,3)$, $(4,3)$, $(7,6)$, $(7,3)$, $(6,3)$, $(8,3)$, $(9,3)$. Всего 9 инверсий. Перестановка нечетная.
4.37. 1) $\dfrac{n(n-1)}{2}$;
2) $\dfrac{n(n-1)}{2}$;
3) $\dfrac{n(n+1)}{2}$.
4.38. $\dfrac{n(n-1)}{2}-k$.
4.39. 1) $\begin{pmatrix}1&2&3&4&5\\1&2&4&5&3\end{pmatrix}$; 2) $\begin{pmatrix}1&2&3&4&5\\5&3&4&2&1\end{pmatrix}$.
4.40. 1) $(1\ 3)(2\ 4\ 5)$; 2) $(1\ 3)(2\ 4)(5)$; 3) $(1\ 4\ 2\ 5\ 3)$; 4) $(1\ 2\ 3\ 4\ 5)$.
4.41. $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&2&3&4&5&7&8&6&9&10\end{pmatrix}$. *Указание:* Предварительно разложить в произведение независимых циклов.
4.54. 1) Кольцо, но не поле.
2) Не является кольцом.
3) Не является кольцом.
4) Не является кольцом.
5) Кольцо, но не поле.

6) Кольцо, но не поле.
7) Кольцо, но не поле.
8) Поле.
9) Не является кольцом.
10) Поле.
11) Поле.
12) Кольцо, но не поле.
13) Поле.

4.55. 1) Кольцо, но не поле.
2) Поле.
3) Не является кольцом.
4) Не является кольцом.
5) Кольцо, но не поле.
6) Поле. *Указание:* Если $\sqrt[3]{4} = a + b\sqrt[3]{2}$, то, домножая обе части на $\sqrt[3]{2}$, получаем $2 = a\sqrt[3]{2} + b(a + b\sqrt[3]{2})$. Из полученного равенства выразить $\sqrt[3]{2}$.

4.59. Не является, так как относительно дизъюнкции не является группой (к 1 нет симметричного элемента).

4.60.
1) Для чисел 24, 89 находим коэффициенты Безу. Ими являются числа -7, 26. Имеем $1 = 26\cdot 24 + (-7)\cdot 89$, откуда $26 \cdot 24 \equiv 1 \pmod{89}$, т. е. $\overline{24}^{-1} = \overline{26}$ в $\mathbb{Z}_{89}$.
2) Для чисел 103, 691 находим коэффициенты Безу. Имеем $1 = (-161)\cdot 103 + 24\cdot 691$, откуда $(-161)\cdot 103 \equiv 1 \pmod{691}$, т. е. $\overline{103}^{-1} = \overline{-161} = \overline{530}$ в $\mathbb{Z}_{691}$.
3) $\overline{82}$.

4.61. Пусть для $\overline{a}$ существует обратный $\overline{b}$. Тогда $ab \equiv 1 \pmod{n}$, что эквивалентно $ab + kn = 1$ для некоторого целого k, откуда НОД $\{a, n\} = 1$. Обратно, если НОД $\{a, n\} = 1$, то существуют $ua + vn = 1$ для некоторых u, v, откуда $ua \equiv 1 \pmod{n}$, поэтому $\overline{a}^{-1} = u$.

4.62. Обратим внимание, что $1003 = 17 \cdot 59$ — число составное, поэтому кольцо $\mathbb{Z}_{1003}$ полем не является. Тем не менее, согласно предыдущему упражнению, к некоторым элементам этого кольца (а именно, взаимно простым с 1003) обратный элемент существует.
1) Так как 231 и 1003 взаимно простые, то обратный существует. Имеем $1 = 165\cdot 231 + (-38)\cdot 1003$, откуда $165 \cdot 231 \equiv 1 \pmod{1003}$, т. е. $\overline{231}^{-1} = \overline{165}$ в $\mathbb{Z}_{1003}$.
2) Обратного нет, так как числа 289 и 1003 взаимно простыми не являются: НОД $\{289, 1003\} = 17$.

4.67. 1) Пусть φ — автоморфизм $\mathbb{Q} \to \mathbb{Q}$. Имеем $\varphi 0 = 0$, $\varphi 1 = 1$, поэтому $\varphi 2 = \varphi(1 + 1) = \varphi 1 + \varphi 1 = 1 + 1 = 2$, $\varphi 3 = \varphi(2+1) = \varphi 2 + \varphi 1 = 2 + 1 = 3$, ... Следовательно, все целые неотрицательные числа отображаются тождественно. Далее, если a — целое неотрицательное, то $\varphi(-a) = -\varphi a$. Следовательно, все целые числа отображаются тождественно. Если p, q — целые и $q \neq 0$, то $\varphi\left(\dfrac{p}{q}\right) = \dfrac{\varphi p}{\varphi q} = \dfrac{p}{q}$. Таким оразом, $\mathbb{Q}$ отображается тождественно.
2) Пусть φ — автоморфизм $\mathbb{R} \to \mathbb{R}$. Сперва докажем, что положительные числа переводятся в положительные. Действительно, пусть $a > 0$. Тогда найдется такое b, что $a = b^2$. Имеем $\varphi a = \varphi b^2 = (\varphi b)^2 > 0$. Теперь выводим, что если $a < b$, то $\varphi a < \varphi b$, так как $\varphi b - \varphi a = \varphi(b - a) > 0$. Теперь докажем от противного, что все вещественные числа отображаются тождественно. Пусть $a \in \mathbb{R}$, $\varphi a = b \neq a$. Рассмотрим случай $\varphi a < b$. Найдется рациональное c, такое, что $a < c < b$. Тогда $c < b = \varphi a < \varphi c = c$. Противоречие. Аналогичные рассуждения, если $\varphi a > b$.

4.68. Два автоморфизма: тождественный и переводящий каждое число в сопряженное. *Решение:* Легко проверить, что указанные отображения — автоморфизмы. Пусть φ — автоморфизм $\mathbb{C} \to \mathbb{C}$. Так как $i^2 = -1$, то $\varphi(i^2) = (\varphi i)^2 = \varphi(-1) = -1$. Следовательно, $\varphi i = i$ или $\varphi i = -i$ и других автоморфизмов, кроме указанных выше нет.

4.69. Не изоморфны.