Конспекты лекций по алгебре-геометрии

Ведёт: Верников Борис Муневич
перенесено в электронный формат Ширкуновым А.

2024-2025 учебный год, первый семестр

1 Введение в алгебру

1.1 Множества и отображения

Множество - неопределяемое понятие, которое понимается как совокупность произвольного числа объектов, выделенная исходя из какого-то признака и рассматриваемая как единое целое. Понятие множества внутренне противоречиво (см. *парадокс Рассела*), поэтому мы пользуемся таким наивным "определением".

В работе с множествами используются **кванторы** – специальные символы для описания логики рассуждений.

Например, $\{x \in \mathbb{Z} \mid x = 2n+1\}$ читается как 'множество всех целых нечётных x', где в фигурных скобках объявляется x, а после вертикальной черты – условие вхождения x во множество.

Свойства логических операций над множествами: коммутативность, ассоциативность, дистрибутивность, идемпотентность и проч.

$A \cup B = B \cup A;\ A \cap B = B \cap A$ – *коммутативность*
$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ – *дистрибутивность отн. объединения*
$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ – *дистрибутивность отн. пересечения*
$(A \cup B) \cup C = A \cup (B \cup C);\ (A \cap B) \cap C = A \cap (B \cap C)$ – *ассоциатив-ть*
$A \cup A = A;\ A \cap A = A$ – *идемпотентность*
$(A \cup B) \cap A = A;\ (A \cap B) \cup A = A$ – *законы поглощения*
$\overline{\overline{A}} = A$ – *закон снятия двойного отрицания*
$\overline{A \cup B} = \overline{A} \cap \overline{B};\ \overline{A \cap B} = \overline{A} \cup \overline{B}$ – *законы де-Моргана*
$A \cup \overline{A} = U$ – *определение универсального множества*
$A \setminus B = A \cap \overline{B}$ – *определение разности множеств*

Важно отметить, что у операций объединения, пересечения и разности множеств одинаковый приоритет. Поэтому при работе с множествами нужно отделять части выражения скобками.

Декартовым произведением множеств A и B называется множество $A \times B$, состоящее из всех упорядоченных пар (a, b) таких, что $a \in A,\ b \in B$. Важно помнить, что декартово произведение некоммутативно и неассоциативно.

$$A_1 \times A_2 \times \ldots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}$$

A^n – **декартова степень** множества, определяется как множество всех кортежей длины n, состоящих из элементов данного множества.

1.2 Отображение

Отображением f из A в B называется подмножество f множества $A \times B$, которое определеяется следующим образом: $\forall x \in A,\ \exists! y \in B : (x, y) \in f$. Если множества A и B состоят из чисел, то f называется **функцией**.

Форма записи: $f : A \to B$ – отображение из A в B. Запись $(x, y) \in f$ часто обозначают как $y = f(x)$, где $f(x)$ – **образ** элемента x, а x – **прообраз** элемента $f(x)$ при отображении f.

Если α – отображение из A в B, а $X \subseteq \alpha$, то **ограничением** α на подмножество X называется отображение из X в B, обозначаемое через ${}^a\mid_x$ и определяемое правилом ${}^a\mid_x (x) = \alpha(x)$ для всякого $x \in X$.

Отображение f из A в B называется:

- взаимно однозначным отображением (или **инъективным** отображением), если для любых $x, y \in A$ из того, что $x \neq y$ следует, что $f(x) \neq f(y)$, то есть образы двух различных элементов различны
- отображеним A на B (или **сюрьективным** отображением), если $\forall y \in B\ \exists x \in A : f(x) = y$, то есть каждый элемент из B имеет прообраз.
- взаимно однозначным соответствием (или **биективным** отображением), если f инъективно и сюрьективно.

Пусть f – отображение из A в B, а g – отображение из B в C. **Произведением** (а также композицией или суперпозицией) отображений f и g называется отображение h из A в C, задаваемое правилом $h(x) = g(f(x))$. Часто обозначается через $fg(x)$.

Замечания: произведение отображений ассоциативно, но некоммутативно. Произведение биективных отображений биективно. Произведение инъективных отображений инъективно, а произведение сюрьективных отображений сюрьективно.

Отображение f из множества A в себя, задаваемое правилом $f(x) = x$ называется **тождественным**, которые мы будем обозначать буквой ϵ. Пусть f – отображение из A в B. Отображение g из $f(A)$ в A называется **обратным** к f, если отображение fg является тождественным. Обратное отображение обозначается как f^{-1}.

Критерий существования обратного отображения: отображение, обратное к f, существует тогда и только тогда, когда f – инъекция.

Доказательство: предположим, что отображение, обратное к f, существует. Если при этом $f(x_1) = f(x_2)$ для некоторых $x_1, x_2 \in A$, то:

$$x_1 = \epsilon(x_1) = (ff^{-1})(x_1) = f^{-1}(f(x_1) = f^{-1}(f(x_2)) = (ff^{-1})(x_2) = x_2$$

Таким образом, $x_1 = x_2$, т.е отображение f инъективно. Необходимость доказана.

Докажем и достаточность: $\forall y \in f(A)\ \exists x \in A : f(x) = y$. По условию f инъективно $\Rightarrow$ элемент x определён однозначно. Это позволяет определить $g : f(A) \to A$ правилом $g(y) = x$. Если $x \in A$, то $(fg)(x) = g(f(x)) = g(y) = x$, т.е $fg = \epsilon$. Следовательно, $g = f^{-1}$, т.е f^{-1} существует.

Замечание: если f – биективное отображение из A в B, то f^{-1} – биективное отображение из B в A.

Свойства обратного отображения (A, B, C – множества $f : A \to B$, $g : B \to C$):

- Если существует отображение f^{-1}, то существует $(f^{-1})^{-1} = f$.
- Если существуют отображения f^{-1} и g^{-1}, то существует $(fg)^{-1} = g^{-1}f^{-1}$.

1.3 Мощность конечного множества

Множества A и B называют **равномощными**, если существует биективное отображение из A на B.

Конечные множества A и B равномощны тогда и только тогда, когда они содержат одно и то же число элементов *(доказывается по свойству биекции)*.

Число элементов конечного множества S называется **мощностью** этого множества и обозначается через $|S|$.

Если $S_1, S_2, \ldots, S_n$ – конечные множества и $|S_i| = k$ для всех $i = 1, 2, \ldots, n$, то $|S_1 \times S_2 \times \ldots \times S_n| = k_1 \cdot k_2 \cdot \ldots \cdot k_n$.

Доказательство проведём индукцей по n. При $n = 1$ доказываемое очевидно. Если $n > 1$, $S_n = \{x_1, x_2, \ldots, x_{k_n}\}$. Для всякого $i = 1, 2, \ldots, k_n$ обозначим через T_i множество всех кортежей из множества $S_1 \times S_2 \times \ldots \times S_n$, у которых последняя компонента равна x_i. Ясно, что $S_1 \times S_2 \times \ldots \times S_n = T_1 \cup T_2 \cup \ldots \cup T_{k_n}$ и множества $T_1, T_2, \ldots, T_{k_n}$ попарно пересекаются по пустому множеству. Следовательно, $|S_1 \times S_2 \times \ldots \times S_n| = |T_1| + |T_2| + \ldots + |T_{k_n}|$. Очевидно, что для всякого $i = 1, 2, \ldots, k_n$ существует биекция из T_i в $S_1 \times S_2 \times \ldots \times S_{n-1}$, которая кортежу $(y_1, y_2, \ldots, y_{n-1}, x_i) \in T_i$ ставит в соответствие кортеж $(y_1, y_2, \ldots, y_{n-1}) \in S_1 \times S_2 \times \ldots \times S_{n-1}$. Следовательно, $|T_i| = |S_1 \times S_2 \times \ldots \times S_{n-1}$, и потому $|S_1 \times S_2 \times \ldots \times S_n = k_n \cdot |S_1 \times S_2 \times \ldots \times S_{n-1}|$. По предположению индукции $|S_1 \times S_2 \times \ldots \times S_{n-1}| = k_1 \cdot k_2 \cdot \ldots \cdot k_{n-1}$. Следовательно, $|S_1 \times S_2 \times \ldots \times S_n| = k_1 \cdot k2 \cdot \ldots \cdot k_{n-1} \cdot k_n$, что и требовалось доказать *(советую вдумчиво подумать над д-вом, оно очень симпатичное)*.

Следствие: если S – конечное множество и $|S| = k$, а n – натуральное число, то $|S^n| = k^n$.

1.4 Булеан множества

Булеаном множества S называют множество всех подмножеств множества S. Булеан обозначается по-разному: $B(S), P(S), 2^S$.

Если S – конечное множество и $|S| = n$, то $|B(S)| = 2^n$.

Доказательство проведём индукцией по n. База индукции: если $n = 0$, то $S = \emptyset$ и $|B(S)| = 1 = 2^0 = 2^{|S|}$.

Шаг индукции: пусть $n > 0$. Зафиксируем произвольный элемент $x \in S$ и положим $S' = S \setminus \{x\}$. Тогда $|S'| = n - 1$ и, по предположению индукции, $|B(S')| = 2^{|S'|} = s^{n-1}$. Все подмножества множества S можно разбить на два типа: те, которые не содержат x, и те, которые содержат x. Любое подмножество множества S, не содержащее x, содержится в S'. Число таких подмножеств равно мощности булеана множества S', т.е 2^{n-1}. Далее, любое подмножество множества S, содержащее x, получатеся из какого-то подмножества множества S' путём прибавления к нему x. Число таких подмножеств равно числу подмножеств, содержащих x, т.е 2^{n-1}. Следовательно, общее число подмножеств множества S равно $2^{n-1} + 2^{n-1} = 2^n$.

2 Элементы комбинаторики

2.1 Рамещения и перестановки

Пусть X – непустое конечное множество из n элементов и $k \leq n$. **Размещением** из n элементов по k элементов называется произвольный упорядоченный набор из k попарно различных элементов множества X. Число размещений из n элементов по k элементов обозначается через A_n^k.

$$A_n^k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

Пусть X – непустое конечное множество из n элементов. **Перестановкой** на множестве X называется размещение из n элементов на этом множестве. Число перестановок из n элементов обозначается через P_n.

$$P_n = A_n^n = n!$$

Говорят, что перестановка $(j_1, j_2, \ldots, j_n)$ получена из $(i_1, i_2, \ldots, i_n)$ **транспозицией** символов i_k и i_m, если $j_k = i_m, j_m = i_k, j_r = i_r$ для всех $r \in \{1, 2, \ldots, n\}$, отличных от k и m. Транспозиция называется **смежной**, если $k = m + 1$ или $m = k + 1$.

Говорят, что символы i_k и i_m образуют **инверсию** в перест-ке $(i_1, i_2, \ldots, i_n)$ множества $\{1, 2, \ldots, n\}$, если $k < m$, а $i_k > i_m$. Число инверсий в перестановке обозначается через $I(i_1, i_2, \ldots, i_n)$. Перестановка называется **чётной**, если число инверсий чётно, и **нечётной** в противном случае.

Если перестановка $(j_1, j_2, \ldots, j_n)$ получена из перестановки $(i_1, i_2, \ldots, i_n)$ транспозицией, то чётности этих перестановок различны.

Все перестановки на множестве $\{1, 2, \ldots, n\}$, где $n > 1$, можно упорядочить так, что каждая следующая перестановка будет получаться из предыдущей транспозицией пары символов. При этом в качестве первой перестановки можно взять любую на данном множестве.

Если $n \geq 2$, то как число чётных, так и число нечётных перестановок на множестве $\{1, 2 \ldots, n\}$ равно $\frac{n!}{2}$.

2.2 Сочетания

Пусть X – непустое конечное множество из n элементов и $k \leq n$. Сочетанием из n элементов по k элементов на этом множестве называется любое подмножество множества X, состоящее из k элементов. Число сочетаний из n по k обозначается через C_n^k. Для удобства вычислений будем считать, что $C_n^0 = 1$.

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Числа вида C_n^k называются **биномиальными коэффициентами**.

Свойства биномиальных коэффициентов:

- $C_n^k = C_n^{n-k}$
- $C_n^{k-1} + C_n^k = C_{n+1}^k$
- $C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$

Пусть n – произвольное натуральное число. Следующая формула называется биноминальной формулой Ньютона или просто **биномом Ньютона**.

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^{n-k} y^k$$

Эта формула объясняет термин "биномиальные коэффициенты": числа вида C_n^k есть коэффициенты при одночленах в биноме Ньютона.