А. В. Овчинников

ТЕОРИЯ ГРУПП
Лекционный курс

МОСКВА

2016

Оглавление

ЛЕКЦИЯ 1

Алгебраические системы

АЛГЕБРА — это раздел математики, в котором изучаются свойства операций над элементами множеств произвольной природы; эти операции представляют собой обобщения обычных операций сложения и умножения чисел.

Каждое множество может быть снабжено некоторыми отношениями и операциями; например, на множестве вещественных чисел имеется отношение строгого порядка $<$, отношение равенства $=$, операции сложения $+$ и умножения $\cdot$ чисел и т. д. Множества с введёнными на них дополнительными математическими структурами называют *алгебраическими системами*. В этой лекции кратко представлены простейшие и в то же время наиболее важные типы алгебраических систем.

1. Операции на множестве

A. Основные определения.

1.1. В математике под алгебраической *операцией* понимается отображение, которое одному или нескольким элементам множества (аргументам) ставит в соответствие другой элемент (значение). Операции классифицируются по присущим им специфическим свойствам и по количеству аргументов (арности).

1.2. Определение. Пусть A, B, C — тройка непустых множеств. *Бинарной операцией* f на паре множеств A и B со значениями в C называется отображение $f\colon A \times B \to C$, которое ставит в соответствие упорядоченной паре $(a, b) \in A \times B$ некоторый элемент множества C. Если $A = B = C$, то бинарная операция называется *внутренней*, в противном случае — *внешней*. Для обозначения значения операции f на упорядоченной паре $(a, b) \in A \times B$ вместо записи $f(a, b)$ используется, как правило, *инфиксная* запись с помощью специальных знаков операций, например, $a + b$ для сложения чисел; эта форма записи подразумевает, что знак операции вставляется *между* элементами, к которым применяется эта операция. Отметим, что бинарная операция $f\colon A \times B \to C$ может быть определена не для всех упорядоченных пар $(a, b) \in A \times B$.

1.3. Простейшими примерами внутренних бинарных операций являются операции сложения и умножения на множествах вещественных чисел или числовых функций, операция сложения векторов (направленных отрезков), а примерами внешних операций — операция умножения направленного отрезка на число или скалярного произведения направленных отрезков.

1.4. Определение. *Унарная операция* на множестве A — это отображение $f\colon A \to A$.

1.5. Примерами унарных операций могут служить операции перехода от множества к его дополнению, изменение знака числа, преобразование подобия в геометрии, логическое отрицание.

1.6. Определение. *Тернарная операция* — это операция с тремя аргументами, т.е. отображение $f\colon A \times B \times C \to D$; чаще всего рассматриваются *внутренние* тернарные операции, т.е. отображения $f\colon A\times A\times A \to A$. Тернарная операция, не являющаяся внутренней, называется *внешней*. Примером (внешней) тернарной операции может служить смешанное произведение векторов.

Б. Атрибуты унарных операций. Каждая операция обладает определёнными свойствами (атрибутами), характеризующими её и определяющими взаимоотношения этой операции с другими отображениями рассматриваемого множества.

1.7. Определение. Унарная операция $\lozenge$ на множестве A называется *инволютивной* (*инволюцией*), если

$$\forall a \in A: \quad \lozenge\,(\lozenge\, a) = a.$$

1.8. ***Примеры*** инволютивных операций: изменение знака вещественного числа, комплексное сопряжение, дополнение подмножества в множестве, отрицание высказывания, осевая и центральная симметрии в геометрии и т. д.

1.9. Определение. Унарная операция $\lozenge$ на множестве A называется *идемпотентной*, если

$$\forall a \in A: \quad \lozenge\,(\lozenge\, a) = \lozenge\, a.$$

1.10. ***Примеры*** идемпотентных операций: взятие модуля числа, операция проектирования в геометрии.

В. Атрибуты бинарных операций.

1.11. Употребительны две основные формы записи бинарных операций:

(а) *мультипликативная*: операцию в этом случае называют *умножением*, результат операции — *произведением* (обозначение ab или $a \cdot b$); выражения вида aa, aaa и т.п. называют *степенями* элемента a и записывают в виде a^2, a^3, ...;
(б) *аддитивная*: операцию называют сложением, результат операции — суммой (обозначение $a + b$); выражения вида $a + a$, $a + a + a$, $-a - a$ и т.п. называют *кратным* и элемента и записывают в виде $2a$, $3a$, $-2a$.

1.12. Определение. Внутренняя бинарная операция $*\colon A \times A \to A$ на множестве A называется *коммутативной*, если

$$a * b = b * a$$

для всех $a, b \in A$.

1.13. Примеры.

1. Сложение и умножение вещественных чисел коммутативны: $a + b = b + a$, $a \cdot b = b \cdot a$ для всех $a, b \in \mathbb{R}$.
2. Логические операции конъюнкция и дизъюнкция на множестве высказываний коммутативны: $A \wedge B \equiv B \wedge A$, $A \vee B \equiv B \vee A$.
3. Объединение, пересечение и симметрическая разность множеств коммутативны: $A \cup B = B \cup A$, $A \cap B = B \cap A$, $A \triangle B = B \triangle A$.
4. Вычитание, деление и возведение в степень вещественных чисел коммутативными не являются: $a - b \neq b - a$, $\dfrac{a}{b} \neq \dfrac{b}{a}$, $a^b \neq b^a$.
5. Некоммутативной является операция умножения матриц: вообще говоря, $AB \neq BA$ даже для квадратных матриц.

1.14. Определение. Внутренняя бинарная операция $*\colon A \times A \to A$ на множестве A называется *ассоциативной*, если

$$(a * b) * c = a * (b * c)$$

для всех $a, b, c \in A$.

1.15. Примеры.

1. Сложение и умножение вещественных чисел ассоциативны: $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всех $a, b, c \in \mathbb{R}$.
2. Логические операции конъюнкция и дизъюнкция на множестве высказываний ассоциативны: $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$, $(A \vee B) \vee C \equiv A \vee (B \vee C)$.
3. Операции объединения и пересечения множеств ассоциативны: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$.
4. Операция композиции отображений ассоциативна: для произвольных отображений $f\colon X \to Y$, $g\colon y \to Z$, $h\colon Z \to W$ имеем $(h \circ g) \circ f = h \circ (g \circ f)$.
5. Операция вычитания вещественных чисел не является ассоциативной: $(a - b) - c \neq a - (b - c)$.

1.16. Свойства ассоциативности и коммутативности бинарной операции независимы. Так, примеры операций, одновременно ассоциативных и коммутативных, читателю хорошо известны. Операция $*$ на $\mathbb{Z}$, заданная правилом $n*m \stackrel{\text{def}}{=\!=} -n-m$, очевидно, коммутативна, но ассоциативной не является:

$$(1*2)*3 = (-1-2)*3 = -(-1-2)-3 = 0,$$
$$1*(2*3) = -1-(2*3) = -1-(-2-3) = 4.$$

Примером ассоциативной, но не коммутативной операции может служить композиция отображений.

1.17. Пусть A — множество с заданной на нём бинарной операцией. Будем использовать мультипликативную форму записи. Можно различными способами составлять различные произведения, состоящие из n сомножителей, не меняя их порядка:

(1) при $n = 2$ такое произведение лишь одно: a_1a_2;
(2) при $n = 3$ имеется два произведения: $(a_1a_2)a_3$ и $a_1(a_2a_3)$;
(3) при $n = 4$ таких произведений уже пять: $((a_1a_2)a_3)a_4$, $(a_1(a_2a_3))a_4$, $a_1((a_2a_3)a_4)$, $a_1(a_2(a_3a_4))$, $(a_1a_2)(a_3a_4)$.

Докажем, что в случае ассоциативной операции все эти произведения совпадают.

1.18. Предложение. *Если бинарная операция на множестве A ассоциативна, то результат её применения к n элементам множества не зависит от расстановки скобок.*

Доказательство. При $n = 1$ и $n = 2$ доказывать нечего, при $n = 3$ утверждение теоремы совпадает с определением ассоциативности. Применим индукцию по n. Предположим, что утверждение доказано для числа перемножаемых элементов $<n$ и докажем его для n сомножителей, т.е. проверим, что

$$(a_1 \dots a_k)(a_{k+1} \dots a_n) = (a_1 \dots a_l)(a_{l+1} \dots a_n)$$

для любых k и l, $1 \leqslant k, l \leqslant n-1$. Мы выписали в последнем равенстве лишь внешние пары скобок, поскольку по предположению индукции расстановка внутренних скобок несущественна. Назовём расстановку скобок

$$\Big(\dots \big((a_1a_2)a_3\big) \dots a_{k-1}\Big)a_k$$

левонормированной. Если $k = n-1$, то произведение n сомножителей приводится к левонормированному виду:

$$(a_1 \dots a_{n-1})a_n = \Big(\dots \big((a_1a_2)a_3\big) \dots a_{n-1}\Big)a_n.$$

В случае $k < n-1$ ввиду ассоциативности имеем

$$(a_1 \dots a_k)(a_{k+1} \dots a_n) = (a_1 \dots a_k)\big((a_{k+1} \dots a_{n-1})a_n\big) =$$
$$= \Big((a_1 \dots a_k)(a_{k+1} \dots a_{n-1})\Big)a_n =$$
$$= \Big(\dots\Big(\big(\dots(a_1a_2)\dots a_k\big)a_{k+1}\Big)\dots a_{n-1}\Big)a_n,$$

т.е. снова получили левонормированную расстановку скобок. К такому же виду приводится правая часть доказываемого равенства. □

1.19. Определение. Пусть $\circ$ и $*$ — две бинарные операции, заданные на множестве A. Операция $*$ называется *дистрибутивной* относительно операции $\circ$, если

$$(a \circ b) * c = a * c \circ b * c, \quad c * (a \circ b) = c * a \circ c * b$$

для всех $a, b, c \in A$.

В случае некоммутативной операции нужно различать дистрибутивность справа (первое из приведённых соотношений) и слева (второе соотношение); если же операция коммутативна, то понятия дистрибутивности слева и справа совпадают.

1.20. Примеры.

1. Умножение вещественных чисел дистрибутивно относительно сложения: $(a+b)c = ac+bc$, $c(a+b) = ca+ca$ для всех $a, b, c \in \mathbb{R}$.
2. Конъюнкция и дизъюнкция взаимно дистрибутивны:
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$
3. Объединение и пересечение множеств взаимно дистрибутивны:
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C),$$
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$
4. Сложение вещественных чисел не является дистрибутивным относительно умножения: $(a \cdot b) + c \neq (a + c) \cdot (b + c)$.

Г. Нейтральные и симметричные элементы.

1.21. Определение. Пусть $*$ — бинарная операция на множестве A. Элемент $e \in A$ называется *нейтральным* относительно операции $*$, если

$$\forall a \in A: \quad e * a = a * e = a.$$

1.22. В случае некоммутативной операции $*$ различают левый нейтральный элемент e_L, определяемый соотношением $e_L * a = a$, и правый нейтральный элемент e_R, определяемый соотношением $a * e_R = a$. Впрочем, даже в случае некоммутативной операции

левый и правый нейтральные элементы могут совпадать. Например, единичная матрица является двусторонним (т.е. одновременно левым и правым) нейтральным элементом относительно некоммутативной операции умножения матриц. Понятия левого и правого нейтральных элементов нам в дальнейшем не понадобятся.

1.23. Примеры.

1. Нуль 0 является нейтральным элементом относительно сложения чисел, а единица 1 — нейтральным элементом относительно умножения.
2. Ложное высказывание 0 является нейтральным элементом относительно дизъюнкции, а истинное высказывание 1 — нейтральным элементом относительно конъюнкции: $A \vee 0 = A$, $A \wedge 1 = A$.
3. Пустое множество является нейтральным элементом относительно операции объединения множеств, а универсальное множество — нейтральным элементом относительно операции пересечения: $A \cup \varnothing = A$, $A \cap U = A$.

1.24. Предложение. *Если нейтральный элемент относительно бинарной операции $*$ существует, то он единствен.*

Доказательство. Пусть e и e' — нейтральные элементы относительно операции $*$. Тогда $e' = e' * e = e$, т.е. $e' = e$. □

1.25. Определение. Пусть $*$ — бинарная операция на множестве A, обладающая нейтральным элементом e. Элемент a' называется *симметричным* к элементу $a \in A$ относительно операции $*$, если $a' * a = e = a * a'$. В этом случае элемент a называется *симметризуемым*, а элементы a и a' — *взаимно симметричными*.

1.26. Очевидно, нейтральный элемент является симметричным самому себе.

1.27. В случае некоммутативной операции различают левый симметричный элемент u, определяемый соотношением $u * a = e$, и правый симметричный элемент v, определяемый соотношением $a * v = e$. Нам эти понятия не понадобятся.

1.28. Примеры.

1. Относительно сложения вещественных чисел симметричным к числу $a \in \mathbb{R}$ является противоположное число $-a$.
2. Относительно умножения вещественных чисел симметричным к ненулевому числу $a \in \mathbb{R}$ является число $1/a$; число нуль не имеет симметричного относительно операции умножения.

1.29. Предложение. *Пусть $*$ — ассоциативная операция, a и b — симметризуемые элементы, a' и b' — их симметричные.*

1. *Элемент a' единствен.*
2. *Элемент $a * b$ симметризуем; его симметричным является $b' * a'$.*
3. *Элемент, симметричный к a', также симметризуем, причём $(a')' = a$.*

Доказательство. 1. Пусть u и v — два элемента, симметричных к a относительно операции $*$, т.е.

$$a * u = e = u * a, \quad a * v = e = v * a.$$

В силу ассоциативности операции $*$ имеем

$$u = u * e = u * (a * v) = (u * a) * v = e * v = v.$$

2. В силу ассоциативности $*$ имеем

$$(a*b)*(b'*a') = \big((a*b)*b'\big)*a' = \big(a*(b*b')\big)*a' = (a*e)*a' = a*a' = e.$$

Аналогично доказывается, что $(b' * a') * (a * b) = e$.

3. Пользуясь предыдущем фактом, получаем

$$(a')' * a' = (a * a')' = e' = e. \qquad \square$$

1.30. При использовании мультипликативной формы записи нейтральный элемент называют обычно *единицей* (обозначения $e, \varepsilon, 1$), а симметричный элемент — *обратным*. При использовании аддитивной формы записи нейтральный элемент называют *нулём* (обозначение 0), а симметричный элемент — *противоположным*.

Д. Множество, замкнутое относительно операции. Пусть $*$ — бинарная операция на множестве A, обладающая нейтральным элементом e.

1.31. Определение. Пусть $*$ — бинарная операция на множестве A. Подмножество $B \subset A$ называется *замкнутым* относительно $*$, если

$$\forall a, b \in B: \quad a * b \in B.$$

Аналогично вводится понятие подмножества, замкнутого относительно унарной или тернарной операции.

1.32. Примеры.

1. Подмножество в $\mathbb{Z}$, состоящее из всех чётных чисел, замкнуто относительно операций сложения и умножения целых чисел.
2. Подмножество в $\mathbb{Z}$, состоящее из всех нечётных чисел, замкнуто относительно операции умножения целых чисел, но не замкнуто относительно операции сложения.
3. Относительно унарной операции изменения знака числа подмножество в $\mathbb{R}$, состоящее из целых чисел, замкнуто, а подмножество, состоящее из положительных чисел, — нет.

2. Алгебраические системы и их отображения

1.33. Определение. *Алгебраической системой* $\mathcal{A}$ будем называть непустое множество X, на котором заданы одна или несколько алгебраических операций; будем писать $\mathcal{A} = (X, *)$ и т.п.

Это не самое общее определение алгебраической системы, но оно вполне пригодно для наших целей.

1.34. Простейшей алгебраической системой является множество без каких бы то ни было операций и отношений; эту систему естественно назвать вырожденной.

Читателю хорошо знаком пример алгебраической системы, представляющей собой множество вещественных чисел $\mathbb{R}$ с определёнными на нём операциями сложения $+$ и умножения $\cdot$ чисел (кроме того, в этой алгебраической системе имеется отношение порядка $<$).

Нас будут интересовать алгебраические системы, обладающие одной или двумя операциями.

1.35. Определение. Пусть $\mathcal{A} = (X, \circ, \dots, *)$ и $\mathcal{A}' = (X, \bullet, \dots, \star)$ — две алгебраические системы с одинаковым количеством операций. Отображение $f : X \to X'$ называется *гомоморфизмом* этих систем, если оно *сохраняет операции*, т.е.

$$\forall x, y \in X \quad f(x \circ y) = f(x) \bullet f(y), \quad \dots, \quad f(x * y) = f(x) \star f(y).$$

1.36. Определение. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Алгебраические системы, между которыми существует изоморфизм, называют *изоморфными* и пишут $\mathcal{A} \simeq \mathcal{A}'$.

1.37. В алгебре мы интересуемся только теми свойствами алгебраических систем, которые выражаются в терминах операций, заданных на этих системах. Две изоморфные алгебраические системы являются «одинаково устроенными» в том смысле, что любое утверждение, сформулированное только в терминах операций, справедливо в одной из этих систем тогда и только тогда, когда оно справедливо в другой. Поэтому безразлично, какую из изоморфных друг другу алгебраических систем изучать: все они являются различными реализациями (моделями) одного и того же абстрактного объекта. Однако различные модели одной и той же алгебраической системы могут обладать специфическими свойствами, облегчающими их исследование; например, при изучении модели геометрического происхождения можно использовать геометрические методы и т. п.

1.38. Пример. Рассмотрим множество $\mathbb{R}$ всех вещественных чисел с определённой на нём операцией сложения и множество $\mathbb{R}_+$

положительных вещественных чисел с заданной на нём операцией умножения. Любое отображение $x \mapsto a^x$, где $a > 0$, является изоморфизмом.

1.39. Очевидно, каждая алгебраическая система $\mathcal{A}(X, \circ)$ изоморфна сама себе: изоморфизмом может служить тождественное отображение $\mathrm{id} : X \to X$, $x \mapsto x$.

1.40. Определение. Изоморфизм алгебраической системы на себя называется *автоморфизмом*.

3. Группы

А. Определение и простейшие свойства групп.

1.41. Определение. *Группой* $(G, *)$ называется алгебраическая система с одной бинарной операцией $* : G \times G \to G$, обладающей следующими свойствами:

Г1. операция $*$ ассоциативна:

$$\forall x, y, z \in G \quad x * (y * z) = (x * y) * z;$$

Г2. операция $*$ обладает нейтральным элементом e:

$$\exists e \in G \; \forall x \in G \quad x * e = e * x = x;$$

Г3. все элементы множества G обратимы относительно операции $*$:

$$\forall x \in G \; \exists x' \in G \quad x * x' = x' * x = e.$$

Группа называется *абелевой*, если операция в ней коммутативна, т.е.

$$\forall x, y \in G \quad x * y = y * x.$$

1.42. Группа G, содержащая конечное число элементов, называется *конечной*, а число её элементов называется *порядком* и обозначается $|G|$. В противном случае группа называется *бесконечной*.

1.43. Предложение. *Пусть $(G, *)$ — группа с единицей e. Справедливы следующие утверждения*:

(i) *единица e группы единственна*;
(ii) *для каждого элемента $a \in G$ его обратный единствен*;
(iii) *для любых элементов $x, y, z \in G$ из равенств $x * z = y * z$ и $z * x = z * y$ вытекает равенство $x = y$ (законы сокращения справа и слева)*;
(iv) *для любых $x, y \in G$ элемент $x * y \in G$ обратим*; *его обратным является $y^{-1} * x^{-1}$*;
(v) *элемент, обратный к x^{-1}, обратим, причём $(x^{-1})^{-1} = x$.*

Доказательство. Все утверждения, кроме (iii), были доказаны выше (см. предложения 1.24 и 1.29). Для доказательства (iii) нужно умножить равенство $x * z = y * z$ на z^{-1} справа (а $z * x = z * y$ — слева). □

1.44. Для конечной группы можно построить «таблицу умножения»:

	e	x_1	$\cdots$	x_j	$\cdots$	x_n
e	e	x_1		x_j		x_n
x_1	x_1	x_1^2		$x_1 * x_j$		$x_1 * x_n$
$\vdots$						
x_i	x_i	$x_i * x_1$		$x_i * x_j$		$x_i * x_n$
$\vdots$						
x_n	x_n	$x_n * x_1$		$x_n * x_j$		x_n^2

Левый сомножитель произведения берётся из заголовочного столбца, а правый — из заголовочной строки этой таблицы, называемой *таблицей Кэли*. Отметим, что таблица Кэли абелевой группы симметрична относительно главной диагонали.

1.45. Предложение (ослабление аксиом)**.** *Пусть G — множество с заданной на нём ассоциативной операцией $*$, обладающее следующими свойствами:*

(i) *существует такой элемент $e \in G$, что для любого $x \in G$ выполняется $e * x = x$ (левая единица);*

(ii) *для любого $x \in G$ существует такой элемент $x' \in G$, что $x' * x = e$ (левый обратный элемент).*

Тогда $(G, *)$ — группа.

Доказательство. Требуется доказать, что из требований (i) и (ii) данного определения вытекают аксиомы группы **Г2** и **Г3**, т.е. что левая единица является одновременно и правой, а левый обратный элемент — и правым обратным.

Сначала докажем, что если $x * x = x$, то $x = e$. Для любого (в том числе и этого) x существует левый обратный x', т.е. $x' * x = e$. Тогда $x' * (x * x) = x' * x = e$. С другой стороны, $x' * (x * x) = (x' * x) * x = e * x = x$. Следовательно, $x = e$.

Покажем, что если $x' * x = e$, то и $x * x' = e$. Пользуясь свойством ассоциативности, имеем:

$$(x * x') * (x * x') = x * \big((x' * x) * x'\big) = x * (e * x') = x * x',$$

так что по доказанному выше $x * x' = e$. Таким образом, левый обратный является одновременной и правым обратным.

Покажем, что для любого $x \in G$ имеем $x * e = x$, т.е. e является правой единицей. Пусть x' — обратный элемент для x; имеем $x' * x = x * x' = e$. Тогда

$$x * e = x * (x' * x) = (x * x') * x = e * x = x. \qquad \square$$

Б. Понятие подгруппы.

1.46. Определение. Непустое подмножество $S \subset G$ группы $(G, *)$ называется *подгруппой* в G, если оно замкнуто относительно умножения в группе G и взятия обратного элемента, т.е. если выполняются следующие условия:

(i) если $x, y \in S$, то $x * y \in S$;
(ii) если $x \in S$, то $x^{-1} \in S$.

Тот факт, что S является подгруппой в G, обозначается $S \leqslant G$; запись $H \subset G$ используется в случае, когда H — *подмножество* в G (не обязательно являющееся подгруппой).

1.47. Поскольку для любого $x \in S$ имеем $x * x^{-1} = e$, то $e \in S$. Очевидно, $\{e\}$ и G — подгруппы группы G; эти подгруппы называют *тривиальными*. Если S — нетривиальная подгруппа в G, будем писать $S < G$.

1.48. Очевидно, любая подгруппа S группы G сама является группой относительно той же операции.

В. Гомоморфизмы и изоморфизмы. Пусть $(G, *)$ и $(\mathcal{G}, \circ)$ — две группы с нейтральными элементами e и ε соответственно.

1.49. Определение. Отображение $f : G \to \mathcal{G}$ называется *гомоморфизмом*, если

$$\forall x, y \in G \quad f(x * y) = f(x) \circ f(y).$$

Взаимно однозначный гомоморфизм называется *изоморфизмом*. Две группы G и $\mathcal{G}$ называют *изоморфными* (запись $G \simeq \mathcal{G}$), если существует хотя бы один изоморфизм $f : G \to \mathcal{G}$.

1.50. Предложение. *Если $f\colon G \to \mathcal{G}$ — гомоморфизм, то*

(i) $f(e) = \varepsilon$;
(ii) $f(x^{-1}) = [f(x)]^{-1}$ *для любого* $x \in G$.

Доказательство. (i) Пусть $\xi = f(e)$; тогда

$$f(e) = f(e * e) = f(e) \circ f(e) \;\Rightarrow\; \xi = \xi \circ \xi \;\Rightarrow\; \xi \circ \varepsilon = \xi \circ \xi$$

и в силу закона сокращения (см. п. (iii) предложения 1.43) получаем $\xi = \varepsilon$.

(ii) Для любого $x \in G$ имеем:

$$\varepsilon = f(e) = f(x * x^{-1}) = f(x) \circ f(x^{-1}) \;\Rightarrow\; f(x^{-1}) = [f(x)]^{-1}. \quad \square$$

1.51. Изоморфные группы имеют одни и те же свойства, выражаемые в терминах групповой операции, и потому неразличимы с алгебраической точки зрения; в связи с этим для изоморфных групп G и $\mathcal{G}$ часто пишут $G = \mathcal{G}$ вместо $G \simeq \mathcal{G}$.

Г. Примеры.

1.52. ***Тривиальная группа.*** Множество, состоящее из единственного элемента e и снабжённое операцией $*$, действующей по правилу $e * e = e$, является группой; элемент e является нейтральным, порядок этой группы равен 1.

1.53. ***Группа*** $\mathbb{Z}_2$**.** Множество $\{1, -1\}$ является абелевой группой относительно операции умножения; эта группа обозначается $\mathbb{Z}_2$; $|\mathbb{Z}_2| = 2$. Таблица Кэли группы $\mathbb{Z}_2$ имеет вид

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

. (1.1)

1.54. ***Аддитивная группа*** $(\mathbb{R}, +)$**.** Множество вещественных чисел с операцией сложения является абелевой группой $(\mathbb{R}, +)$ и называется *аддитивной группой* $\mathbb{R}$. Нейтральным элементом является нуль, а противоположным к числу $a \in \mathbb{R}$ — число $(-a) \in \mathbb{R}$. Аналогично определяются аддитивные группы элементов числовых полей $\mathbb{Q}$ и $\mathbb{C}$. Эти группы бесконечны.

1.55. ***Мультипликативная группа*** $(\mathbb{R}^*, \cdot)$**.** Множество ненулевых вещественных чисел с операцией умножения является абелевой группой $(\mathbb{R} \setminus \{0\}, \cdot)$ и называется *мультипликативной группой обратимых элементов* $\mathbb{R}^*$. Нейтральным элементом является единица, а обратным к числу $a \in \mathbb{R} \setminus \{0\}$ — число $a^{-1} \in \mathbb{R}_+$. Аналогично определяются мультипликативные группы $\mathbb{Q}^*$ и $\mathbb{C}^*$ ненулевых элементов числовых полей $\mathbb{Q}$ и $\mathbb{C}$.

1.56. Группа $(\mathbb{R}_+, \cdot)$ положительных вещественных чисел с операцией умножения является подгруппой мультипликативной группы $\mathbb{R}^*$.

1.57. Группы $(\mathbb{R}, +)$ и $(\mathbb{R}_+, \cdot)$ изоморфны; изоморфизмом является любое отображение вида $f : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto c^x$, где $c > 0$ — произвольное число. Действительно,

$$\forall a, b \in \mathbb{R} \quad f(a + b) = c^{a+b} = c^a \cdot c^b = f(a) \cdot f(b).$$

1.58. ***Группа целых чисел*** $(\mathbb{Z}, +)$ ***с операцией сложения.*** Нейтральным элементом является нуль, а обратным к числу $a \in \mathbb{Z}$ — число $(-a) \in \mathbb{Z}$. Очевидно, эта группа абелева. Обратите внимание, что множество целых чисел с рассматриваемой на нём операцией умножения группой не является, несмотря на ассоциативность умножения и наличие нейтрального элемента (единицы): обратимыми элементами относительно операции умножения являются лишь ± 1.

1.59. Множество $2\mathbb{Z}$ чётных целых чисел образует подгруппу группы $\mathbb{Z}$ из предыдущего примера. Множество нечётных целых чисел подгруппой не является (почему?).

1.60. В аддитивной группе $\mathbb{C}$ имеется следующая цепочка подгрупп: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

1.61. В мультипликативной группе $\mathbb{C}^*$ имеется следующая цепочка подгрупп: $\mathbb{Z}_2 \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.

1.62. ***Векторные пространства.*** Любое векторное пространство можно рассматривать как абелеву группу с операцией сложения векторов; нейтральным элементом этой группы является нулевой вектор.

1.63. ***Полная линейная группа*** $GL(n)$**.** Множество всех невырожденных квадратных $(n \times n)$-матриц над числовым полем $\mathbb{K}$ является группой относительно операции умножения матриц; эта группа называется полной линейной группой и обозначается $GL(n, \mathbb{K})$ (или $GL(n)$):

$$GL(n, \mathbb{K}) \stackrel{\text{def}}{=\!=} \Big\{ A \in \mathbb{K}^{n \times n} \;\Big|\; \det A \neq 0 \Big\}.$$

Обратимость каждого элемента $A \in CL(n)$ обеспечивается невырожденностью.

1.64. ***Специальная линейная группа*** $SL(n)$**.** Множество всех квадратных $(n \times n)$-матриц с определителем, равным 1, также является группой относительно операции умножения матриц; эта группа называется специальной линейной группой и обозначается $SL(n, \mathbb{K})$ (или $SL(n)$):

$$SL(n, \mathbb{K}) \stackrel{\text{def}}{=\!=} \Big\{ A \in \mathbb{K}^{n \times n} \;\Big|\; \det A = 1 \Big\}.$$

Ясно, что $SL(n, \mathbb{K})$ — подгруппа группы $GL(n, \mathbb{K})$.

4. Кольца и поля

В этом разделе мы сформулируем определения кольца и поля — алгебраических систем с двумя операциями.

A. Определение кольца.

1.65. Определение. *Кольцом* называется непустое множество R с двумя заданными на нём бинарными операциями $+$ (сложение) и $\cdot$ (умножение), которые обладают следующими свойствами:

K1: относительно сложения $+$ множество R образует абелеву группу, называемую *аддитивной группой кольца*; нейтральный элемент этой группы называется *нулём* и обозначается 0;

K2: умножение $\cdot$ дистрибутивно относительно сложения: для любых $a, b, c \in R$ имеют место соотношения

$$(a+b)\cdot c = a\cdot c + b\cdot c, c\cdot(a+b) = c\cdot a + c\cdot b.$$

Если операция умножения коммутативна (ассоциативна), то кольцо называется *коммутативным* (*ассоциативным*); отметим, что некоммутативные и неассоциативные кольца встречаются весьма часто. Если операция умножения обладает нейтральным элементом, то он называется *единицей* кольца, а само кольцо — *унитальным* (или *кольцом с единицей*).

Выведем некоторые следствия аксиом кольца, не являющиеся следствиями аксиом аддитивной абелевой группы.

1.66. Предложение.

1. *Для любого* $a \in R$ *имеем* $a\cdot 0 = 0\cdot a = 0$.
2. *Для любых* $a, \beta \in R$ *имеем* $a\cdot(-b) = (-a)\cdot b = -(ab)$.
3. *Для любых* $a, b, c \in R$ *имеем* $a\cdot(b-c) = a\cdot b - a\cdot c$, $(a-b)\cdot c = a\cdot c - b\cdot c$.
4. *Если кольцо с единицей* 1 *содержит более одного элемента, то* $1 \neq 0$.
5. *В кольце с единицей, содержащем более одного элемента, нулевой элемент необратим относительно умножения, т.е. делить на нуль невозможно.*
6. *Все обратимые элементы кольца с единицей* R *образуют группу* R^* *относительно операции умножения. Эта группа называется мультипликативной группой кольца.*

Доказательство. 1. Пусть $a\cdot 0 = b$. Тогда

$$b + b = a\cdot 0 + a\cdot 0 = a\cdot(0+0) = a\cdot 0 = b,$$

откуда $b = b - b = 0$. Равенство $0\cdot a = 0$ доказывается аналогично.

2. Имеем

$$ab + a(-b) = a(b+(-b)) = a\cdot 0 = 0 \quad \Rightarrow \quad a(-b) = -(ab)$$

и аналогично для $(-a)b$.

3. Имеем

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

и аналогично для $(a-b)c$.

4. Предположим, что $1=0$. Тогда для любого $a\in R$ имеем

$$a=a\cdot 1=a\cdot 0=0,$$

т.е. кольцо состоит из одного нуля, противоречие.

5. Предположив, что a — элемент, обратный к 0, т.е. $0\cdot a=1$, получаем противоречие с п. 1. (Отметим, что в кольце, состоящем из единственного элемента $0=1$, нулевой элемент обратим относительно умножения, причем $0^{-1}=0$.)

6. Единица кольца, будучи обратимой, принадлежит множеству R^*. Поскольку

$$a\in R^* \quad\Rightarrow\quad a^{-1}\in R^*$$

и умножение в R^* ассоциативно, остаётся лишь убедиться, что множество R^* замкнуто относительно умножения. Действительно, если $a,b\in R^*$, то $a^{-1},b^{-1}\in R^*$ и $(ab)^{-1}=b^{-1}a^{-1}$, т.е. элемент ab обратим и потому принадлежит R^*. □

1.67. Свойство, обратное к утверждению 1.66.1, вообще говоря, не имеет места: может случиться так, что произведение ненулевых элементов a, b кольца равно нулю; такие элементы называют *делителями нуля* (a — левым, b — правым).

1.68. Предложение. *В кольце R без делителей нуля имеет место закон сокращения: если $ac=bc$ (или $ca=cb$) и $c\neq 0$, то $a=b$.*

Доказательство. $ac=bc\Rightarrow(a-b)c=0\Rightarrow a-b=0\Rightarrow a=b$. □

1.69. Определение. Непустое подмножество $S\subset R$ кольца R называется *подкольцом* в R, если оно замкнуто относительно операций сложения, вычитания (т.е. операции, обратной к сложению) и умножения:

(1) $x+y\in S$ для любых $x,y\in S$;
(2) $-x\in S$ для любого $x\in S$;
(3) $x\cdot y\in S$ для любых $x,y\in S$.

Б. Примеры колец.

1.70. Множество $\mathbb{Z}$ целых чисел с операциями сложения и умножения является коммутативным ассоциативным кольцом с единицей $(\mathbb{Z},+,\cdot)$.

1.71. Цепочка подгрупп аддитивной группы $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$ (см. пример 1.60) является одновременно и цепочкой подколец.

1.72. Множество $2\mathbb{Z}$ чётных чисел с операциями сложения и умножения является коммутативным ассоциативным кольцом без единицы $(2\mathbb{Z},+,\cdot)$.

1.73. Множество всех числовых функций, определённых на некотором подмножестве числовой прямой, является коммутативным ассоциативным кольцом с единицей относительно обычных операций сложения и умножения функций. Это кольцо обладает делителями нуля; например, произведение функций

$$f(x) = \begin{cases} 0, & x < 0, \\ 1, & x \geqslant 0, \end{cases} \qquad g(x) = \begin{cases} 1, & x < 0, \\ 0, & x \geqslant 0, \end{cases}$$

тождественно равно нулю.

1.74. Множество многочленов от переменной x с вещественными коэффициентами является коммутативным и ассоциативным кольцом с единицей относительно операций сложения и умножения многочленов; это кольцо обозначается $\mathbb{R}[x]$. Это кольцо не имеет делителей нуля, т.е. произведение ненулевых многочленов является ненулевым многочленом.

1.75. Множества $\mathbb{R}^{n\times n}$, $\mathbb{C}^{n\times n}$ всех вещественных и комплексных квадратных матриц фиксированного размера являются ассоциативными, но не коммутативными кольцами с единицей, роль которой выполняет единичная матрица. Эти кольца обладают делителями нуля.

1.76. Множество геометрических векторов с введёнными на нём операциями сложения и векторного умножения векторов является некоммутативным неассоциативным кольцом. Векторное произведение $[\boldsymbol{a}, \boldsymbol{b}]$ вместо коммутативности обладает свойством $[\boldsymbol{a}, \boldsymbol{b}] = -[\boldsymbol{b}, \boldsymbol{a}]$, которое естественно назвать *антикоммутативностью*, а вместо ассоциативности — свойством

$$[\boldsymbol{a}, [\boldsymbol{b}, \boldsymbol{c}]] + [\boldsymbol{b}, [\boldsymbol{c}, \boldsymbol{a}]] + [\boldsymbol{c}, [\boldsymbol{a}, \boldsymbol{b}]] = \boldsymbol{0};$$

это тождество называется *тождеством Якоби*. Кольца, обладающие указанными двумя свойствами, называются *кольцами Ли*.

1.77. Множество $\mathcal{P}(A)$ всех подмножеств данного множества A, снабжённое операцией симметрической разности в качестве сложения и операцией пересечения в качестве умножения является коммутативным ассоциативным кольцом с единицей:

$$X + Y \stackrel{\text{def}}{=\!=} X \triangle Y = (X \cup Y) \setminus (X \cap Y) = (X \setminus Y) \cup (Y \setminus X),$$
$$X \cdot Y \stackrel{\text{def}}{=\!=} X \cap Y.$$

Нулевым элементом является пустое множество: $0 = \varnothing$, единичным — всё множество: $1 = A$. Все элементы кольца обладают свойством идемпотентности: $X \cdot X = X$. Каждый элемент является

обратным к самому себе относительно сложения: $X + X = 0$. Очевидно, это кольцо обладает делителями нуля; таковыми являются любые два непересекающиеся подмножества множества A.

B. Определение и примеры полей.

1.78. Определение. *Полем* называется коммутативное ассоциативное кольцо с единицей, в котором любой ненулевой элемент обратим.

Кольцо, состоящее из одного нулевого элемента (в котором $1 = 0$), полем не считается.

1.79. Множества рациональных чисел $\mathbb{Q}$ и вещественных чисел $\mathbb{R}$ являются примерами полей, хорошо знакомых читателю из школьного курса.

1.80. Кольцо $\mathbb{Z}$ целых чисел полем не является, поскольку в нём обратимы только ± 1.

1.81. Менее тривиальным примером поля является множество $\mathbb{Q}[\sqrt{2}] \stackrel{\text{def}}{=\!=} \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ (проверьте самостоятельно!).

1.82. Множество рациональных функций, т.е. функций вида $f(x) = P(x)/Q(x)$, где $P(x)$ и $Q(x)$ — многочлены от переменной x, также является полем относительно обычных операций сложения и умножения функций.

1.83. Предложение. *В любом поле*

$$ab = 0 \quad \Rightarrow \quad (a = 0) \vee (b = 0).$$

Доказательство. Если $a \neq 0$, то, умножив обе части равенства $ab = 0$ на a^{-1}, получим $b = 0$. □

1.84. Определение. Подмножество $\mathbb{L} \subset \mathbb{K}$ поля $\mathbb{K}$ называется *подполем* в $\mathbb{K}$, если оно замкнуто относительно операций сложения, вычитания (т.е. операции, обратной к сложению), умножения и деления (т.е. операции, обратной к умножению); очевидно, $\mathbb{L}$ при этом само является полем. Поле $\mathbb{K}$ при этом называется *расширением* поля $\mathbb{L}$.

1.85. Пример. Поле вещественных чисел $\mathbb{R}$ является расширением поля рациональных чисел $\mathbb{Q}$, а само является подполем поля комплексных чисел $\mathbb{C}$.

Г. Кольца вычетов. Важные примеры колец, состоящих из конечного числа элементов, доставляют кольца вычетов.

1.86. Два целых числа x и y называются *сравнимыми по натуральному модулю* m (обозначение $x \equiv y \pmod m$), если разность $x-y$ делится на m. Очевидно, $x \equiv y \pmod m$ тогда и только тогда, когда числа x и y при делении на m дают одинаковый остаток.

1.87. Предложение. *Отношение* $\equiv \pmod m$ *сравнимости целых чисел по модулю является отношением эквивалентности.*

Доказательство. Рефлексивность: очевидно, $x \equiv x \pmod m$, поскольку $x - x = 0$ делится на m.

Симметричность: $x \equiv y \pmod m$ означает, что $x - y$ делится на m, а потому и $y - x = -(x-y)$ делится на m, т.е. $y \equiv x \pmod m$.

Транзитивность: соотношения $x \equiv y \pmod m$ и $y \equiv z \pmod m$ означают, что числа $x - y$ и $y - z$ делятся на m; но тогда $x - z = (x-y) + (y-z)$ также делится на m, т.е. $x \equiv z \pmod m$. □

1.88. Таким образом, множество $\mathbb{Z}$ всех целых чисел разбивается на классы эквивалентности по отношению сравнимости: одному классу принадлежат все целые числа, имеющие одинаковый остаток при делении на m. Так как при делении целых чисел на m возможные остатки суть $0, 1, \ldots, m-1$ (всего имеется m различных остатков), существует ровно m классов эквивалентности по отношению $\equiv \pmod m$; они называются *классами вычетов* по модулю m.

1.89. Соответствующее фактор-множество (т.е. множество, элементами которого являются указанные классы эквивалентности) состоит из m элементов (классов вычетов) и обозначается $\mathbb{Z}_m$:

$$\begin{aligned}
[0]_m &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod m\} = \{0 + mk,\ k \in \mathbb{Z}\},\\
[1]_m &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod m\} = \{1 + mk,\ k \in \mathbb{Z}\}, \quad \ldots,\\
[m-1]_m &= \{x \in \mathbb{Z} \mid x \equiv m-1 \pmod m\} = \{(m-1) + mk,\ k \in \mathbb{Z}\}.
\end{aligned}$$

(Если модуль сравнения m зафиксирован и в процессе рассуждений не меняется, то для краткости можно писать $[a]$ вместо $[a]_m$, что мы и будем делать в дальнейшем изложении.)

1.90. Отметим, что каждый класс эквивалентности может быть обозначен многими разными способами, например, классы эквивалентности по модулю 2 суть

$$\begin{aligned}
[0]_2 = [2]_2 = [4]_2 = [-2]_2 = [-4]_2 = \ldots,\\
[1]_2 = [3]_2 = [5]_2 = [-1]_2 = [-3]_2 = \ldots,
\end{aligned}$$

а по модулю 3 —

$$[0]_3 = [3]_3 = [6]_3 = [-3]_3 = [-6]_3 = \dots,$$
$$[1]_3 = [4]_3 = [7]_3 = [-2]_3 = [-5]_3 = \dots,$$
$$[2]_3 = [5]_3 = [8]_3 = [-1]_3 = [-4]_3 = \dots.$$

1.91. Любая совокупность чисел, взятых по одному из каждого класса, называется *полной системой вычетов по модулю* m. Например, полными системами вычетов по модулю m являются

$$0,\ 1,\ \dots,\ m-1 \qquad \text{и} \qquad 1,\ 2,\ \dots,\ m;$$

в случае нечётного модуля, $m = 2k+1$, полной системой вычетов является, например,

$$-k,\ -k+1,\ \dots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \dots,\ k.$$

1.92. Предложение. *Пусть* $x \equiv x' \pmod m$ *и* $y \equiv y' \pmod m$. *Тогда*

$$x + y \equiv x' + y' \pmod m, \quad xy \equiv x'y' \pmod m.$$

Доказательство. Записи $x \equiv x' \pmod m$ и $y \equiv y' \pmod m$ означают, что

$$x \equiv x' \pmod m \ \Leftrightarrow\ x - x' = m\alpha \ \Leftrightarrow\ x' = x + m\alpha,\ \alpha \in \mathbb{Z},$$
$$y \equiv y' \pmod m \ \Leftrightarrow\ y - y' = m\beta \ \Leftrightarrow\ y' = y + m\beta,\ \beta \in \mathbb{Z}.$$

Складывая последние равенства, получим

$$x' + y' = (x + y) + m(\alpha + \beta) \quad \Leftrightarrow \quad x + y \equiv x' + y' \pmod m.$$

Для умножения проверка аналогична:

$$x'y' = \big(x + m\alpha\big)\big(y + m\beta\big) =$$
$$= xy + m\underbrace{\big(x\beta + y\alpha + m\alpha\beta\big)}_{\in\mathbb{Z}} \equiv xy \pmod m. \quad \square$$

1.93. Определим на множестве классов эквивалентности $\mathbb{Z}_m$ операции сложения и умножения элементов следующим образом:

$$[x] + [y] \stackrel{\text{def}}{=\!=} [x + y], \quad [x] \cdot [y] \stackrel{\text{def}}{=\!=} [x \cdot y].$$

Для того чтобы найти, например, сумму классов $[x]$ и $[y]$, нужно в каждом из них произвольно взять по представителю (например, $x \in [x]$ и $y \in [y]$), вычислить сумму (произведение) этих представителей и объявить результатом класс, содержащий результат вычисления. Тот факт, что полученный класс не зависит от выбора представителей, обеспечивается предложением 1.92.

Таким образом, множество $\mathbb{Z}_m$ становится кольцом, называемым *кольцом вычетов по модулю* m.

Такие свойства операций сложения и умножения на множестве $\mathbb{Z}$, как коммутативность, ассоциативность, наличие нейтрального элемента и обратного элемента наследуются операциями на $\mathbb{Z}_m$. Например, если операция сложения на $\mathbb{Z}$, обладающая нейтральным элементом — нулём 0, то класс эквивалентности $[0]$ является нейтральным элементом (нулём) в $\mathbb{Z}_m$; если $(-x)$ — элемент, противоположный элементу $x \in \mathbb{Z}$, то класс $[-x] \in \mathbb{Z}_m$ является элементом, противоположным элементу $[x]$.

1.94. Элементы кольца $\mathbb{Z}_m$ образуют абелеву группу относительно операции сложения, которая называется (аддитивной) *группой* $\mathbb{Z}_m$ *вычетов по модулю* m.

1.95. ***Кольцо*** $\mathbb{Z}_2$**.** Кольцо вычетов по модулю 2 состоит из двух элементов — $[0]$ и $[1]$, первый из которых представляет собой класс всех чисел, делящихся на 2 без остатка, т.е. из чётных чисел, а второй класс $[1]$ состоит из нечётных чисел. Операции сложения и умножения соответствуют естественным представлениям о сумме и произведении чётных и нечётных чисел, например, сумма двух нечётных чисел есть чётное число ($[1] + [1] = [0]$) и т. д. Таблицы сложения и умножения в кольце $\mathbb{Z}_2$ имеют следующий вид:

$$\begin{array}{|c|cc|}\hline + & [0] & [1] \\ \hline [0] & [0] & [1] \\ [1] & [1] & [0] \\ \hline \end{array}, \qquad \begin{array}{|c|cc|}\hline \cdot & [0] & [1] \\ \hline [0] & [0] & [0] \\ [1] & [0] & [1] \\ \hline \end{array}. \tag{1.2}$$

Таблица умножения показывает, что ненулевой элемент $[1]$ кольца $\mathbb{Z}_2$ обратим: $[1]^{-1} = [1]$, так что кольцо $\mathbb{Z}_2$ является полем. Это простейший пример конечного поля.

1.96. ***Кольцо*** $\mathbb{Z}_3$**.** Кольцо вычетов по модулю 3 имеет следующие таблицы сложения и умножения:

$$\begin{array}{|c|ccc|}\hline + & [0] & [1] & [2] \\ \hline [0] & [0] & [1] & [2] \\ [1] & [1] & [2] & [0] \\ [2] & [2] & [0] & [1] \\ \hline \end{array}, \qquad \begin{array}{|c|ccc|}\hline \cdot & [0] & [1] & [2] \\ \hline [0] & [0] & [0] & [0] \\ [1] & [0] & [1] & [2] \\ [2] & [0] & [2] & [1] \\ \hline \end{array}. \tag{1.3}$$

Здесь также ненулевые элементы обратимы:

$$[1]^{-1} = [1], \quad [2]^{-1} = [2],$$

поэтому $\mathbb{Z}_3$ — поле.

1.97. ***Кольцо*** $\mathbb{Z}_4$**.** В кольце вычетов по модулю 4 таблицы сложения и умножения следующие:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

,

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

. (1.4)

В кольце $\mathbb{Z}_4$ имеются делители нуля (см. определение 1.67): $[2]\cdot[2]=[0]$. Это кольцо полем не является.

1.98. Предложение. *Кольцо вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число.*

Доказательство. Если число m — составное, т.е. $m = kl$, где $1 < k, l < m$, то оба класса $[k]_m$ и $[l]_m$ ненулевые, но

$$[k]_m \cdot [l]_m = [kl]_m = [m]_m = [0]_m,$$

т.е. в кольце $\mathbb{Z}_m$ имеются делители нуля, и потому оно не является полем.

Рассмотрим теперь случай, когда число m — простое. Пусть $[a]_m \neq [0]_m$, т.е. число a не делится на m. Попытаемся найти обратный элемент для $[a]_m$ подбором, умножая $[a]_m$ по очереди на все элементы кольца. Получим элементы

$$[0]_m,\ [a]_m,\ [2a]_m,\ \ldots,\ [(m-1)a]_m. \tag{1.5}$$

Докажем, что все эти элементы различны. Действительно, если $[ka]_m = [la]_m$, где $0 \leqslant k < l \leqslant m-1$, то $[(l-k)a]_m = 0$, т.е. число $(l-k)a$ делится на m, что невозможно, поскольку ни $l-k$, ни a не делятся на m. Поэтому в последовательности элементов (1.5) встречаются все элементы кольца $\mathbb{Z}_m$, в том числе $[1]_m$, что означает обратимость элемента $[a]_m$. □

ЛЕКЦИЯ 2

Дальнейшие примеры и свойства групп

1. Циклические группы

А. Определения.

2.1. В произвольной группе G можно определить степени элемента $x \in G$ с целыми показателями:

$$x^n \stackrel{\text{def}}{=\!=} \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n}, & \text{если } n > 0, \\ e, & \text{если } n = 0, \\ \underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n}, & \text{если } n < 0. \end{cases}$$

Элементарно доказываются соотношения $x^m x^n = x^{m+n}$ для любых $m, n \in \mathbb{Z}$ и $(x^n)^{-1} = x^{-n}$.

2.2. Предложение. *Все степени произвольного элемента x группы G образуют подгруппу в G, которая называется* циклической подгруппой, *порождённой элементом x, и обозначается $\langle x \rangle$. Ясно, что группа $\langle x \rangle$ абелева.*

Доказательство. Поскольку $x^0 = e$ и $x^m x^n = x^{m+n}$, остаётся сослаться на предложение 2.12. □

2.3. Определение. Группа G называется циклической, если существует такой элемент $x \in G$, что $G = \langle x \rangle$. Любой такой элемент называется *порождающим элементом* группы G.

2.4. Возможны два принципиально различных случая: либо все степени элемента x различны, либо нет. В первом случае циклическая группа $G = \langle x \rangle$ бесконечна и изоморфна группе $(\mathbb{Z}, +)$; изоморфизм задаётся формулой

$$f\colon \mathbb{Z} \to G, \quad n \mapsto x^n.$$

2.5. Может оказаться, что $x^k = x^l$, где $k > l$; тогда $x^{k-l} = e$. Наименьшее из натуральных чисел m, для которых $x^m = e$, называется *порядком* элемента x и обозначается $\operatorname{ord} x$.

2.6. Предложение. *Пусть* $\operatorname{ord} x = m$.

1. $x^k = e$ *тогда и только тогда, когда* k *делится на* m.
2. $x^k = x^l$ *тогда и только тогда, когда* $k - l$ *делится на* m.
3. *Подгруппа* $\langle x \rangle$ *содержит* m *элементов*: $\bigl|\langle x \rangle\bigr| = \operatorname{ord} x$, *т.е. порядок циклической подгруппы равен порядку порождающего её элемента.*[1]
4. $\operatorname{ord} x^k = \dfrac{m}{(m,k)}$.
5. *Элемент* x^k *циклической группы* $G = \langle x \rangle$ *порядка* m *является порождающим тогда и только тогда, когда* $(m,k) = 1$.

Доказательство. 1. Разделим число k на m с остатком: $k = qm + r$, где $0 \leqslant r < m$. По определению $\operatorname{ord} x$ имеем

$$e = x^k = (x^m)^q \cdot x^r = x^r \;\Leftrightarrow\; r = 0.$$

2. Согласно только что доказанному

$$x^k = x^l \;\Leftrightarrow\; x^{k-l} = e \;\Leftrightarrow\; k - l \text{ делится на } m.$$

3. Действительно, $\langle x \rangle = \{e, x, x^2, \ldots, x^m\}$.

4. Пусть $(m,k) = d$; тогда $m = m_1 d$ и $k = k_1 d$, так что m_1 и k_1 взаимно просты: $(m_1, k_1) = 1$. Выясним, для каких натуральных p выполняется соотношение $(x^k)^p = e$. Имеем:

$(x^k)^p = e \;\Leftrightarrow\; kp$ делится на $m \;\Leftrightarrow\; k_1 p$ делится на $m_1 \;\Leftrightarrow\; p$ делится на m_1.

Следовательно, наименьшее натуральное p, для которого $(x^k)^p = e$, равно $m_1 = m/d$, т.е. $\operatorname{ord} x^k = m/(m,k)$.

5. Это утверждение непосредственно вытекает из предыдущего. □

Б. Примеры циклических групп.

2.7. ***Аддитивная группа*** $(\mathbb{Z}, +)$ является бесконечной циклической группой, $\mathbb{Z} = \langle 1 \rangle$.

2.8. ***Аддитивная группа*** $(\mathbb{Z}_m, +)$ ***вычетов по модулю*** m является конечной циклической группой, $\mathbb{Z}_m = \langle [1] \rangle$.

2.9. ***Мультипликативная группа*** C_m ***корней степени*** m ***из единицы*** состоит из комплексных чисел

$$z_k = \exp \frac{2\pi i k}{m} = \cos \frac{2\pi k}{m} + i \sin \frac{2\pi k}{m}, \quad k = 0, 1, \ldots, m-1.$$

Ясно, что $z_k = z_1^k$. Следовательно, $C_m = \langle z_1 \rangle$.

[1] Обратите внимание, что здесь слово «порядок» используется в двух различных смыслах (ср. определения 1.42 и 2.5).

Порождающие элементы группы C_m называются *первообразными корнями* m-й степени из единицы. Это корни $z_k = \exp \dfrac{2\pi i k}{m}$, где $(m, k) = 1$. Например, первообразные корни 12-й степени из 1 — это z_1, z_5, z_7, z_{11}.

В. Строение циклических групп и их подгрупп.

2.10. Теорема. *Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$. Любая конечная циклическая группа порядка m изоморфна группе $\mathbb{Z}_m$.*

Доказательство. Первое утверждение было доказано в п. 2.4. Пусть $G = \langle x \rangle$ — конечная циклическая группа порядка m. Рассмотрим отображение

$$f\colon \mathbb{Z}_m \to G, \quad [k] \mapsto x^k, \quad k \in \mathbb{Z}.$$

Так как

$$[k] = [l] \;\Leftrightarrow\; k \equiv l \pmod m \;\Leftrightarrow\; x^k = x^l,$$

то отображение f корректно определено и взаимно однозначно. Свойство $f(k + l) = f(k)f(l)$ вытекает из формулы $x^{k+l} = x^k x^l$. Таким образом, f — изоморфизм. □

2.11. Предложение. *Любая подгруппа циклической группы сама является циклической.*

Доказательство. Пусть $G = \langle x \rangle$ — циклическая группа и S — её подгруппа, отличная от e. Ясно, что если $x^{-k} \in S$, $k \in \mathbb{N}$, то $x^k \in S$. Пусть m — наименьшее из натуральных чисел, для которых $x^m \in S$. Докажем, что $S = \langle x^m \rangle$.

Пусть $x^k \in S$. Разделим k на m с остатком: $k = qm + r$, $0 \leqslant r < m$. Тогда

$$x^k = (x^m)^q\, x^r \Rightarrow x^r = x^k (x^m)^{-q} \in S,$$

откуда в силу определения числа m следует, что $r = 0$, так что $x^k = (x^m)^q$. □

2. Подгруппы и смежные классы

А. Подгруппы и их свойства. Докажем некоторые важные свойства подгрупп.

2.12. Предложение. *Подмножество H группы $(G*)$ является подгруппой тогда и только тогда, когда $e \in H$ и для любых $x, y \in H$ выполнено $x * y^{-1} \in H$.*

Доказательство. Достаточность почти очевидна: если $H < G$, то в силу требований (i) и (ii) определения 1.46 для всех $x, y \in H$ имеем $x * y^{-1} \in H$.

Необходимость. Пусть для любых $x, y \in H$ выполнено условие $x * y^{-1} \in H$. Выбрав пару элементов $e, x \in H$, убеждаемся, что $e{*}x^{-1} = x^{-1} \in H$. Поскольку $(y^{-1})^{-1} = y$, то $x{*}y = x{*}(y^{-1})^{-1} \in H$. □

2.13. Предложение. *Если $H_1 < G$ и $H_2 < G$, то $H_1 \cap H_2 < G$ (пересечение подгрупп является подгруппой).*

Доказательство. Так как $e \in H_1$ и $e \in H_2$, то $e \in H_1 \cap H_2$. Далее, рассмотрим произвольные элементы $x, y \in H_1 \cap H_2$:

$$x, y \in H_1 \cap H_2 \Rightarrow \left\{\begin{matrix} x, y \in H_1 \\ x, y \in H_2 \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} xy^{-1} \in H_1 \\ xy^{-1} \in H_2 \end{matrix}\right\} \Rightarrow xy^{-1} \in H_1 \cap H_2,$$

так что согласно предложению 2.12 получаем $H_1 \cap H_2 < G$. □

Б. Классы смежности и теорема Лагранжа. Пусть S — подгруппа в группе G.

2.14. Для каждого элемента $g \in G$ левым классом смежности этого элемента по подгруппе S называется множество

$$Sg \stackrel{\text{def}}{=\!=} \{sg \mid s \in S\},$$

а правым классом смежности — множество

$$gS \stackrel{\text{def}}{=\!=} \{gs \mid s \in S\}.$$

2.15. Предложение. *Если $S \leqslant G$, то $Sx = Sy$ тогда и только тогда, когда $xy^{-1} \in S$. Аналогично, $xS = yS$ тогда и только тогда, когда $y^{-1}x \in S$.*

Доказательство. Если $Sx = Sy$, то $x = ex \in Sx = Sy$, так что существует такой $s \in S$, что $x = sy$, так что $xy^{-1} = s \in S$.

Обратно, пусть $xy^{-1} = s \in S$; тогда $x = sy$. Чтобы доказать, что $Sx = Sy$, проверим, что $Sx \subset Sy$ и $Sy \subset Sx$.

Если $z \in Sx$, то $z = tx$, где $t \in S$, так что $z = tsy \in Sy$ (поскольку $ts \in S$). Обратно, если $w \in Sy$, то $w = t'y$, где $t' \in S$, так что $w = t's^{-1}x \in Sx$ (поскольку $t's^{-1} \in S$). Следовательно, $Sx = Sy$. □

2.16. Предложение. *Если $S \leqslant G$, то любые два левые (правые) класса смежности по S либо совпадают, либо не пересекаются.*

Доказательство. Докажем, что если существует элемент $z \in Sx \cap Sy$, то $Sx = Sy$. Действительно, $sx = z = ty$, где $s, t \in S$. Следовательно, $xy^{-1} = s^{-1}t \in S$, так что согласно предложению 2.15 $Sx = Sy$. □

2.17. Предложение. *Группа G является дизъюнктным*[1] *объединением левых (правых) классов смежности по любой подгруппе $S \leqslant G$.*

Доказательство. Любой элемент x группы лежит в некотором классе смежности, именно, в Sx, а различные классы не имеют общих элементов. □

2.18. Предложение. *Для любой подгруппы $S \leqslant G$ число левых классов смежности по S равно числу левых классов смежности.*

Доказательство. Отображение $f\colon G \to G$, $x \mapsto x^{-1}$, взаимно однозначно. Проверим, что образом каждого левого класса $Sx = \{sx \mid s \in S\}$ будет правый класс:

$$f(Sx) = \{(sx)^{-1} \mid s \in S\} = \{x^{-1}s^{-1} \mid s \in S\} = x^{-1}S.$$

Таким образом, между левыми и правыми классами смежности установлено взаимно однозначное соответствие. □

2.19. Определение. Индексом подгруппы $S \leqslant G$ в группе G называется число классов смежности по этой подгруппе; обозначение $(G : S)$.

2.20. Предложение (теорема Лагранжа)**.** *Порядок конечной группы G делится на порядок любой её подгруппы S и $(G : S) = |G|/|S|$.*

Доказательство. Согласно предложению 2.17 группу G можно представить в виде дизъюнктного объединения классов смежности

$$G = Sx_1 \sqcup Sx_2 \sqcup \cdots \sqcup Sx_k,$$

так что

$$|G| = |Sx_1| + |Sx_2| + \cdots + |Sx_n|.$$

Все смежные классы состоят из одного и того же числа элементов, равного $|S|$, так что $|G| = n|S|$, где $n = (G : S)$. □

2.21. Следствие.

1. *Порядок любой конечной группы делится на порядок любого её элемента.*

[1] Дизъюнктное объединение — это объединение попарно непересекающихся множеств.

2. *Если порядок группы G — простое число, то эта группа является циклической.*
3. *Если $|G| = n$, то $x^n = e$ для любого $x \in G$.*

Доказательство. 1. Поскольку $\operatorname{ord} x = |\langle x\rangle|$ (см. предложение 2.6.3), остаётся применить теорему Лагранжа.

2. Пусть $x \in G$, $x \neq e$. Тогда циклическая подгруппа $\langle x\rangle$ состоит более чем одного элемента (она содержит e и x), а её порядок $|\langle x\rangle| > 1$ является делителем числа $|G|$. Поскольку $|G|$ — простое число, получаем $|\langle x\rangle| = |G|$, так что $\langle x\rangle = G$.

3. Пусть $\operatorname{ord} x = m$; тогда n делится на m (см. утверждение 1), т.е. $n = mq$ и $x^n = (x^m)^q = e^q = e$. □

3. Прямое произведение групп

Пусть $(G, *)$ и $(H, \circ)$ — две группы с нейтральными элементами e и ε соответственно. Определим на декартовом произведении $G\times H$ бинарную операцию $\bullet$ следующим образом:

$$(g_1, h_1) \bullet (g_2, h_2) \stackrel{\text{def}}{=\!=} (g_1 * g_2,\ h_1 \circ h_2).$$

2.22. Предложение. *Множество $G \times H$ является группой относительно бинарной операцией $\bullet$, причём $|G \times H| = |G| \cdot |H|$.*

Доказательство. Ассоциативность операции $\bullet$ проверяется непосредственной, но утомительной выкладкой. Пусть $p_1 = (g_1, h_1)$, $p_2 = (g_2, h_2)$, $p_3 = (g_3, h_3)$ — произвольные элементы группы $G\times H$. Имеем:

$$\begin{aligned}
(p_1 \bullet p_2) \bullet p_3 &= \Big((g_1, h_1) \bullet (g_2, h_2)\Big) \bullet (g_3, h_3) = \\
&= \Big(g_1 * g_2,\ h_1 \circ h_2\Big) \bullet (g_3, h_3) == \Big((g_1 * g_2) * g_3,\ (h_1 \circ h_2) \circ h_3\Big) = \\
&= \Big(g_1 * (g_2 * g_3),\ h_1 \circ (h_2 \circ h_3)\Big) = (g_1, h_1) \bullet \Big(g_2 * g_3,\ h_2 \circ h_3\Big) = \\
&= (g_1, h_1) \bullet \Big((g_2, h_2) \bullet (g_3, h_3)\Big) = p_1 \bullet (p_2 \bullet p_3).
\end{aligned}$$

Очевидно, нейтральным элементом группы $G \times H$ является (e, ε), а обратным элементом к (g, h) — элемент $(g, h)^{-1} \stackrel{\text{def}}{=\!=} (g^{-1}, h^{-1})$. □

2.23. Множества $G\times\{\varepsilon\} = \{(g, \varepsilon) \mid g \in G\}$ и $\{e\}\times H = \{(e, h) \mid h \in H\}$ являются подгруппами в $G \times H$.

4. Симметрические группы

Пусть N — n-множество, т.е. конечное множество мощности n; для удобства положим $N = \{1, 2, \dots, \}$. *Перестановкой* множества N называется взаимно однозначное отображение $\sigma\colon N \to N$ множества N в себя. Перестановку можно задать таблицей значений отображения σ, в явном виде указывая образы всех элементов множества N:

$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}.$$

Если переставить местами столбцы этой таблицы, сохраняя все соответствия $i \mapsto \sigma(i)$, то получим другую запись той же перестановки, например

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 1 & 4 & 2 \\ 2 & 4 & 3 & 1 \end{bmatrix}.$$

Для простоты принято записывать перестановки так, чтобы числа в верхнем ряду таблицы находились в «естественном порядке», т.е. $1, 2, \dots, n$.

Перестановка ε, заданная формулой $\varepsilon(i) = i$ для любого $i \in N$, т.е.

$$\varepsilon = \begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{bmatrix},$$

называется тождественной.

Обозначим символом S_n множество всех перестановок n-множества N.

2.24. Предложение. $|S_n| = n!$.

Доказательство. В процессе построения таблицы значений перестановки $\sigma\colon N \to N$ элемент $\sigma(1)$ может быть выбран n способами, элемент $\sigma(2)$ — $(n-1)$ способами и т. д. Перемножая полученные числа, приходим к результату. □

Так, множество S_1 состоит из единственной перестановки ε, S_2 состоит из $2! = 2$ перестановок:

$$\varepsilon = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$

а множество S_3 — из $3! = 6$ элементов:

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix},$$

$$\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix},\quad \begin{bmatrix}1&2&3\\3&1&2\end{bmatrix},\quad \begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}.$$

Ещё раз подчеркнём что каждый элемент множества S_n является отображением $N \to N$. Введём на S_n бинарную операцию композиции отображений: если $\sigma : N \to N$ и $\tau : N \to N$ — перестановки (элементы множества S_n), то их произведением назовём перестановку $\tau\sigma$ (σ — первый «сомножитель», τ — второй), определённую правилом

$$\forall i \in N \quad (\tau\sigma)(i) = \tau\big(\sigma(i)\big).$$

Например, если

$$\sigma = \begin{bmatrix}1&2&3\\3&1&2\end{bmatrix},\quad \tau = \begin{bmatrix}1&2&3\\2&1&3\end{bmatrix},$$

то

$$\tau\sigma = \begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix} = \begin{bmatrix}1&2&3\\3&1&2\end{bmatrix},$$

$$\sigma\tau = \begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix} = \begin{bmatrix}1&2&3\\2&3&1\end{bmatrix},$$

поскольку

$$\begin{array}{rccc} & 1&2&3 \\ \sigma\colon & \downarrow&\downarrow&\downarrow \\ & 3&2&1 \\ \tau\colon & \downarrow&\downarrow&\downarrow \\ & 3&1&2 \end{array} \qquad\qquad \begin{array}{rccc} & 1&2&3 \\ \tau\colon & \downarrow&\downarrow&\downarrow \\ & 2&1&3 \\ \sigma\colon & \downarrow&\downarrow&\downarrow \\ & 2&3&1 \end{array}$$

Введённая таким образом операция умножения перестановок некоммутативна (это видно из приведённого примера), но, как и любая композиция отображений, обладает свойством ассоциативности. Тождественная перестановка является, очевидно, нейтральным элементом этой операции. Кроме того, нетрудно видеть, что любая перестановка имеет обратную относительно введённой операции: для её построения достаточно поменять местами строки таблицы, задающей перестановку, после чего переставить столбцы местами так, чтобы элементы верхней строки стояли в естественном порядке $1, 2, \ldots, n$. Например,

$$\sigma = \begin{bmatrix}1&2&3&4\\3&1&4&2\end{bmatrix},\quad \sigma^{-1} = \begin{bmatrix}3&1&4&2\\1&2&3&4\end{bmatrix} = \begin{bmatrix}1&2&3&4\\2&4&1&3\end{bmatrix}.$$

Таким образом, множество S_n всех перестановок n-множества, снабжённое операцией композиции (умножения) перестановок, является группой, которая называется *симметрической группой*.

Для записи перестановок часто используется сокращённая форма записи с помощью циклов. Пусть

$$\{i_1, i_2, \dots, i_r\} \subset N = \{1, 2, \dots, n\}.$$

Перестановка $\alpha \in S_n$ называется *циклом* (длины r), если

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \dots, \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1,$$
$$\alpha(i) = i \quad \forall i \in N \setminus \{i_1, i_2, \dots, i_r\},$$

и обозначается $(i_1, i_2, \dots, i_r)$.

Циклы $(i_1, \dots, i_r)$ и $(j_1, \dots, j_s)$ называются *независимыми*, если

$$\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \varnothing;$$

так, циклы $(1, 5, 3)$ и $(2,4)$ независимы, а циклы $(1, 2, 4, 3)$ и $(2, 5)$ — нет (в каждом из них имеется двойка).

Легко доказать, что каждая перестановка может быть представлена в виде совокупности независимых циклов. Приведём несколько примеров:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix} = (1, 2, 3, 4, 5), \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{bmatrix} = (1, 3, 2, 5, 4),$$

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{bmatrix} = (1, 3, 2)(4, 5), \quad \rho = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{bmatrix} = (1, 5)(2, 4, 3),$$

$$\upsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} = (1, 2, 3)(4)(5) = (1, 2, 3).$$

Циклы длины 1 в записи перестановки для краткости опускают (см. последний пример); это не приводит к недоразумениям, если известно, на каком множестве N задана перестановка. Совокупность циклов длины 1 есть не что иное, как тождественная перестановка ε, которую обозначают символом ( ).

Умножение перестановок, записанных в виде совокупности циклов, выполняют, вычисляя последовательно образы каждого элемента $i \in N$:

$$\tau\sigma = (1, 3, 2, 5, 4) \cdot (1, 2, 3, 4, 5) = (1, 5, 3)(2)(4) = (1, 5, 3),$$

поскольку

$$\boxed{1} \xrightarrow{\sigma} 2 \xrightarrow{\tau} \boxed{5} \xrightarrow{\sigma} 1 \xrightarrow{\tau} \boxed{3} \xrightarrow{\sigma} 4 \xrightarrow{\tau} \boxed{1},$$

$$\boxed{2} \xrightarrow{\sigma} 3 \xrightarrow{\tau} \boxed{2}, \qquad \boxed{4} \xrightarrow{\sigma} 5 \xrightarrow{\tau} \boxed{4}.$$

2.25. Пример. Элементы группы S_2 записываются следующим образом:

$$\begin{bmatrix}1 & 2\\ 1 & 2\end{bmatrix} = (\,), \quad \begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix} = (1,2).$$

Вычисляя произведение этих перестановок, легко получить таблицу Кэли группы S_2:

	$(\,)$	$(1,2)$
$(\,)$	$(\,)$	$(1,2)$
$(1,2)$	$(1,2)$	$(\,)$

, (2.1)

сравнив которую с таблицей Кэли (1.1) группы $\mathbb{Z}_2$ (см. с. 15), обнаруживаем, что эти две группы изоморфны:

$$\mathbb{Z}_2 \simeq S_2, \quad 1 \leftrightarrow (\,), \quad -1 \leftrightarrow (1,2).$$

2.26. Пример. Элементы группы S_3 имеют вид

$$\begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix} = (\,), \quad \begin{bmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{bmatrix} = (2,3), \quad \begin{bmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{bmatrix} = (1,2),$$

$$\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{bmatrix} = (1,2,3), \quad \begin{bmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{bmatrix} = (1,3,2), \quad \begin{bmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{bmatrix} = (1,3),$$

а таблица Кэли[1] (проверьте самостоятельно!) —

	$(\,)$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(\,)$	$(\,)$	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	$(\,)$	$(1,3,2)$	$(1,2,3)$	$(2,3)$	$(1,3)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$(\,)$	$(1,3,2)$	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	$(1,3,2)$	$(1,2,3)$	$(\,)$	$(1,3)$	$(1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	$(\,)$
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,2)$	$(1,3)$	$(\,)$	$(1,2,3)$

(2.2)

5. Образующие и соотношения

A. Свободная группа.

[1] Напомним (см. п. 1.44, с. 13), что в соответствии с соглашением о порядке «сомножителей» из заголовочного столбца таблицы берётся левый (т.е. второй!) сомножитель, а из заголовочной строки — правый (первый) сомножитель.