ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Кафедра «Прикладная математика»

Краткое введение в теорию групп

Часть 1

«Высшая алгебра»

Авторы
И.В. Баранов,
И.А. Гусева

Ростов-на-Дону, 2022

Аннотация

Методические указания предназначены для студентов всех форм обучения.

Авторы

доцент, к.ф.–м.н.,
доцент каф. «Прикладная математика»
Баранов И.В.

доцент, к.ф.–м.н.,
доцент каф. «Теоретическая и прикладная механика»
И.А. Гусева

Оглавление

ПРЕДИСЛОВИЕ

Теория групп - важный раздел современной алгебры, находящий свои применения не только в математике, но и современной физике, химии, кристаллографии, а также в различных приложениях, таких, например как теория кодирования информации. Теория групп - изумительно изящный инструмент описания симметрий различных объектов. Поистине удивителен тот факт, что универсальные алгебраические структуры - такие как группа, были обнаружены относительно недавно - в 19 веке. Идеи, что называется, носились в воздухе. Возникновение теории групп по праву связано с именем гениального французского математика Эвариста Галуа (1811-1832г.), заложившего основы этой теории - человека с удивительной и трагической судьбой. Работы Галуа не были поняты современниками. Кроме, того, его преследовала воистину роковая цепь трагических неудач. Галуа послал известному математику Фурье труд о своих открытиях, но спустя несколько дней Фурье неожиданно умер, так и не успев им заняться, а сама рукопись исчезла — в оставшихся после смерти бумагах она не была обнаружена. Статья, посланная другому известному математику - Пуассону, была отвергнута с резолюцией, в которой было указано, что "доказательство г-на Галуа не обладает ни достаточной ясностью, ни достаточной полнотой для того, чтобы судить об его точности". Несмотря на роковое невезение Галуа всё же удалось опубликовать 3 статьи с изложением основ своей теории. Прожив всего 20 лет, и впервые прочитав в возрасте 16 лет работу Нильса Абеля касающуюся неразрешимости решения алгебраических уравнений степени 5 и выше в радикалах, Галуа за 4 года своей математической жизни, до трагической гибели в возрасте 20 лет на дуэли, успел заложить основы теории групп, идеи которой питали исследования в этой области сотни лет.

Данное пособие задумывалось как краткое введение в начальные главы теории групп. Несмотря на огромное количество книг, посвященных теории групп, существует потребность в коротком и ясном введении, которое помогло бы студенту освоиться с начальными понятиями и результатами этой теории и научить применять их к решению задач. Авторы пытались совместить конспективный, почти справочный стиль изложения с доказательством наиболее важных фактов. Определения и теоремы по возможности проиллюстрированы примерами. Структура изложения была выбрана так, чтобы все необходимые понятия были "под рукой", и не возникало особой необходимости обращаться к вспомогательной литературе. Насколько этот опыт получился успешным, судить конечно же читателю.

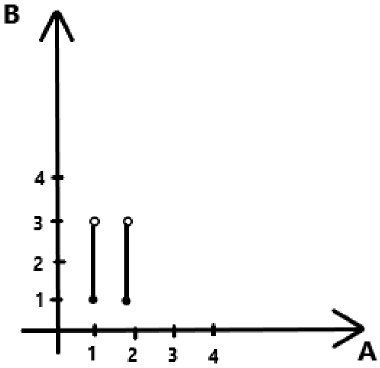
Ниже использованы стандартные обозначения N, Z, Q, R, C для множеств соответственно натуральных, целых, рациональных, вещественных и комплексных чисел. Значок ∀ - всякий, каждый, ∃ - существует, имеется, найдётся. Символ nZ обозначает множество чисел кратных n. Символом K_m обозначена мультипликативная группа корней из единицы степени m. Символом Z_n обозначена группа классов вычетов по модулю n.

§ 1. ДЕКАРТОВО ПРОИЗВЕДЕНИЕ, БИНАРНЫЕ ОТНОШЕНИЯ И КЛАССЫ ЭКВИВАЛЕНТНОСТИ

Определение.
Пусть A и B – множества.
Декартовым произведением множеств A и B называется множество *всевозможных упорядоченных* пар (a, b), где $a \in A$, $b \in B$
$A \times B = \{(a, b) | \forall a \in A, \forall b \in B\}$.

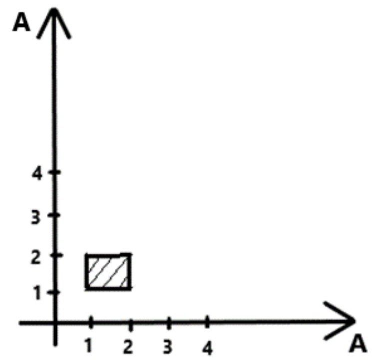
Пример.(множества A и B конечные)
$A = \{1, 2\}$
$B = \{\Sigma, \Psi, \Omega\}$
$A \times B = \{(1, \Sigma), (1, \Psi), (1, \Omega), (2, \Sigma), (2, \Psi), (2, \Omega)\}$

Пример.(множество A конечное, множество B бесконечное)
$A = \{1, 2\}$
$B = \{$*числовой промежуток* $[1, 3)\}$
$A \times B = \{(x, y) \mid x = 1$ *или* $2, 1 \le y < 3\}$, что можно изобразить на рисунке



В случае, когда $B = A$, декартово произведение $A \times A$ называется декартовым квадратом и обозначается A^2.

Пример.
$A = \{$*промежуток* $[1; 2]\}$
$A \times A = A^2 = \{(x, y) \mid 1 \le x \le 2, 1 \le y \le 2\}$



Пример.
Пусть $A = R = (-\infty; +\infty)$, тогда
$R \times R = R^2$ – декартова координатная плоскость.

Аналогично, можно обобщить понятие декартового произведения на случай n множеств. Пусть $A_1, A_2, \dots, A_n$ – множества. Тогда
$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots x_n) \mid \forall x_1 \in A_1, \forall x_2 \in A_2, \dots, \forall x_n \in A_n\}$.
Например,

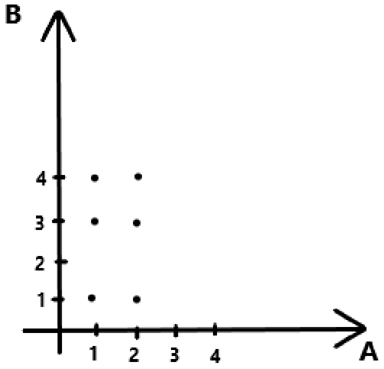
$R \times R \times R = R^3$ - декартово координатное пространство (пространство точек с тремя координатами)

$\underbrace{R \times R \times \ldots \times R}_{n \text{ раз}} = R^n$ - пространство точек с n координатами.

Напомним, что $|A|$ обозначает мощность множества A. Если A – конечное множество, то $|A|$ равно числу элементов множества A.

Теорема.
Если A и B конечные множества и $|A| = m$, $|B| = n$, то $|A \times B| = mn$.

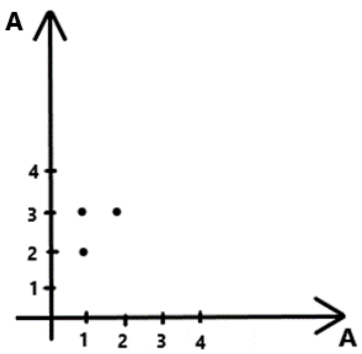
Пример.
$A = \{1, 2\}$, $|A|=2$,
$B = \{1, 3, 4\}$, $|B|=3$,
$A \times B = \{(1, 1), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4)\}$, $|A \times B|=6$.



Пусть A и B – множества.

Определение.
Бинарное отношение – всякое подмножество C из декартового произведения $A \times B$
$C \subset A \times B$
Если пара $(a, b) \in C$, пишут $a \rho b$, где ρ – отношение между элементами a и b, задаваемое C.

Пример.
$A = \{1, 2, 3\}$
$A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$
Зададим на $A \times A$ например такое отношение ρ: $C = \{(1, 2), (1, 3), (2, 3)\}$,
или $1 \rho 2$, $1 \rho 3$, $2 \rho 3$



Легко догадаться, что отношение ρ суть отношение "меньше (<)" на множестве A.

Определение.
Отношение $a \rho b$ называется *рефлексивным*, если для любого a принадлежащего отношению ρ выполняется $a \rho a$.

Пример.
Отношение « ≤ » на множестве *N* натуральных чисел является рефлексивным.

Определение.
Отношение *a ρ b* называется *симметричным*, если из *a ρ b* следует (=>) *b ρ a*.

Пример.
На множестве *N* отношение «=» является симметричным.

Определение.
Отношение *a ρ b* называется *транзитивным*, если из *a ρ b* и *b ρ c* => *a ρ c*.

Пример.
Рассмотрим отношение « > » на множестве *N*. Оно является транзитивным, так как для любых элементов $\forall$ *a, b, c* $\in$ *N* выполняется условие
$(a > b) \wedge (b > c) \Rightarrow (a > c)$.

Определение.
Отношение *ρ* называется отношением *эквивалентности*, если оно рефлексивно, симметрично и транзитивно. Для него используют значок
"волна" $a \sim b$.

Пример.
Отношение « = » на множестве чисел является отношением эквивалентности.

Классы эквивалентных элементов.
Пусть "~" отношение эквивалентности на $A \times A$ (или, коротко, просто на A)
Подмножество $\bar{a} = \{b \in A \mid a \sim b\}$ всех элементов, эквивалентных a, называется *классом эквивалентности* элемента a. Любой элемент класса $\bar{a}$ называется *представителем* этого класса. В частности, элемент a представитель класса $\bar{a}$, так как $a \sim a$ в силу рефлексивности. Иногда для обозначения класса вместо $\bar{a}$ используют обозначение $[a]$.

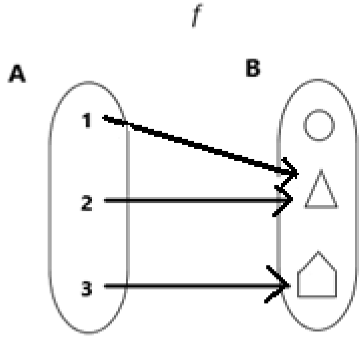
Теорема. Отношение эквивалентности "~" на A задает разбиение этого множества на непересекающиеся подмножества – классы эквивалентных элементов.

Доказательство.
Т.к всякий элемент $a \in \bar{a}$, то $A = \bigcup \bar{a}$
Далее, класс $\bar{a}$ однозначно задается любым своим представителем, т.е. $\bar{a} = \bar{a}_1 \Leftrightarrow a \sim a_1$. Действительно, т.к. классы $\bar{a}$ и $\bar{a}_1$ совпадают, то $a \sim a_1$. Пусть $a_2 \in \bar{a} \Rightarrow a_2 \sim a \Rightarrow a_2 \sim a_1 \Rightarrow a_2 \in \bar{a}_1 \Rightarrow \bar{a} \subset \bar{a}_1$. С другой стороны из $a \sim a_1$ следует $a_1 \sim a$, поэтому выполнено и обратное включение $\bar{a}_1 \subset \bar{a}$, стало быть $\bar{a}_1 = \bar{a}$. В другую сторону $a \in \bar{a}$, поэтому из $\bar{a}_1 = \bar{a}$ следует $a \in \bar{a}_1 \Rightarrow a \sim a_1$.
Докажем теперь, что два класса либо не пересекаются, либо совпадают. Предположим $\bar{a}_1 \neq \bar{a}_2$ но при этом $\bar{a}_1 \cap \bar{a}_2 \neq \varnothing$, тогда найдется $x \in \bar{a}_1 \cap \bar{a}_2$, тогда $x \sim a_1$ и $x \sim a_2$. Отсюда в силу того, что "~" транзитивно, имеем $a_1 \sim a_2$, т.е. $\bar{a}_1 = \bar{a}_2$. Противоречие.

§2. ОТОБРАЖЕНИЯ

Определение.
Пусть *A* и *B* – множества.
Отображением f из *A* в *B* называется правило, согласно которому каждому
a ϵ A ставится в соответствие *точно один b ϵ B*.

Пример.
$A = \{1, 2, 3\}$
$B = \{○ , Δ, ⌂\}$



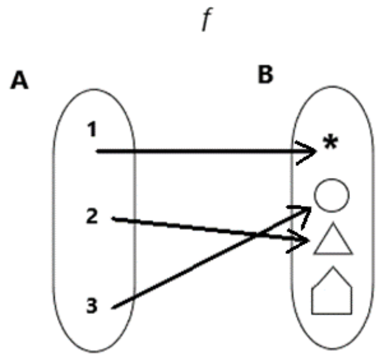
Пишут:
f(a) = b; *b* – образ *a*, *a* – прообраз *b*.

$a \xmapsto{f} b$

$f\colon A \to B$
Например *f(2)*=Δ, или в других обозначениях $2 \longmapsto Δ$.

Определение.
Отображение $f\colon A \to B$ называется *инъективным* или инъекцией, если для
$\forall\, a1, a2 \in A$:(таких, что) $a1 \neq a2$ =>(выполняется) $f(a1) \neq f(a2)$.

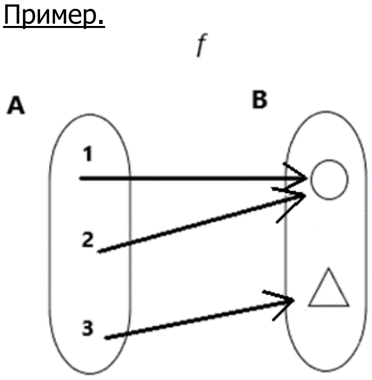
Пример.



f – инъекция.

Определение.
Отображение $f\colon A \to B$ называется *сюръективным* или сюръекцией, если
$\forall\, b \in B$ имеет прообраз $a \in A$.

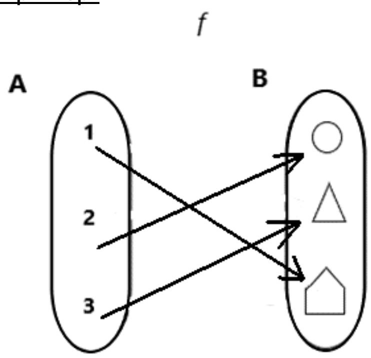
Пример.



f – сюръекция.

Определение.
Отображение *f: A→B* называется *биективным* (биекцией), если оно инъективно и сюръективно.

Пример.



f – биекция.

Напомним, что слово *композиция* означает последовательное выполнение каких-либо действий.
Определение.
Пусть имеются два отображения: $f: U \to V$ и $g: V \to W$.
Композицией отображений *f* и *g* называется отображение $h: U \to W$, которое действует по правилу: $h(u) = g(f(u))$.

$$\begin{tikzcd} U \arrow[rr, "h"] \arrow[dr, "f"'] & & W \\ & V \arrow[ur, "g"'] & \end{tikzcd}$$

Запись композиции ("$\circ$" -- символ композиции):
$h(u) = (g \circ f)(u)$ или коротко $h = g \circ f$
Нижеприведенные два примера демонстрируют, что композиция, вообще говоря, не коммутативна (надеть сначала рубашку а затем пиджак вовсе не то же самое, что надеть пиджак, а затем рубашку).

Пример.
Пусть $U = V = W = R$,
$f = \sin()$
$g = ()^2$
тогда
$(g \circ f)(x) = \sin^2(x)$
$(f \circ g)(x) = \sin(x^2)$
Заметим, что $g \circ f \neq f \circ g$

Пример.

Возьмем следующие отображения:

$f: R \to R$ действующее по правилу: $\forall x \quad f(x) = 1$, (любое x отображение f переводит в 1) и $g: R \to R$ такое что $g(x) = 2$, $\forall x$, (любое x отображение g переводит в 2), тогда

$(f \circ g)(u) = f(g(u)) = f(2) = 1$

$(g \circ f)(u) = g(f(u)) = g(1) = 2$

Снова видим, что $g \circ f \neq f \circ g$

Теорема (об ассоциативности композиции отображений).

Пусть $f: U \to V$, $g: V \to W$, $h: W \to T$ отображения,

тогда $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство.

$$\begin{tikzcd} U \arrow[d, "f"'] \arrow[dr, "\beta"] & T \\ V \arrow[r, "g"'] \arrow[ur, "\alpha"] & W \arrow[u, "h"'] \end{tikzcd}$$

Обозначим

$\alpha = h \circ g$

$\beta = g \circ f$

Нужно показать, что значения равенства совпадают на любом элементе u из U.

$((h \circ g) \circ f)(u) = (\alpha \circ f)(u) = \alpha(f(u)) = (h \circ g)(f(u)) = h(g(f(u)))$

$(h \circ (g \circ f))(u) = (h \circ \beta)(u) = h(\beta(u)) = h((g \circ f)(u)) = h(g(f(u)))$

Правые части совпали, следовательно совпадают и левые.

Определение.

Отображение $e_x: X \to X$, которое каждый элемент x множества X оставляет на месте, то есть действующее по правилу $e_x(x) = x$, называется *тождественным* отображением.

Определение.

Пусть $f: X \to Y$ и $g: X \to Y$ – отображения.

Отображение g называется *левым обратным* к f, если $g \circ f = e_x$.

Определение.

Отображение g называется *правым обратным* к f, если $f \circ g = e_y$.

Определение.

Если отображение g одновременно является и левым, и правым обратным к f, то его называют *двусторонним обратным* (или просто *обратным*) и обозначают f^{-1}.

Теорема.

Если $f: X \to Y$ биективно, то для него существует обратное отображение.

Доказательство.

Так как по условию f – биекция, то f – сюръекция, а значит

$\forall y \in Y, \quad \exists \; x \in X: \; f(x) = y$. Заметим, что такой x точно один. Действительно, если бы $\exists$ еще один x_1 такой что $f(x_1) = y$, то это противоречило бы инъективности f. Эти факты дают возможность определить отображение

$g: Y \to X$ действующее по правилу $g(y) = x$.

Тогда $(g \circ f)(x) = g(f(x)) = g(y) = x$, следовательно $g \circ f = e_x$

Далее, $(f \circ g)(y) = f(g(y)) = f(x) = y$, значит $f \circ g = e_y$

Таким образом, отображение g является двусторонним обратным к f или просто обратным.

Следствие.
Если отображение $f: X \to Y$ – биекция, то обратное отображение $f^{-1}: Y \to X$ тоже будет биекцией.

Доказательство.
Нужно показать, что f^{-1} обладает свойствами инъективности и сюръективности.
Заметим, что, согласно доказанной теореме, отображение f^{-1} существует.
Докажем инъективность:
Возьмем $\forall y_1, y_2 \in Y$ такие, что $y_1 \neq y_2$ и покажем, что, если $x_1 = f^{-1}(y_1)$ и $x_2 = f^{-1}(y_2)$, то $x_1 \neq x_2$.
Предположим, что $x_1 = x_2$. Тогда $f(x_1) = f(x_2) \Rightarrow y_1 = y_2$ – противоречие.
Инъективность доказана.
Докажем сюръективность:
Заметим, по условию f – отображение, но тогда для $\forall x \in X \quad \exists \ y = f(x) \in Y$. Согласно теореме, существует обратное отображение f^{-1}, действующее по правилу: $f^{-1}(y) = x$. То есть, у любого образа x у отображения f^{-1} есть прообраз y. А это и означает сюръективность f^{-1}.

Теорема (о композиции инъективных отображений).
Если $f: X \to Y$ и $g: Y \to Z$ – два инъективных отображения, то тогда отображение $(g \circ f)$ тоже будет инъективным. Коротко: композиция инъективных отображений – инъективное отображение.

Доказательство.
Возьмём 2 любых элемента $x_1, x_2 \in X$, таких, что $x_1 \neq x_2$. Тогда $f(x_1) \neq f(x_2)$, так как f – инъекция по условию. Обозначим $y_1 = f(x_1)$, $y_2 = f(x_2) \Rightarrow y_1 \neq y_2$, тогда $g(y_1) \neq g(y_2)$, так как g – инъекция. Обозначим $z_1 = g(y_1)$, $z_2 = g(y_2) \Rightarrow z_1 \neq z_2$.
Имеем, что
$h(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(y_1) = z_1$
$h(x_2) = (g \circ f)(x_2) = g(f(x_2)) = g(y_2) = z_2$
$z_1 \neq z_2 \Rightarrow h(x_1) \neq h(x_2) \Rightarrow$ инъекция.
Теорема доказана.

Теорема (о композиции сюръекций).
Если $f: X \to Y$ и $g: Y \to Z$ – сюръекции, то их композиция $(g \circ f)$ – сюръекция.
Коротко: композиция сюръекций является сюръекцией.

Доказательство.

Т.к. g - сюрьекция, то у $\forall z \in Z$ есть прообраз $y \in Y$, такой что $g(y)=z$.
Т.к. f - сюрьекция, то у $\forall y \in Y$ есть прообраз $x \in X$, такой что $f(x)=y$.
Имеем, что $z=g(y)=g(f(x))$, или $z=(g \circ f)(x)$. Т.е. у $\forall z \in Z$ имеется прообраз $x \in X$.

Теорема (о композиции биекций).
Композиция биекций является биекцией.

Доказательство.
Непосредственно вытекает из двух предыдущих теорем.

§3. БИНАРНАЯ ОПЕРАЦИЯ

Определение.
Бинарной операцией на непустом множестве M называется правило «$\circ$», которое *каждой упорядоченной паре* элементов a, b множества M сопоставляет (определяет) точно один элемент c этого же множества M.

Формально, бинарная операция «$\circ$» -- это отображение из декартового квадрата $M\times M$ в M, то есть $\circ : M\times M\to M$

Пример.
Операция сложения на множестве N натуральных чисел является бинарной, т.к. сумма двух натуральных чисел всегда является натуральным числом
Операция вычитания не является бинарной на множестве N натуральных чисел, т.к. разность двух натуральных чисел не всегда является натуральным числом, например $2-3=-1 \notin N$.
Однако на множестве Z вычитание является бинарной операцией, т.к. разность двух любых целых чисел снова целое число.

Определение.
Бинарная операция «$\circ$» на множестве M называется *ассоциативной*, если для любых 3-х элементов $a, b, c \in M$ выполняется $(a\circ b)\circ c = a\circ (b\circ c)$.

Определение.
Операция «$\circ$» на множестве M называется *коммутативной*, если для любых 2-х элементов $a, b \in M$ => $a\circ b = b\circ a$.

Следует отметить, что свойства ассоциативности и коммутативности независимы друг от друга.

Пример.
Рассмотрим операцию «*» на множестве Z (целые числа) $<Z, *>$, которая определена правилом $m * n = - m - n$. Она бинарна, т.к. для произвольных целых чисел m и n число ($-m-n$) тоже целое.
Операция «*» коммутативна, так как $n*m = - n - m = - m - n = m*n$
Проверим ассоциативность:
$(a\circ b)\circ c = (- b - a) * c = - c - (- b - a) = - c + b + a$
$a\circ (b\circ c) = a * (- c - b) = - (- c - b) - a = c + b - a$
$- c + b + a \neq c + b - a$, значит данная операция не ассоциативна.

§4. НЕЙТРАЛЬНЫЙ ЭЛЕМЕНТ

Определение.
Пусть имеется множество M, снабженное бинарной операцией «$\circ$». Коротко пишут $<M, \circ>$.
Элемент $e \in M$ называется *нейтральным* относительно бинарной операции «$\circ$», если для всех $a \in M$ выполняется $a\circ e = e\circ a = a$.

Предложение.
Если нейтральный элемент в $<M, \circ>$ существует, то он единственен. Иными словами, в $<M, \circ>$ может существовать не более одного нейтрального элемента.

Доказательство.
Предположим противное, а именно, что в $<M, \circ>$ имеется еще один нейтральный элемент e_1, который не равен e. Тогда имеем: $e_1 \circ e = e_1$, поскольку e - нейтральный элемент. С другой стороны, $e_1 \circ e = e$, так как e_1 тоже нейтральный. Следовательно $e_1 = e$. Противоречие.

Пример.
Рассмотрим множество *Q*, снабженное действием, выполняемым по правилу *a ○ b = (a·b)/2*. Эта операция является бинарной на *Q*, причем система <*Q*, ○ > обладает нейтральным элементом *e=2*.

Пример.

Является ли коммутативной или ассоциативной операция $a*b=\frac{ab}{a+b}$, заданная на множестве положительных действительных чисел? Имеется ли относительно этой операции нейтральный элемент?

Решение.

Проверим коммутативность: $a*b=\frac{ab}{a+b}=\frac{ba}{b+a}=b*a$, следовательно, операция * является коммутативной.
Проверим ассоциативность:

$$(a*b)*c=\frac{ab}{a+b}*c=\frac{\frac{ab}{a+b}c}{\frac{ab}{a+b}+c}=\frac{\frac{abc}{a+b}}{\frac{ab+c(a+b)}{a+b}}=\frac{abc}{ab+(a+b)c}=\frac{abc}{ab+ac+bc}.$$

$$a*(b*c)=a*\frac{bc}{b+c}=\frac{a\frac{bc}{b+c}}{a+\frac{bc}{b+c}}=\frac{\frac{abc}{b+c}}{\frac{a(b+c)+bc}{b+c}}=\frac{abc}{a(b+c)+bc}=\frac{abc}{ab+ac+bc}.$$

Таким образом, для любых элементов *a, b, c* $(a*b)*c=a*(b*c)$, следовательно, операция * ассоциативна.
Проверим существование нейтрального элемента.

$$a*e=\frac{ae}{a+e}=a,$$
$$ae=a(a+e),$$
$$ae=a^2+ae,$$
$$a^2=0.$$

Как видим, условие $a*e=a$ может выполняться только при $a=0$, а это означает, что на множестве положительных действительных чисел нейтрального элемента относительно операции * не существует.

Ответ: операция $a*b=\frac{ab}{a+b}$, заданная на множестве положительных действительных чисел, является коммутативной и ассоциативной, однако, относительно этой операции не существует нейтрального элемента.

Определение.
Множество *M*, снабженное бинарной операцией «○ », называется полугруппой, если операция «○ » - ассоциативна.
Таким образом <*M*, ○ > - полугруппа, если:
1) *(a ○ b) ○ c = a ○ (b ○ c), ∀ a, b, c є M*

Определение.
Полугруппа, в которой существует нейтральный элемент, называется моноидом.
Таким образом <*M*, ○ > - моноид, если:
1) *(a ○ b) ○ c = a ○ (b ○ c), ∀ a, b, c є M*
2) *∃ e є M: a ○ e = e ○ a = a, ∀ a є M*
Если *M* – конечное множество, то говорят, о конечном моноиде<*M*, ○ >.

$|M|$ - порядок моноида.

Пример.

Пусть M – произвольное множество. Обозначим через $\Omega(M)$ множество всевозможных отображений $M \to M$.

Несложно проверить, что $<\Omega(M), \circ>$ - моноид:

Действительно, композиция отображений подчиняется закону ассоциативности (см. теорему об ассоциативности композиции).

Кроме того, в $\Omega(M)$ имеется нейтральный элемент e_Ω – тождественное отображение.

Рассмотрим частный случай, когда M – конечное множество

$|M| = n < \infty$. В этом случае можно считать, что $M = \{1, 2, 3,\dots n\}$. Всякое такое отображение $f: M \to M$ на конечном множестве однозначно определяется указанием последовательности чисел $f(1), f(2), f(3),\dots f(n)$.

Всего таких отображений будет, очевидно n^n.

Пример.

Пусть $M = \{1, 2\}$

$|M| = n = 2$

Выпишем всевозможные отображения (всего их $2^2 = 4$, назовём их e, f, g, h):

	1	2
e	1	2
f	1	1
g	2	1
h	2	2

Вычислим композиции этих отображений:

$f \circ f = f$ $\quad 1 \to 1 \to 1$

$2 \to 1 \to 1$

$f \circ g = f$ $\quad 1 \to 2 \to 1$

$1 \to 1 \to 1$

$f \circ h = f$ $\quad 1 \to 2 \to 1$

$2 \to 2 \to 1$

$g \circ f = h$ $\quad 1 \to 1 \to 2$

$2 \to 1 \to 2$

$g \circ g = e$ $\quad 1 \to 2 \to 1$

$2 \to 1 \to 2$

$g \circ h = f$ $\quad 1 \to 2 \to 1$

$2 \to 2 \to 1$

$h \circ f = h$ $\quad 1 \to 1 \to 2$

$2 \to 1 \to 2$

$h \circ g = h$ $\quad 1 \to 2 \to 2$

$2 \to 1 \to 2$

$h \circ h = h$ $\quad 1 \to 2 \to 2$

$2 \to 2 \to 2$

Сведём вычисления в таблицу:

"○"	e	f	g	h
e	e	f	g	h
f	f	f	f	f
g	g	h	e	f
h	h	h	h	h

Видим, что $<\Omega(M), \circ>$ - моноид (причём некоммутативный).

Пример.
Обозначим $M_n(R)$ - множество квадратных матриц размера $n \times n$ с вещественным элементами. Рассмотрим $< M_n(R), +>$ с обычной операцией сложения матриц. Операция сложения матриц на этом множестве бинарная, ассоциативный закон верен (смотри алгебру матриц), нейтральный элемент имеется (нулевая матрица). Следовательно, это моноид, причем коммутативный.
$< M_n(R), \cdot >$ с обычной операцией умножения матриц доставляет пример некоммутативного моноида.

Пример.
Пусть M – множество, I - множество всех его подмножеств.
Рассмотрим на I операцию "U" объединения подмножеств.
$< I, U>$ -моноид с нейтральным элементом $e = \varnothing$
Аналогично, I с операцией пересечения подмножеств
$<I, \cap>$ - моноид с нейтральным элементом $e = M$.

Пример.
Обозначим $nZ = \{nk \mid k \in Z\}$ множество чисел, кратных n.
$<nZ, +>$ - моноид с нейтральным элементом $e = 0$

§5. СТЕПЕНИ

Пусть $< M, \circ >$ -- моноид, $a \in M$.
В моноиде выполняется закон ассоциативности, т.е. порядок расстановки скобок значения не имеет, поэтому для сокращения записи скобки можно опускать.

Удобно обозначить:

$$\underbrace{a \circ a \circ a \circ \ldots \circ a}_{n \text{ раз}} = a^n$$

Например,
$a \circ a = a^2$,
$(a \circ a) \circ a = a \circ (a \circ a) = a^2 \circ a = a^3$, и так далее.
Условимся, также, что
$a^1 = a$
$a^0 = e$

Теорема. (Свойства степеней в моноиде)
1) $a^m \circ a^n = a^{m+n}$
2) $(a^m)^n = a^{mn}$
$m, n \in N \cup \{0\}$

Доказательство.
1) $a^m \circ a^n$ (случай $m, n \in N$)

$$a^m \circ a^n = (\underbrace{a \circ a \circ a \circ \ldots \circ a}_{m \text{ раз}}) \circ (\underbrace{a \circ a \circ a \circ \ldots \circ a}_{n \text{ раз}}) = \underbrace{a \circ a \circ a \circ \ldots \circ a}_{m+n \text{ раз}}$$

Случай $m = 0$.

$$a^m \circ a^n = a^0 \circ \underbrace{a \circ a \circ a \circ \ldots \circ a}_{n\text{ раз}} = e \circ \underbrace{a \circ a \circ a \circ \ldots \circ a}_{n\text{ раз}} = a^n = a^{0+n} = a^{m+n}$$

Аналогично рассматриваются оставшиеся случаи $n = 0$ или $m = 0$, $n = 0$.

2) $(a^m)^n$ (случай $m, n \in N$)

$$(a^m)^n = (\underbrace{a \circ a \circ a \circ \ldots \circ a}_{m\text{ раз}})^n =$$

$$= \overbrace{(\underbrace{a \circ a \circ a \circ \ldots \circ a}_{m\text{ раз}}) \circ (\underbrace{a \circ a \circ a \circ \ldots \circ a}_{m\text{ раз}}) \circ \ldots \circ (\underbrace{a \circ a \circ a \circ \ldots \circ a}_{m\text{ раз}})}^{n\text{ раз}} = a^{m*n}$$

Случай $m = 0$ и/или $n = 0$ предоставляется для самостоятельного рассмотрения.

<u>Лемма (о коммутирующих элементах моноида).</u>

Если в моноиде $<M, \circ>$ элементы x и y коммутируют $x \circ y = y \circ x$, то тогда $(x \circ y)^n = x^n \circ y^n$.

<u>Доказательство.</u>

$$(x \circ y)^n = \underbrace{(x \circ y) \circ (x \circ y) \circ \ldots \circ (x \circ y)}_{n\text{ раз}} =$$

$$= x \circ (x \circ y) \circ \ldots \circ y = x \circ (y \circ x) \circ \ldots \circ y =$$

$$= (x \circ x \circ x \circ \ldots \circ x) \circ (y \circ y \circ y \circ \ldots \circ y) = x^n \circ y^n$$

<u>Пример.</u>

Рассмотрим моноид $<nZ, +>$. В этом случае бинарная операция «$\circ$» = $+$, а нейтральный элемент $e = 0$. Под степенью элемента х понимается

$x^n = x \circ x \circ x \circ \ldots \circ x = x + x + x + \ldots + x = nx$

Замечаем, что любая пара элементов $x, y \in nZ$ коммутирует. И видим, что

$(x \circ y)^n = n(x + y) = xn + ny = x^n \circ y^n$

§6. ОБРАТИМЫЕ ЭЛЕМЕНТЫ

<u>Определение.</u>

Пусть $<M, \circ>$ - моноид с нейтральным элементом е.

Элемент $a \in M$ называется обратимым, если $\exists\ a^{-1} \in M$ такой, что выполняется $a \circ a^{-1} = a^{-1} \circ a = e$.

(Элемент a^{-1} называют обратным к элементу a).

Здесь следует дать некие пояснения по поводу корректности приведенного выше определения. Назовем элемент $b_1 \in M$ левым обратным к $a \in M$, если $b_1 \circ a = e$, аналогично $b_2 \in M$ правый обратный к $a \in M$, если $a \circ b_2 = e$. Несложное рассуждение показывает, что в моноиде всякий левый обратный элемент одновременно является и правым обратным. Пусть b левый обратный к a, т.е. $b\circ a = e$. Обозначим $a\circ b=T$. Умножим это равенство слева на b, тогда $b\circ (a\circ b)=b\circ T \Rightarrow (b\circ a)\circ b=b\circ T \Rightarrow e\circ b=b\circ T \Rightarrow b=b\circ T$. Отсюда имеем $T=e$, т.е. $a\circ b=e$.

<u>Лемма.</u>

Если элемент a^{-1} $\exists$, то он единственен.

<u>Доказательство.</u>

Пусть b – элемент, обратный к a.

Предположим противное – есть еще один обратный к a. Обозначим его b_1, причем $b \neq b_1$.

Тогда

$b_1 = e \circ b_1 = (b \circ a) \circ b_1 = b \circ (a \circ b_1) = b \circ e = b$

Противоречие.

Следовательно, $b = b_1$, b – единственный.

Лемма доказана.

Пример.

Множество *M* чисел вида *M={a+b*√5 | *a,b*∈*M}* с операцией обычного умножения обладает нейтральным элементом *e*=1+0√5, и является моноидом. В этом моноиде элемент 2+√5 обратим (обратный элемент равен -2+√5), а элемент 5-2√5 необратим, т.к обратный для него элемент 1+(2/5)√5 не принадлежит *M*.

§7. ПЕРЕСТАНОВКИ И ПОДСТАНОВКИ

Пусть *M* – конечное множество, содержащее *n* элементов.

Природа элементов этого множества не важна, так как оно конечно, и его элементы можно занумеровать конечным числом натуральных чисел и вместо *M* рассмотреть *M´* (числовое множество) такое, что *M´ = {1, 2, 3,… n}.*

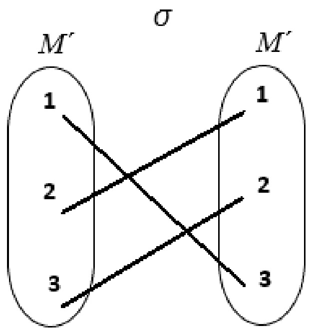
|M|= n.

Определение.

Рассмотрим биекцию *σ: M´ → M´*. Такая биекция называется *подстановкой*.

Пример.

M´ = {1, 2, 3}.



σ(1) = 3,   σ(2) = 1,   σ(3) = 2

Или в общем случае

$\sigma(k) = i_k$, $k = 1, 2, 3$

Рассмотрим еще один пример.

Имеется 3 предмета, занумерованных числами от 1 до 3 . Поменяем их местами и получим новое расположение, называемое *перестановкой*.

M´ = {1, 2, 3}.

1) было 1 2 3

2) стало 2 3 1

$$\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$$

Таким образом, мы выполнили перестановку.

Заметим, что переставляя предметы мы выполнили подстановку, между перестановками и подстановками можно установить взаимно однозначное соответствие, и эти термины употреблять как синонимы.

Множество всех подстановок *n* - элементов принято обозначать S_n.

Подстановка $\sigma \in S_n$ может быть записана в виде таблицы

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

в первой строке выписаны в произвольном порядке числа $1,2,\dots,n$, а во второй строке – их образы, другими словами $\sigma(i_k) = j_k$

Теорема о числе перестановок n-элементного множества.

Если *M* – конечное множество, причем количество элементов в нем равно *n*, то тогда число перестановок его элементов равно *n!*

Доказательство.
Даны элементы 1, 2, 3, … n, и имеется n свободных ячеек для них.

		. . .	

В 1-ю ячейку можно положить любой из n элементов. Это можно сделать n способами. Во 2-ю ячейку можно положить следующий элемент $n - 1$ способами, в 3-ю – $n - 2$ способами, и так далее. В n-тую ячейку можно положить только 1 оставшийся элемент 1 способом.
Таким образом, общее количество способов:
$n(n - 1)(n - 2)\ldots 1 = n!$

Пример.
Пусть множество M содержит 3 элемента. Множество S_3 всевозможных подстановок трех элементов содержит $|S_3|=3!=6$ подстановок. На S_3 можно ввести операцию «$\circ$» композиции (т.к. каждая подстановка есть отображение). Например,

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\circ\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

(первой выполняем подстановку записанную справа)
Эта операция, очевидно будет бинарной (композиция биекций есть биекция из M в M), ассоциативной (см. теорему об ассоциативности композиции отображений), кроме того, имеется нейтральный элемент - тождественное отображение, оставляющее все элементы M на месте, т.е. подстановка

$$e=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$$

Далее, видим, что для всякой подстановки a имеется обратная a^{-1}, например, если

$$a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\ \text{то}\quad a^{-1}=\begin{pmatrix}2 & 3 & 1\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

СПИСОК ИССПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Кострикин И.А. Введение в алгебру. – М.: Физматлит, 2001.

2. Ерусалимский, Я.М. Дискретная математика: теория, задачи, приложения. – М.: Вузовская книга, 2011.

3. Алексеев В.Б. Теорема Абеля в задачах и решениях. – М.: Наука, 1976.

4. Нечаев В.А. Задачник практикум по алгебре. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения – Просвещение, 1983.

5. Б.Л. Ван дер Варден. Алгебра. – М.: Наука, 1976