АЛГЕБРА

§1. «Полуаксиоматическая» теория множеств

Все-таки тянет начать, ай, всё, да с нуля.

Точное знание аксиом не является обязательным. Однако обязательной является вера в то, что вся классическая математика следует из всех этих аксиом.

Дж. Бёрджес[1]

Теория множеств строится на системе аксиом, из которых логически выводятся все утверждения этой теории. Часто в качестве стандартной системы аксиом теории множеств используется ZFC (Цермело – Френкеля с аксиомой выбора), хотя существуют и другие, например, NBG (фон Неймана – Бернайса – Гёделя), в которой помимо множеств рассматриваются классы.[2]

Язык: переменные x, y, $\dots$, символы связок $\wedge$, $\Rightarrow$, $\dots$, кванторы $\forall$ и $\exists$, знак равенства $=$, знак принадлежности $\in$, вспомогательные символы: скобки, запятые и т.п. ***Формула*** — неформально говоря, осмысленная конечная последовательность символов языка (например, $x \forall = \in \exists$ — не формула, $\exists x \forall y \, y \notin x$ — формула). Единственный тип объектов — ***множества***, единственное отношение между ними — ***принадлежность***. Мы будем формулировать аксиомы ZFC на естественном языке (как в школьной геометрии), но их можно переписать и в виде формул.

ZF1 (аксиома экстенсиональности) Множество определяется своими элементами, то есть два множества равны тогда и только тогда, когда они имеют одни и те же элементы.

Определим ***подмножество*** x в множестве y ($x \subseteq y$): для любого z из $z \in x$ следует $z \in y$. Тогда $x = y$ равносильно $x \subseteq y$ и $y \subseteq x$. Подмножество x называется ***собственным подмножеством*** ($x \subset y$, $x \subsetneq y$) множества y, если $x \subseteq y$ и $x \neq y$.

ZF2 (аксиома существования пустого множества). Существует множество, называющееся ***пустым***, не содержащее ни одного элемента.[3]

[1] Джон П. Бёрджес. Вынуждение // Справочная книга по математической логике. Ч. II. Теория множеств, с. 100.

[2] См. о ней, например, в Э. Мендельсон. Введение в математическую логику.

[3] Венедикт Ерофеев: «В поваренной книге определение того, что такое гювеч — болгарское национальное кушанье из мяса, риса и овощей, которое может быть без мяса, и без риса, и без овощей».

Теорема 1.1. *Пустое множество единственно (и обозначается $\varnothing$).*

ZF3 (аксиома пары) Для любых двух множеств x и y существует множество $\{x, y\}$, единственными элементами которого являются x и y (***неупорядоченная пара*** элементов x и y).

Синглетон — одноэлементное множество, например, $\{\varnothing\}$.

Упорядоченная пара $(x, y) = \{\{x\}, \{x, y\}\}$. Аналогично можно определить упорядоченную n-ку (***кортеж длины n***).

Теорема 1.2. $(x, y) = (a, b)$ *тогда и только тогда, когда* $x = a$ *и* $y = b$.

ZF4 (аксиома объединения) Для любого множества x существует множество $\bigcup x$ — объединение множеств-элементов x; его элементами являются в точность все элементы элементов множества x.

Теперь определим ***объединение*** $x \cup y$, состоящее из элементов, лежащих в x или y (возможно, одновременно и в x, и в y), то есть равного множеству $\bigcup\{x, y\}$.

ZF5 (аксиома бесконечности) Существует множество, содержащее в качестве элемента $\varnothing$, и вместе с каждым элементом x содержащее и элемент $x \cup \{x\}$.

ZF6 (схема аксиом выделения) Для любого множества x и любого свойства φ существует множество всех y из x, обладающих свойством φ: $\{y \in x \mid \varphi(y)\}$.

Теорема 1.3. (***«парадокс» Рассела***) *Никакое множество не может содержать все множества в качестве элементов.*[4]

Теперь можно определить ***пересечение*** $x \cap y$, состоящее из элементов, лежащих как в x, так и в y; ***разность*** $x \setminus y = \{z \in x \mid z \notin y\}$; ***симметрическую разность*** $x \triangle y = (x \cup y) \setminus (x \cap y) = (x \setminus y) \cup (y \setminus x)$.

ZF7 (аксиома степени) Для любого множества x существует множество, состоящее из всех подмножеств множества x; оно называется ***множеством-степенью*** или ***булеаном*** и обозначается $\mathscr{P}(x)$ или 2^x.

ZF8 (аксиома регулярности) Каждое непустое множество x содержит элемент y такой, что $x \cap y = \varnothing$.

C (аксиома выбора) Для каждого множества x, состоящего из непересекающихся непустых элементов, существует множество, которое пересекается с каждым элементом множества x ровно по одному элементу.[5]

[4] «Острие критики логических парадоксов было нацелено на содержащееся в них допущение, состоящее в том, что для любого свойства $P(x)$ существует соответствующее множество всех элементов x, обладающих свойством $P(x)$. Стоит лишь отвергнуть это допущение, и логические парадоксы становятся невозможными» (Э. Мендельсон. Введение в математическую логику, с. 10).

[5] Одна из многочисленных равносильных формулировок аксиомы выбора.

Определим ***декартово произведение*** $X \times Y = \{(x,y) \mid x \in X,\ y \in Y\}$. Аналогично можно определить декартово произведение большего числа множеств. $X^0 = \{\varnothing\}$, $X^1 = X$, $X^2 = X \times X$ (декартов квадрат), $X^3 = X \times X \times X$ (декартов куб) и т.д.

Опр. 1.1. Любое подмножество множества $X \times Y$ называется ***отношением между*** X и Y; при $X = Y$ их называют ***бинарными отношениями на*** X. Отношение $f \subseteq X \times Y$ называется ***отображением*** или ***функцией*** из X в Y, если $\forall x \in X\, \exists y \in Y\, (x,y) \in f$ и $\forall x \forall y_1 \forall y_2\, (((x,y_1) \in f \wedge (x,y_2) \in f) \Rightarrow y_1 = y_2)$.[6] $X = D(f) = \delta_f$ — ***область определения*** отображения f, $Y = R(f) = \rho_f$ — его ***область значений***.[7]

Замечание. Области определения или значений входят в определение отображения! Соответственно, два отображения $f\colon X \to Y$ и $g\colon A \to B$ считаются ***равными***, если $X = A$, $Y = B$ и $\forall x \in X\ f(x) = g(x)$.

Все отображения из X в Y обозначаются Y^X, $\mathrm{Map}(X,Y)$ или $\mathrm{Func}(X,Y)$. Обычно вместо $f \in Y^X$ пишут $f\colon X \to Y$. Если $(x,y) \in f$, то пишут $y = f(x)$ или $f\colon x \mapsto y$ и y называется ***образом*** x, x — ***прообразом*** y. ***Тождественное отображение*** $\mathrm{id}_X \in X^X$, $x \mapsto x$. $\pi_1\colon X \times Y \to X$, $(x,y) \mapsto x$; $\pi_2\colon X \times Y \to Y$, $(x,y) \mapsto y$ — ***проекции*** декартова произведения на первый и второй сомножители соответственно.

Опр. 1.2. ***Образ множества*** $A \subseteq X$: $f(A) = \{y \in Y \mid \exists x \in A\, y = f(x)\}$. ***Прообраз множества*** $B \subseteq Y$: $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$.
$f^{-1}(y) = \{x \in X \mid f(x) = y\}$ — ***полный прообраз*** y или ***слой отображения*** f ***над*** y.

Опр. 1.3. Отображения X^X обычно называются ***преобразованиями*** множества X. Отображение $f\colon X \to Y$ называется ***инъекцией***, если $\forall x_1, x_2 \in x$ $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. Отображение $f\colon X \to Y$ называется ***сюръекцией*** (***отображением*** ***<u>на</u>***) если $f(X) = Y$. Если отображение одновременно является инъекцией и сюръекцией, то оно называется ***биекцией*** или ***взаимно однозначным отображением***.

Множества всех инъекций, сюръекций и биекций из X в Y обозначаются $\mathrm{Inj}(X,Y)$, $\mathrm{Sur}(X,Y)$ и $\mathrm{Bij}(X,Y)$ соответственно. Отображения из $\mathrm{Bij}(X,X)$ называются ***перестановками*** множества X.

Опр. 1.4. ***Композиция*** отображений $f\colon X \to Y$ и $g\colon Y \to Z$ — отображение $g \circ f\colon X \to Z$, $x \mapsto g(f(x))$.

---

[6] Иногда первая часть (чтоб пробегалось <u>всё</u> X) не требуется. См., например, Н. К. Верещагин, А. Шень. Начала теории множеств, с. 32–33.

[7] Эти определения отличаются от школьных и от определений во многих учебниках математического анализа (и не только). Здесь используются определения из Кострикин А. И. Введение в алгебру. Часть I. Основы алгебры.

Теорема 1.4. (***ассоциативность композиции***) *Если одна из композиций* $(h \circ g) \circ f$ *и* $h \circ (g \circ f)$ *определена, то определена и вторая, при этом верно равенство* $(h \circ g) \circ f = h \circ (g \circ f)$.

Замечание. В общем случае композиция не коммутативна: $f \circ g \neq g \circ f$.

Опр. 1.5. Отображение $g\colon Y \to X$ называется ***левым обратным*** к $f\colon X \to Y$, если $g \circ f = \mathrm{id}_X$, и ***правым обратным*** к тому же f, если $f \circ g = \mathrm{id}_Y$. Само отображение f при этом называется ***обратимым слева*** или ***обратимым справа*** соответственно. Отображение g называется ***обратным*** к f, если оно одновременно является и левым обратным, и правым обратным — само f при этом называется ***обратимым***.

Лемма 1.1. *Если у отображения есть левое обратное и правое обратное, то они совпадают. Следовательно, отображение обратимо тогда и только тогда, когда оно обратимо слева и обратимо справа.*

Теорема 1.5. $f\colon X \to Y$.
1) *Пусть* $X \neq \varnothing$. f *обратимо слева тогда и только тогда, когда* f *— инъекция*;
2) f *обратимо справа тогда и только тогда, когда* f *— сюръекция*;
3) f *обратимо тогда и только тогда, когда* f *— биекция.*

Опр. 1.6. Пусть $X \neq \varnothing$. Отношение $R \subseteq X^2$ называется ***отношением эквивалентности*** или просто ***эквивалентностью***, если оно
• рефлексивно: $(x, x) \in R \quad \forall x \in X$;
• симметрично: $(x, y) \in R \Rightarrow (y, x) \in R \quad \forall x, y \in X$;
• транзитивно: $((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R \quad \forall x, y, z \in X$.
Часто эквивалентность обозначается значком $\sim$.

Опр. 1.7. ***Класс эквивалентности*** $\overline{x}$ элемента x — множество всех элементов X, эквивалентных x: $\overline{x} = \{y \in X \mid y \sim x\}$.

Теорема 1.6. *Любое отношение эквивалентности разбивает множество на непересекающиеся классы эквивалентности. И наоборот, любому такому разбиению соответствует некоторое отношение эквивалентности.*

Опр. 1.8. Множество $X/{\sim} = \{\overline{x} \mid x \in X\}$ классов эквивалентности $\sim$ называется ***фактормножеством*** X по отношению $\sim$, а отображение $\pi\colon X \to X/{\sim}$, $x \mapsto \overline{x}$ — ***канонической проекцией*** X на $X/{\sim}$ (легко заметить, что оно сюръективно). ***Трансверсаль*** к эквивалентности — подмножество в X, содержащее ровно один элемент из каждого класса эквивалентности.

Теорема 1.7. *Для каждого отношения эквивалентности существует трансверсаль.*

Важный вопрос о факторструктурах: в какой степени $X/{\sim}$ наследует имеющиеся на X структуры?

Единственный инвариант относительно биекций называется ***мощностью***[8]: два множества называются ***равномощными***, если между ними существует биекция. Мощность множества X обозначается $|X|$. Множество называется ***конечным***, если оно не равномощно никакому своему собственному подмножеству, в противном случае — ***бесконечным***.

Мощности можно сравнивать: говорят, что $|X| \leqslant |Y|$, если существует инъекция из X в Y (другими словами, если X равномощно некоторому подмножеству множества Y). $|X| < |Y|$, если $|X| \leqslant |Y|$ и $|X| \neq |Y|$. Например, $|\varnothing| < |\{\varnothing\}| < |\{\varnothing, \{\varnothing\}\}|$. Другими словами, $|X| = |Y| \Leftrightarrow \mathrm{Bij}(X, Y) \neq \varnothing$, а $|X| \leqslant |Y| \Leftrightarrow \mathrm{Inj}(X, Y) \neq \varnothing$.

Теорема 1.8. (***принцип Дирихле***) *Если $|X| > |Y|$, то не существует инъекций из X в Y.*

Замечание. Если X и Y конечны, то $|Y^X| = |Y|^{|X|}$. В частности, если $X = \varnothing$, то существует ровно одно отображение из X в Y — пустое. Если же $Y = \varnothing$, то для непустого X точке из X нечего сопоставить — всего нуль отображений. Если же и X, и Y оба пусты, то существует ровно одно отображение — пустое (в данном случае тождественное), следовательно, $|\varnothing^\varnothing| = 1$.

§2. Бесконечные числовые системы

Учитель сказал, что я совсем не знаю математики
и поставил мне в дневник какую-то цифру.

Система Пеано — тройка $\langle X, e, s\rangle$, где X — множество (носитель системы), а 0-местная функция (= константа) e и 1-местная функция $s\colon X \to X$ удовлетворяют следующим аксиомам:

1) $e \in X$;
2) s инъективна;
3) $e \notin s(X)$;
4) (схема аксиом индукции) Подмножество в X, содержащее e и вместе с каждым $x \in X$ содержащее и $s(x)$, совпадает со всем множеством X.

Натуральные числа без нуля $\mathbb{N} = \{\{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \ldots\}$, $e = \{\varnothing\} = 1$.

Натуральные числа с нулём $\mathbb{N}_0 = \omega = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \ldots\}$, $e = \varnothing = 0$.

$s(x) = x \cup \{x\}$, тогда $s(\varnothing) = 1$, $1 = \{0\}$, $2 = \{0, 1\}$, … , $n = \{0, 1, 2, \ldots, n-1\}$, то есть $\mathbb{N}_0$ — мощности конечных множеств. Тогда $m \leqslant n$ означает, что $m \subseteq n$, $m < n$ — что $m \subset n$.

[8] Георг Кантор: «*Мощностью* или *кардинальным числом* множества M мы называем то общее понятие, которое получается при помощи нашей активной мыслительной способности из M, когда мы абстрагируемся от качества его различных элементов m и от порядка их задания».

Теорема 2.1. (***принцип Дирихле bis***) *Если у нас есть n кроликов, которых мы хотим рассадить по m клеткам, причём $n > m$, то хотя бы в одной клетке окажется по крайней мере два кролика.*

$|\mathbb{N}| = |\mathbb{N}_0| = \aleph_0$. Все множества мощности $\aleph_0$ (т.е. находящиеся во взаимно однозначном соответствии с множеством натуральных чисел) называются ***счётными***. Бесконечные множества, не являющиеся счётными, называются ***несчётными***. Наименьшая мощность несчётного множества обозначается $\aleph_1$.[9]

Определим бинарную операцию $f\colon \mathbb{N}^2 \to \mathbb{N}$ рекурсивно:
С1) $f(x, 1) = s(x)$;
С2) $f(x, s(y)) = s(f(x, y))$.

Теорема 2.2. *f ассоциативна и коммутативна.*

Лемма 2.1. $\forall x, y, z \in \mathbb{N}\ f(x, z) = f(y, z) \Rightarrow x = y$.

Определим и бинарную операцию $g\colon \mathbb{N}^2 \to \mathbb{N}$ рекурсивно:
У1) $g(x, 1) = x$;
У2) $g(x, s(y)) = f(g(x, y), x)$.

Теорема 2.3. *g ассоциативна и коммутативна, g дистрибутивна относительно f.*

Суть f и g: это привычные сложение и умножение (можно было определять их на $\mathbb{N}_0$).

Рассмотрим множество $\mathbb{N}_0^2$ и зададим на нём отношение $\sim$ следующим образом: $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 + y_2 = y_1 + x_2$. Определим операции $+$ и $\cdot$ на $\mathbb{N}_0^2$:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

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

Можно показать, что $\sim$ является отношением эквивалентности на $\mathbb{N}_0^2$, согласованным с операциями. Классы эквивалентности отношения $\sim$ называются ***целыми числами*** и обозначаются $\mathbb{Z}$. Введённые операции соответствуют привычным операциями над целыми числами. Можно естественным образом вложить (неформально говоря, получить в большей структуре «копию» меньшей с сохранением всех свойств меньшей) натуральные числа в так определённые целые: $\mathbb{N}_0 \hookrightarrow \mathbb{Z}$, $n \mapsto \overline{(n, 0)}$. Нетрудно заметить, что нулём (нейтральным по

[9] При построении иерархии мощностей возникают вопросы: 1) Верно ли, что любые мощности сравнимы в указанном выше смысле? Положительный ответ равносилен аксиоме выбора; 2) Существуют ли вообще несчётные множества? Далее будут примеры. 3) Непонятно, почему среди их мощностей непременно есть наименьшая. Об этом см., например, Н. К. Верещагин, А. Шень. Начала теории множеств (https://mccme.ru/free-books/shen/shen-logic-part1-2.pdf), глава 2. Упорядоченные множества.

сложению) в $\mathbb{Z}$ является класс $\overline{(0,0)}$. Тогда отрицательные целые числа — это классы $\overline{(0,n)}$.

Теперь рассмотрим множество $\mathbb{Z} \times \mathbb{N}$ и зададим на нём отношение $\sim$ следующим образом: $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 \cdot y_2 = x_2 \cdot y_1$. Определим операции $+$ и $\cdot$ на $\mathbb{Z} \times \mathbb{N}$:

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

Вновь можно показать, что $\sim$ является отношением эквивалентности на $\mathbb{Z} \times \mathbb{N}$, согласованным с операциями. Классы эквивалентности отношения $\sim$ называются ***рациональными числами*** и обозначаются $\mathbb{Q}$. Введённые операции соответствуют привычным операциями над рациональными числами. Можно естественным образом вложить целые числа в так определённые рациональные: $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $x \mapsto \overline{(x,1)}$.

Теорема 2.4. $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

$|\mathscr{P}(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}| = \mathfrak{c}$ — ***мощность континуума***.

Теорема 2.5. $\mathfrak{c} > \aleph_0$.

Теорема 2.6. (***теорема Кантора***) *$|\mathscr{P}(X)| > |X|$ для любого множества X.*

Следствие 2.6.1. *$n < 2^n$ для любого $n \in \mathbb{N}_0$.*

Континуум-гипотеза: верно ли, что $\aleph_1 = \mathfrak{c}$? В 1963 г. П. Коэн доказал, что континуум-гипотеза не зависит от аксиом ZFC, то есть это одно из тех утверждений, которые в рамках ZFC нельзя ни доказать, ни опровергнуть.

Функции из $\mathbb{N}$ называются ***последовательностями***. Последовательность $f\colon \mathbb{N} \to \mathbb{Q}$ называется ***фундаментальной***, если для любого $n \in \mathbb{N}$ существует такое $N \in \mathbb{N}$, что для всех $m, k \in \mathbb{N}$

$$m, k \geqslant N \Rightarrow |f(m) - f(k)| < \frac{1}{2^n}.$$

Определим на множестве $\mathscr{R}$ всех фундаментальных последовательной отношение $\sim$: $f \sim g$ тогда и только тогда, когда для любого $n \in \mathbb{N}$ существует $N \in \mathbb{N}$ такое, что для всех $m \in \mathbb{N}$

$$m \geqslant N \Rightarrow |f(m) - g(m)| < \frac{1}{2^n}.$$

$\sim$ — эквивалентность на $\mathscr{R}$. Классы эквивалентности $\mathscr{R}/\!\sim\, = \mathbb{R}$ называются ***вещественными числами***. Можно определить на них естественные операции и порядок, и вложить $\mathbb{Q} \hookrightarrow \mathbb{R}$, $q \mapsto (q, q, q, \ldots)$.[10]

Теорема 2.7. $|\mathbb{R}| = \mathfrak{c}$.

[10] Более подробно о построении целых, рациональных и вещественных чисел как фактор-структур и о корректности введённых операций см., например, С. В. Судоплатов, Е. В. Овчинникова. Дискретная математика, § 3.1 Бесконечные числовые системы.

§3. Алгебраические операции и алгебраические системы

Что такое алгебра? Является ли она областью математики, методом или психологической установкой?

И. Р. Шафаревич[11]

Алгебра является не просто частью математики. Она играет по отношению к математике такую же роль, какую сама математика долгое время играла по отношению к физике.

К. Шевалле[12]

...главная трудность для начинающего заключается в овладении разумным словарным запасом за короткое время. Ни одно из новых понятий само по себе не является трудным, но их последовательное накопление может иногда показаться тяжким.

С. Ленг[13]

Опр. 3.1. ***n-арная*** (***n-местная***) ***алгебраическая операция*** — отображение $X_1 \times X_2 \times \ldots \times X_n \to Y$, где $X_1, X_2, \ldots, X_n, Y$ — непустые множества.

Опр. 3.2. Если $X_1 = X_2 = \ldots = X_n = Y$, то алгебраическая операция называется ***внутренней***.

$n = 0$ (нульарная): $\{\varnothing\} = X^0 \to X$ — выбор элемента в X — константа.
$n = 1$ (унарная): $X = X^1 \to X$ — отображение из X в X.
$n = 2$ (бинарная): $X^2 \to X$.
$n = 3$ (тернарная): $X^3 \to X$.

Замечание. В дальнейшем, если не оговорено иное, будем рассматривать внутренние бинарные операции, которые ещё называются ***внутренним законом композиции***.

Замечание. Обычно для записи бинарной операции используется ***инфиксная*** нотация, когда знак операции пишется ***между*** операндами: $x * y$, $x \circ y$, $x \smiley y$. Чаще всего мы будем использовать мультипликативную запись $(x \cdot y, xy)$ и называть операнды ***множителями***, а результат операции — ***произведением***. Аддитивную запись $(x + y)$ будем чаще всего использовать в контексте разговора об абелевых группах, тогда операнды называются ***слагаемыми***, а результат операции — ***суммой***.

[11] И. Р. Шафаревич. Основные понятия алгебры. — Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001, с. 9.
[12] Claud Chevalley. Fundamental Concepts of Algebra. — New York: Academic Press, 1956, p. V.
[13] С. Ленг. Алгебра — М.: Мир, 1968, с. 16.

Опр. 3.3. ***Алгебраическая система*** $\mathscr{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$ — объект, являющийся совокупностью непустого множества A и непустого набора алгебраических операций, заданных на A. Множество A называется ***носителем*** алгебраической системы.

Опр. 3.4. $\mathscr{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$ и $\mathscr{B} = \langle B, g_1, g_2, \ldots, g_k, \ldots \rangle$ — алгебраические системы с одним и тем же числом операций, причём операции f_i и g_i с одним и тем же индексом имеют одинаковую арность n_i. Отображение $\varphi\colon A \to B$ называется ***гомоморфизмом*** алгебраических систем $\mathscr{A}$ и $\mathscr{B}$, если для любого индекса i и любого кортежа $(a_1, a_2, \ldots, a_{n_i}) \in A^{n_i}$ верно равенство

$$\varphi(f_i(a_1, a_2, \ldots, a_{n_i})) = g_i(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{n_i})).$$

Гомоморфизм системы в себя — ***эндоморфизм***, биективный изоморфизм систем — ***изоморфизм***, изоморфизм на себя — ***автоморфизм***.

Отношение изоморфности на множестве рассматриваемых алгебраических систем является отношением эквивалентности. Изоморфные системы выглядят по-разному, а по сути одно и то же: они совпадают с точностью до переобозначений элементов и операций. Изоморфность влечёт полное совпадение алгебраических свойств систем. Другими словами, любое утверждение, которое можно записать в терминах алгебраических операций, заданных на одной из систем, будет верно и для второй системы (разумется, в терминах соответствующих операций второй системы). Для доказательства изоморфности достаточно указать один изоморфизм. Если носители систем не равномощны, то системы точно не изоморфны. Как доказать неизоморфность, если носители равномощны? Нужно указать свойство операции одной системы, которое не выполняется для соответствующей операции второй системы.

Опр. 3.5. Говорят, что множество B ***замкнуто относительно операции*** $*$, если $\forall x, y \in B\ x * y \in B$.

Опр. 3.6. Система $\mathscr{B} = \langle B, f_1, f_2, \ldots, f_k, \ldots \rangle$ называется ***подсистемой*** системы $\mathscr{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$, если $B \subseteq A$ и B замкнуто относительно всех операций f_i.

Пусть на множестве X задана бинарная операция $*$. Если множество X конечно, то есть $X = \{x_1, \ldots, x_n\}$, то операцию можно задать с помощью ***таблицы Кэли***: на пересечении i-той строки и j-того столбца стоит элемент $x_i * x_j$.

Опр. 3.7. Элемент $x \in X$ называется ***идемпотентом***, если $x * x = x$.

Опр. 3.8. Элемент $e_L \in X$ называется ***левым нейтральным***, если $\forall x \in X$ $e_L * x = x$. Элемент $e_R \in X$ называется ***правым нейтральным***, если $\forall x \in X$ $x * e_R = x$. Элемент $e \in X$ называется ***нейтральным***, если он одновременно левый нейтральный и правый нейтральный. В мультипликативной нотации (левый/правый) нейтральный называется (***левой/правой***) ***единицей***, в аддитивной — (***левым/правым***) ***нулём***.

Лемма 3.1. *Если в X есть левый нейтральный и правый нейтральный, то они совпадают.*

Опр. 3.9. Элемент x множества X с нейтральным элементом e называется ***инволюцией***, если $x * x = e$.

Опр. 3.10. Элемент $x \in X$ называется ***регулярным слева***, если на него можно сокращать слева: $\forall y, z \in X \; x * y = x * z \Rightarrow y = z$. Элемент $x \in X$ называется ***регулярным справа***, если на него можно сокращать справа. Если элемент регулярен и слева, и справа, он называется ***регулярным***.

Опр. 3.11. Элемент $y \in X$ с нейтральным элементом e называется ***левым симметричным*** к x, если $y * x = e$. Элемент $y \in X$ с нейтральным элементом e называется ***правым симметричным*** к x, если $x * y = e$. Элемент $y \in X$ с нейтральным элементом e называется ***симметричным*** к x, если $x*y = y*x = e$. При использовании аддитивной записи (левый/правый) симметричный называются (***левым***/***правым***) ***противоположным***, при использовании мультипликативной записи — (***левым***/***правым***) ***обратным***. Если элемент имеет (левый/правый) симметричный, то он называется ***симметризуемым*** (***слева***/***справа***). При использовании же мультипликативной записи, он называется ***обратимым*** (***слева***/***справа***)

Опр. 3.12. Операция $*$ на множестве X называется ***ассоциативной***, если $\forall x, y, x \in X \; (x * y) * z = x * (y * z)$.

Опр. 3.13. Операция $*$ на множестве X называется ***коммутативной***, если $\forall x, y \in X \; x * y = y * x$.

Теорема 3.1. (***об обобщённой ассоциативности***) *Если на X задана ассоциативная операция $*$, то она обладает обобщённой ассоциативностью: результат $x_1 * x_2 * \ldots * x_n$ не зависит от расстановки скобок.*[14]

Опр. 3.14. Множество X с заданной на нём ассоциативной операцией называется ***полугруппой***.

Опр. 3.15. Полугруппа с нейтральным элементом называется ***моноидом***.

Лемма 3.2. *Пусть X — моноид. Тогда если у элемента $x \in X$ есть правый симметричный и левый симметричный, то они совпадают.*

Лемма 3.3. *Элемент x моноида X, обратимый слева/справа, является регулярным слева/справа.*

В набор операций для полугруппы входит только бинарная операция, а для моноида — ещё и нульарная операция (константа — нейтральный элемент). В свете этого, определение гомоморфизма для них принимает следующий вид:

[14] На лекции не доказывалась. Доказательство см., например, в А. И. Кострикин. Введение в алгебру. Часть I. Основы алгебры.

Опр. 3.16. Пусть $\langle X, * \rangle$ и $\langle Y, \star \rangle$ — полугруппы. Отображение $f\colon X \to Y$ называется ***гомоморфизмом полугрупп***, если $f(x_1 * x_2) = f(x_1) \star f(x_2)$ для любых $x_1, x_2 \in X$. Если X и Y — моноиды, то f называется ***гомоморфизмом моноидов***, если это гомоморфизм соответствующих полугрупп и $f(e_X) = e_Y$ (e_X, e_Y — соответствующие нейтральные элементы). ***Изоморфизм*** полугрупп/моноидов — их биективный гомоморфизм.

Вновь к **важному вопросу о факторструктурах**:

Опр. 3.17. Отношение эквивалентности $\sim$ на множестве X называется ***согласованным*** с операцией $*\colon X \times X \to X$, если из $a \sim b$ и $c \sim d$ следует $a * b \sim c * d$.

В таком случае на фактормножестве $X/\sim$ можно корректно определить операцию $*$: $(\overline{a}, \overline{b}) \mapsto \overline{a} * \overline{b} = \overline{a * b}$ (что и было сделано при построении $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$). То есть для проведения операции над двумя классами эквивалентности $\overline{a}$ и $\overline{b}$ нужно выбрать в них представителей a и b, произвести операцию над ними и взять тот класс, в который попал элемент $a * b$. Независимость результата от выбора представителей как раз обеспечивается согласованностью эквивалентности с операцией. Свойства операции в X, имеющие характер тождества, наследуются операцией в $X/\sim$. То же верно насчёт наличия нейтральных и симметричных элементов.

§4. Группы

...понятие группы является древнейшим математическим понятием, не только более древним, чем алгебраические уравнения, но даже более древним, чем само понятие числа, и неотделимым от человеческой цивилизации.

Н. А. Вавилов[15]

Опр. 4.1. ***Группа*** — моноид, в котором все элементы обратимы.

Лемма 4.1. $(x^{-1})^{-1} = x,\ (xy)^{-1} = y^{-1}x^{-1}$.

В произвольном моноиде X все обратимые элементы образуют ***группу*** X^* ***обратимых элементов моноида***.

Лемма 4.2. *G — группа. $\forall g, h \in G\ \exists!\, x \in G\ hx = g$; $\forall g, h \in G\ \exists!\, x \in G\ xh = g$.*

Опр. 4.2. ***Порядок группы*** — мощность носителя группы. Обозначается $|G|$.

Опр. 4.3. Группа с коммутативной операцией называется ***абелевой группой***.

[15]Николай Вавилов. Конкретная теория групп.

Опр. 4.4. ***Прямое произведение групп*** $\langle G_1, *_1\rangle$ и $\langle G_2, *_2\rangle$ — группа с носителем $G_1 \times G_2$ и операцией $(a, b) * (c, d) = (a *_1 b, c *_2 d)$.

Опр. 4.5. Пусть G — группа. Её подсистема H называется ***подгруппой*** (обозначается $H \leqslant G$), если она является группой относительно той же групповой операции. Другими словами,

1) H замкнуто относительно групповой операции;
2) $x \in H \Rightarrow x^{-1} \in H$;
3) $e \in H$;

Замечание. В реальности в группе три операции: умножение — бинарная, нейтральный элемент — нульарная, взятие обратного — унарная. Именно поэтому в определении подгруппы нужны пункты 2 и 3, а не только 1. Кроме того, если строго разграничивать саму группу (и вообще любую алгебраическую систему) и её носитель, то надо использовать буквы разного вида и писать $\mathscr{G} = \langle G, \cdot, e, \_^{-1}\rangle$. Мы, как и многие другие, будем допускать вольность и часто обозначать алгебраические системы и их носители буквой одного вида (что уже делали раньше). В старой литературе для обозначения алгебраических систем очень любили готические буквы $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ и т.д.[16]

Определим n-ную ($n \in \mathbb{Z}$) ***степень*** элемента $g \in G$: $g^0 = e$; $g^n = \underbrace{g \cdot \ldots \cdot g}_{n}$, если $n > 0$; $g^n = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}$, если $n < 0$ (при аддитивной записи аналогично определяются ***кратные*** ng элемента g). $g^n g^k = g^{n+k}$ для любых $n, k \in \mathbb{Z}$. Степени элемента g образуют подгруппу $\langle g\rangle \leqslant G$ — она называется ***циклической подгруппой, порождённой элементом*** g.

Опр. 4.6. ***Порядок элемента*** g ***группы*** G — наименьшее натуральное n такое, что $g^n = e$, если такое существует. Если такого натурального числа нет, то порядок равен ∞. Обозначение $|g|$, $\mathrm{ord}(g)$, $o(g)$.

Опр. 4.7. Группа называется G ***циклической***, если существует такой элемент $g \in G$ (***порождающий элемент*** группы G), что $G = \langle g\rangle$.

Лемма 4.3. 1) $g^n = e \Leftrightarrow o(g) \mid n$;
2) $g^n = g^m \Leftrightarrow n \equiv m \pmod{o(g)}$;
3) $|\langle g\rangle| = o(g)$;
4) $o(g^n) = \dfrac{o(g)}{\text{НОД}(o(g), n)}$;
5) *элемент* $g^n \in G = \langle g\rangle$ *является порождающим тогда и только тогда, когда* $\text{НОД}(o(g), n) = 1$.

Опр. 4.8. Пусть $\langle G, *\rangle$ и $\langle H, \star\rangle$ — группы. Отображение $\varphi\colon G \to H$ называются ***гомоморфизмом***, если $\forall x, y \in G$ $\varphi(x * y) = \varphi(x) \star \varphi(y)$. Гомоморфизм группы в себя называется ***эндоморфизмом***. Биективный гомоморфизм называется ***изоморфизмом*** ($G \simeq H$). Изоморфизм на себя называется ***автоморфизмом***.

[16] См., например, Б. Л. ван дер Варден. Алгебра.

По идее, в соответствии с общим определением гомоморфизма, нужно потребовать «сохранения» нейтрального элемента и обратных элементов. Однако это излишне, так как верна следующая лемма.

Лемма 4.4. *Образом нейтрального элемента при гомоморфизме групп является нейтральный. Образом обратного к x — обратный к образу x.*

Теорема 4.1. *Любая конечная циклическая группа изоморфна группе $\mathbb{Z}_n$. Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$.*

Опр. 4.9. Пусть G — группа, $H \leqslant G$. Будем говорить, что $g_1, g_2 \in G$ ***сравнимы по модулю*** H, если $g_1^{-1}g_2 \in H$, то есть $g_2 = g_1H$. Это отношение является эквивалентностью. Классы этой эквивалентности называются ***левыми смежными классами***.

Левый смежный класс, содержащий элемент g, имеет вид $gH = \{gh \mid h \in H\}$.

Замечание. Иногда смежные классы gH называют правыми смежными классами.

Лемма 4.5. (***свойства смежных классов***)
1) *Образуют разбиение множества G на попарно непересекающиеся подмножества;*
2) *Существует биекция между H и gH ($H \ni h \mapsto gh \in H$) и, следовательно, $|H| = |gH|$.*

Теорема 4.2. (***теорема Лагранжа***)
Пусть G — конечная группа, $H \leqslant G$, тогда $|G| = |H||G/H|$.

Следствие 4.2.1.
1) *Порядок любой подгруппы конечной группы делит порядок группы;*
2) *Порядок любого элемента конечной группы делит порядок группы;*
3) *Всякая конечная группа простого порядка является циклической;*
4) *$g^{|G|} = e$ для любого $g \in G$.*

Опр. 4.10. Число смежных классов G по подгруппе H называется ***индексом подгруппы*** H и обозначается $|G : H|$, $[G : H]$ или просто $|G/H|$.

Замечание. Можно рассмотреть смежность справа по подгруппе H, тогда получатся ***правые смежные классы*** $Hg = \{hg \mid h \in H\}$. Отображение $g \mapsto g^{-1}$ устанавливает биекцию $(gH)^{-1} = Hg^{-1}$ и вся теория переносится на правые смежные классы.

Опр. 4.11. Разбиение группы на левые (правые) смежные классы называется её ***левым*** (соответственно, ***правым***) ***разложением***.

§5. Группа перестановок

...вместилище всех вообще конечных групп, рассматриваемых с точностью до изоморфизма.

А. И. Кострикин[17]

Свойства перестановок настолько красивы, что представляют и самостоятельный интерес.

Д. Кнут[18]

Опр. 5.1. ***Группой S_n перестановок на n точках*** называется группа всех биекций на множестве $\{1, 2, \dots, n\}$ относительно операции композиции.

Опр. 5.2. ***Полная запись перестановки*** — запись перестановки σ в виде $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$.

Замечание. В контексте разговора о перестановках операция композиции часто называется умножением.

Теорема 5.1. $|S_n| = n!$

Опр. 5.3. Перестановка $\sigma \in S_n$ называется ***циклом*** длины k, если для некоторых различных $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$ $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, …, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$, а для всех остальных $i \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\}$ $\sigma(i) = i$. Цикл длины 1 будем называть ***тривиальным циклом***. Цикл длины n называется ***длинным циклом***.

Лемма 5.1. *Порядок цикла длины k равен k.*

Опр. 5.4. Циклы называются ***независимыми***, если множества перемещаемых ими элементов не пересекаются.

Опр. 5.5. Пусть $\sigma \in S_n$. Определим отношение $\sim$ на $\{1, 2, \dots, n\}$ так: $i \sim j \Leftrightarrow j = \sigma^k(i)$ для некоторого $k \in \mathbb{Z}$. Это отношение является эквивалентностью на множестве $\{1, 2, \dots, n\}$. Её классы эквивалентности называются ***орбитами*** σ.

Теорема 5.2.
1) *Любая перестановка раскладывается в произведение независимых циклов. Такое разложение единственно с точностью до порядка множителей.*
2) *Независимые циклы коммутируют.*

Опр. 5.6. ***Цикленная запись перестановки*** — запись перестановки в виде произведения независимых циклов.

---

[17] А. И. Кострикин. Введение в алгебру. Часть I. Основы алгебры.
[18] Дональд Э. Кнут. Искусство программирования. Том 3. Сортировка и поиск.

Замечание. Зависимые циклы в общем случае не коммутируют.

Опр. 5.7. ***Транспозиция*** — цикл длины 2, то есть перестановка двух элементов. ***Фундаментальная транспозиция*** — перестановка двух соседних элементов.

Лемма 5.2. *Любая перестановка раскладываться в произведение транспозиций.*

Опр. 5.8. Говорят, что пара элементов $\sigma(i)$ и $\sigma(j)$ образует ***инверсию***, если $\sigma(i) > \sigma(j)$ при $i < j$.

Опр. 5.9. ***Чётность перестановки*** σ — чётность числа инверсий $\operatorname{inv}(\sigma)$ в ней. Соответственно, перестановки делятся на ***чётные*** и ***нечётные***.

Опр. 5.10. ***Знак перестановки*** σ: $\operatorname{sgn}(\sigma) = (-1)^{\operatorname{inv}(\sigma)}$.

Лемма 5.3. *Фундаментальная транспозиция является нечётной перестановкой.*

Лемма 5.4. *Пусть $(i\,j)$ — произвольная транспозиция. Тогда для любой $\sigma \in S_n$ чётности перестановок σ и $\sigma(i\,j)$ различны.*

Следствие 5.2.1. *Любая перестановка раскладывается в произведение фундаментальных транспозиций.*

Теорема 5.3. *В S_n число чётных перестановок равно числу нечётных перестановок и равно $\dfrac{n!}{2}$ $(n > 1)$.*

Теорема 5.4. $\operatorname{sgn}(\sigma\pi) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi)$. *Другими словам, знак перестановки является гомоморфизмом групп S_n и $\{\pm 1\}$.*

Следствие 5.4.1. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Следствие 5.4.2. *Чётность числа транспозиций, на которые раскладывается перестановка, всегда одинакова.*

Следствие 5.4.3. *Все чётные перестановки A_n образуют подгруппу в группе S_n. A_n называется **знакопеременной группой**.*

Теорема 5.5. *Всякую перестановку из S_n можно разложить на $n - s$ транспозиций, где s — числов независимых циклов, на которые раскладывается перестановка, включая тривиальные.*

Опр. 5.11. Число $d(\sigma) = n - s$ из предыдущей теоремы называется ***декрементом*** перестановки σ. Легко заметить, что он равен разности между числом перемещаемых элементов и нетривиальных циклов.

Теорема 5.6. (***смысл декремента***) *Декремент — наименьшее число транспозиций, на которые можно разложить перестановку.*

Теорема 5.7. (***теорема Кэли***) *Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.*