Глава I. Введение. §1. Метод математической индукции. Множества и операции над ними

А. Я. Овсянников

Уральский федеральный университет
Институт естественных наук и математики
Департамент математики, механики и компьютерных наук

Основы алгебры для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Краткое описание курса

Курс основы алгебры изучается в течение 1-го семестра. Он включает введение (элементы теории множеств и комбинаторики, начальные сведения о соответствиях, отображениях и отношениях, понятие об алгебраических операциях и основных типах алгебраических систем – группах, кольцах и полях), системы линейных алгебраических уравнений, матрицы и определители, комплексные числа и многочлены. Список литературы приведен на следующем слайде.

По курсу читаются лекции и проводятся практические занятия.
Для записи лекций и практических занятий нужно завести две ОТДЕЛЬНЫЕ тетради. Ни в коем случае не следует записывать лекции и практические занятия подряд друг за другом в одной тетради!
На практических занятиях решаются задачи и задаются домашние задания. Их можно записывать в одной тетради.

Литература

1. Курош А.Г. Курс высшей алгебры. Любое издание.
2. Кострикин А.И. Основы алгебры. Любое издание.
3. Фаддеев Д.К. Лекции по алгебре. Любое издание.
4. Задачник по алгебре и геометрии для студентов первого курса. Изд-во УрГУ, Екатеринбург, 2004; 2010 (2-е изд).

Книги [1-3] — университетские учебники, [2] и [3] — учебники повышенного уровня. Задачник [4] используется на практических занятиях. Он доступен в виде pdf файла в закладке "Книги"страницы А.Я.Овсянникова на сайте кафедры алгебры и фундаментальной информатики по адресу:
kadm.kmath.ru Преподаватели Овсянников

О слайдах

Изложение курса в виде набора слайдов разбито на главы, главы — на параграфы. Главы нумеруются римскими цифрами, параграфы внутри главы — арабскими. В закладке "Лекции по курсам"страницы А.Я.Овсянникова на сайте кафедры алгебры и фундаментальной информатики эти слайды уже выложены.

Довольно часто приходится делать ссылки на утверждения, доказанные ранее. Эти ссылки делаются так: <утверждение> сл. n §k гл. G означает ссылку на <утверждение> (теорему, предложение, следствие), сформулированное на слайде номер n §k главы G. Аналогично делаются ссылки на выделенные формулы. Если слайд, на который делается ссылка, находится в том же параграфе (главе), то номер параграфе (главы) не указывается.

Определяемые понятия выделяются *курсивом и цветом*. Начало и конец доказательства выделяются символами $\Downarrow$ и $\Uparrow$ соответственно.

Числовые множества

Множество всех натуральных чисел обозначается через $\mathbb{N}$:

$$\mathbb{N} = \{1, 2, \ldots\}.$$

Множество всех целых чисел обозначается через $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Множество всех рациональных чисел обозначается через $\mathbb{Q}$:

$$\mathbb{Q} = \left\{ \frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Множество всех действительных (или вещественных) чисел обозначается через $\mathbb{R}$. Его строгое определение дается в курсе математического анализа.

На всех указанных множествах определены арифметические операции сложения и умножения, а также отношение порядка $\leq$.

Принцип математической индукции

Некоторые утверждения включают в себя переменные величины. Тогда можно сказать, что утверждение зависит от параметра. Например, утверждение "запись в десятичной системе счисления квадрата натурального числа n заканчивается цифрой c"(где $c \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) зависит от параметров n и c.

Пусть $\mathcal{A}(n)$ — некоторое утверждение, зависящее от натурального параметра n и имеющее смысл для всех натуральных чисел n. Если $\mathcal{A}(1)$ выполняется (база индукции) и для любого натурального числа n из того, что $\mathcal{A}(n)$ выполняется, следует, что $\mathcal{A}(n+1)$ выполняется (шаг индукции), то $\mathcal{A}(m)$ справедливо для всех натуральных чисел m.

$\Downarrow$ Для доказательства обозначим через M множество всех натуральных чисел, для которых справедливо утверждение $\mathcal{A}$:
$M = \{n \in \mathbb{N} | \mathcal{A}(n)$ истинно$\}$.
Тогда $1 \in M$ согласно базе индукции и для любого $n \in M$ также $n+1 \in M$ в соответствии с шагом индукции. Следовательно, $M = \mathbb{N}$ (это аксиома индукции).$\Uparrow$

Пример

Для натурального числа n по определению $n! = 1 \cdot 2 \cdot \ldots \cdot n$ ($n!$ читается эн факториал). По определению $1! = 1$. Полезное соглашение: $0! = 1$. Легко видеть, что $(n+1) \cdot n! = (n+1)!$.

Утверждение

Доказать, что для любого натурального числа n имеет место формула

$$1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n! = (n+1)! - 1.$$

$\Downarrow$Утверждение $\mathcal{A}(n)$ состоит в том, что выполняется указанное в условии равенство. Проверяем его истинность при $n = 1$ (база индукции):
$1 \cdot 1! = 2! - 1$ — верное равенство.
Пусть утверждение выполняется для натурального числа n. Докажем его справедливость для числа $n+1$:
$1 \cdot 1! + 2 \cdot 2! + \ldots + (n+1) \cdot (n+1)! = (1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n!) + (n+1) \cdot (n+1)! =$
$(n+1)! - 1 + (n+2-1) \cdot (n+1)! = (n+1)! - 1 + (n+2)! - (n+1)! = (n+2)! - 1.$
Таким образом, $1 \cdot 1! + 2 \cdot 2! + \ldots + (n+1) \cdot (n+1)! = (n+2)! - 1$. Шаг индукции доказан. $\Uparrow$

Принцип полной математической индукции

Теорема

Пусть $\mathcal{A}(n)$ — некоторое утверждение, зависящее от натурального параметра n и имеющее смысл для всех натуральных чисел n таких что $n \geq n_0$ при фиксированном $n_0 \in \mathbb{N}$. Если $\mathcal{A}(n_0)$ выполняется (база индукции) и для любого натурального числа $n > n_0$ из того, что $\mathcal{A}(k)$ выполняется для всех натуральных чисел k таких, что $n_0 \leq k < n$, следует, что $\mathcal{A}(n)$ выполняется (шаг индукции), то $\mathcal{A}(m)$ справедливо для всех натуральных чисел $m \geq n_0$.

$\Downarrow$ Пусть M — множество всех натуральных чисел, для которых выполняется утверждение $\mathcal{A}$: $M = \{n \in \mathbb{N} | \mathcal{A}(n)$ истинно$\}$.
Предположим, от противного, что $M \neq \{n \in \mathbb{N} | n \geq n_0\}$. Тогда существует наименьшее натуральное число m, для которого $\mathcal{A}(m)$ не выполняется.
Так как $\mathcal{A}(n_0)$ выполняется, имеем $m > n_0$.
По выбору числа m для любого натурального k такого что $n_0 \leq k < m$ утверждение $\mathcal{A}(k)$ выполняется. Получаем противоречие: согласно шагу индукции $\mathcal{A}(m)$ должно выполняться. $\Uparrow$

Условие

Доказать, что для любого натурального $n > 4$ справедливо неравенство $2^n > n^2$.

$\Downarrow$Проверяем базу индукции ($n = 5$): $2^5 = 32 > 25 = 5^2$. При $n = 5$ утверждение справедливо.
Доказываем шаг индукции. Предположим, что для всех натуральных чисел $4 < k < n$ утверждение доказано, т.е. $2^k > k^2$. Тогда $2^{n-1} > (n-1)^2$,откуда $2^n = 2 \cdot 2^{n-1} > 2(n-1)^2$. Убедимся, что $2(n-1)^2 > n^2$. В самом деле, $2(n-1)^2 - n^2 = n^2 - 4n + 2$. Квадратный трехчлен $x^2 - 4x + 2$ имеет корни $2 \pm \sqrt{2}$, и при $x > 2 + \sqrt{2}$ этот трехчлен положителен. Так как $4 > 2 + \sqrt{2}$, при всех $n > 4$ выполняется $n^2 - 4n + 2 > 0$, что завершает доказательство.$\Uparrow$

Понятие множества

Это фундаментальное математическое понятие, которое в данном курсе строго не определяется. Мы используем интуитивное представление о множестве как совокупности объектов, объединяемых некоторым свойством. Нужно отметить, что не всякая мыслимая совокупность объектов является множеством. Строгое аксиоматическое построение теории множеств весьма сложно и не используется в дальнейшем. Множества состоят из элементов. Понятие элемента также строго не определяется.

Запись $x \in A$ означает, что x является элементом множества A и читается x принадлежит A.

Для обозначения множеств через элементы используются фигурные скобки. Так, $M = \{a_1, \ldots, a_n\}$ — множество из n (различных) элементов $a_1, \ldots, a_n$, а $S = \{x \in T | \mathcal{P}(x)\}$ — множество всех таких элементов множества T, для которых справедливо утверждение $\mathcal{P}(x)$. Это утверждение может быть произвольным.

Пустое множество по определению не содержит ни одного элемента. Оно обозначается символом $\emptyset$. Пример пустого множества: $\{x \in \mathbb{N} | 2x = 3\} = \emptyset$. Это значит, что уравнение $2x = 3$ не имеет решений в множестве натуральных чисел.

Определение подмножества

Множество A называется *подмножеством* множества B, если каждый элемент множества A принадлежит множеству B.

Обозначение: $A \subseteq B$ (читается A включается в B). Важно не путать символы $\subseteq$ и $\in$. Пустое множество по определению считается подмножеством любого множества.
Примеры включения множеств:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}. \tag{1}$$

Определение равенства множеств

Множества A и B называются *равными*, если $A \subseteq B$ и $B \subseteq A$.

Это означает, что равные множества имеют одни и те же элементы.

Пример: $\{2, 3\} = \{x \in \mathbb{R} | x^2 - 5x + 6 = 0\}$.

Включение $A \subseteq B$ называется *строгим* (и обозначается $A \subset B$), если $A \neq B$, т.е. существует элемент множества B, не принадлежащий множеству A. Все включения в (1) являются строгими.

Операции над множествами: объединение и пересечение

Будем предполагать, что все рассматриваемые множества являются подмножествами одного универсального множества, которое обозначим через U.

Объединение множеств

Объединением множеств A и B называется множество, каждый элемент которого является элементом множества A или элементом множества B (возможно, элементом каждого множества).

Обозначение: $A \cup B$. Запись определения:
$A \cup B = \{x \in U | x \in A \text{ или } x \in B\}$.

Пересечение множеств

Пересечением множеств A и B называется множество, каждый элемент которого является элементом и множества A и множества B.

Обозначение: $A \cap B$. Запись определения: $A \cap B = \{x \in U | x \in A \text{ и } x \in B\}$.

Из определений следует, что $A \cap B \subseteq A \cup B$. Если $A \neq \emptyset$ или $B \neq \emptyset$, то $A \cup B \neq \emptyset$; если $A \neq \emptyset$ и $B \neq \emptyset$, то возможно, что $A \cap B = \emptyset$.

Операции над множествами: разность и дополнение

Разность

Разностью множеств A и B называется множество из всех элементов множеств A, которые не принадлежат B.

Обозначение: $A\backslash B$. Полное название: теоретико-множественная разность.

Дополнение

Дополнением множества A называется множество всех элементов универсального множества, каждый элемент которого не принадлежит A.

Обозначение: $\overline{A}$. Из определений следует, что $\overline{A} = U\backslash A$.

Симметрическая разность

Симметрической разностью множеств A и B называется множество $(A\backslash B) \cup (B\backslash A)$.

Обозначение: $A\triangle B$.

Законы алгебры множеств

Напомним, что через U обозначается универсальное множество.
Для любых множеств X, Y, Z справедливы равенства:
1. Законы идемпотентности. $X \cap X = X$, $X \cup X = X$.
2. Законы коммутативности. $X \cap Y = Y \cap X$, $X \cup Y = Y \cup X$.
3. Законы ассоциативности. $(X \cap Y) \cap Z = X \cap (Y \cap Z)$,
$(X \cup Y) \cup Z = X \cup (Y \cup Z)$.
4. Законы поглощения. $(X \cap Y) \cup X = X$, $(X \cup Y) \cap X = X$.
5. Законы дистрибутивности. $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$,
$(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$.
6. Законы двойственности. $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$, $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$.
7. Закон двойного дополнения. $\overline{\overline{X}} = X$.
8. $X \cup \overline{X} = U$, $X \cap \overline{X} = \emptyset$.
9. $X \cap U = X$, $X \cup U = U$.
10. $X \cap \emptyset = \emptyset$, $X \cup \emptyset = X$.
11. $\overline{U} = \emptyset$, $\overline{\emptyset} = U$.

Доказательства этих равенств проводятся с помощью понятия равенства множеств (сл. 10).

Доказательство первого закона дистрибутивности

$\Downarrow$Докажем, что $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$. Для этого по определению нужно доказать два противоположных включения: $(X \cap Y) \cup Z \subseteq (X \cup Z) \cap (Y \cup Z)$ и $(X \cup Z) \cap (Y \cup Z) \subseteq (X \cap Y) \cup Z$.
Убедимся, что $(X \cap Y) \cup Z \subseteq (X \cup Z) \cap (Y \cup Z)$. Для этого возьмем произвольный элемент $a \in (X \cap Y) \cup Z$. По определению объединения множеств $a \in (X \cap Y)$ или $a \in Z$.
Если $a \in (X \cap Y)$, то по определению пересечения множеств $a \in X$ и $a \in Y$, откуда по определению объединения получаем $a \in X \cup Z$ и $a \in Y \cup Z$. Следовательно, по определению пересечения $a \in (X \cup Z) \cap (Y \cup Z)$.
Если $a \in Z$, по определению объединения снова получаем $a \in X \cup Z$ и $a \in Y \cup Z$, откуда следует $a \in (X \cup Z) \cap (Y \cup Z)$.
Мы доказали, что $(X \cap Y) \cup Z \subseteq (X \cup Z) \cap (Y \cup Z)$.

Окончание доказательства первого закона дистрибутивности

Теперь убедимся, что $(X \cup Z) \cap (Y \cup Z) \subseteq (X \cap Y) \cup Z$. Для этого возьмем произвольный элемент $a \in (X \cup Z) \cap (Y \cup Z)$. Для него имеются две возможности.
1. $a \in Z$. Тогда по определению объединения имеем $a \in (X \cap Y) \cup Z$.
2. $a \notin Z$. Так как $a \in (X \cup Z) \cap (Y \cup Z)$, по определению пересечения получаем $a \in X \cup Z$ и $a \in Y \cup Z$. Из того, что $a \in X \cup Z$ и $a \notin Z$ по определению объединения следует, что $a \in X$. Аналогично заключаем, что $a \in Y$. Таким образом, $a \in (X \cap Y)$ и потому $a \in (X \cap Y) \cup Z$.
Мы доказали, что $(X \cup Z) \cap (Y \cup Z) \subseteq (X \cap Y) \cup Z$. Тем самым равенство $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$ доказано.$\Uparrow$

Доказать, что $\overline{(C \cap \overline{A}) \cap (C \cap \overline{B})} = A \cup B \cup \overline{C}$.

Используя законы алгебры множеств, получаем $\overline{(C \cap \overline{A}) \cap (C \cap \overline{B})} = \overline{(C \cap \overline{A})} \cup \overline{(C \cap \overline{B})} = \overline{C} \cup \overline{\overline{A}} \cup \overline{C} \cup \overline{\overline{B}} = \overline{C} \cup A \cup \overline{C} \cup B = A \cup B \cup \overline{C}$.

Упростить выражение $((\overline{A} \cap B) \cup (\overline{A} \cap C) \cup (B \cap C)) \cup \overline{(\overline{A} \cap B \cap C)}$.

$(\overline{A} \cap B) \cup (\overline{A} \cap C) \cup (B \cap C) \cup \overline{(\overline{A} \cap B \cap C)} = (\overline{A} \cap B) \cup (\overline{A} \cap C) \cup (B \cap C) \cup \overline{\overline{A}} \cup \overline{B \cap C} = (\overline{A} \cap B) \cup (\overline{A} \cap C) \cup A \cup (B \cap C) \cup \overline{B \cap C} = (\overline{A} \cap B) \cup (\overline{A} \cap C) \cup A \cup U = U$.

Декартово произведение двух множеств

Пусть X, Y — множества. *Упорядоченная пара* (x, y) состоит из элементов $x \in X$, $y \in Y$. Ее можно определить как множество $\{x, \{x, y\}\}$. По определению $(x_1, y_1) = (x_2, y_2)$ тогда и только тогда, когда $x_1 = x_2$ и $y_1 = y_2$.

Определение

Декартовым произведением множеств X и Y называется множество всех упорядоченных пар, в которых первый элемент принадлежит множеству X, а второй — множеству Y.

Обозначение: $X \times Y$. Таким образом, $X \times Y = \{(x, y) | x \in X, y \in Y\}$.

Например, $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

Свойства декартова произведения.

1. $X \times \emptyset = \emptyset \times X = \emptyset$.
2. $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$; $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$.
3. $(Y \cap Z) \times X = (Y \times X) \cap (Z \times X)$; $(Y \cup Z) \times X = (Y \times X) \cup (Z \times X)$.
4. $X \times (Y \setminus Z) = (X \times Y) \setminus (X \times Z)$; $(Y \setminus Z) \times X = (Y \times X) \setminus (Z \times X)$.

Декартово произведение нескольких множеств

Пусть $X_1, X_2, \ldots, X_n$ — множества, n — натуральное число. *Кортежем* $(x_1, x_2, \ldots, x_n)$ называется упорядоченный набор элементов $x_i \in X_i$, $i = 1, 2, \ldots, n$; число n называется *длиной* этого кортежа.
Кортеж $(x_1, x_2, \ldots, x_n)$ можно определить как множество $\{x_1, \{x_2, \{x_3, \ldots \{x_{n-1}, x_n\} \ldots\}$.
По определению два кортежа $(x_1, x_2, \ldots, x_n)$ и $(y_1, y_2, \ldots, y_k)$ *равны* тогда и только тогда, когда $n = k$ и $x_i = y_i$ при $i = 1, 2, \ldots, n$.

...

Декартовым произведением множеств $X_1, X_2, \ldots, X_n$ называется множество всех кортежей длины n, в которых i-й элемент принадлежит множеству X_i при $i = 1, 2, \ldots, n$.

Обозначение: $X_1 \times X_2 \times \ldots \times X_n$. Таким образом,
$X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) | x_i \in X_i, i = 1, 2, \ldots, n\}$.

Пример. Пусть $X_1 = \{a, b\}$, $X_2 = \{1, 2, 3\}$, $X_3 = \{\alpha, \beta\}$. Тогда

$$X_1 \times X_2 \times X_3 = \{(a,1,\alpha), (b,1,\alpha), (a,2,\alpha), (b,2,\alpha), (a,3,\alpha), (b,3,\alpha),$$
$$(a,1,\beta), (b,1,\beta), (a,2,\beta), (b,2,\beta), (a,3,\beta), (b,3,\beta)\}.$$

Декартова степень множества

Если все множества $X_1, X_2, \ldots, X_n$ равны множеству M, то их декартово произведение называется n-й *декартовой степенью* множества M и обозначается через M^n.

Таким образом, $M^n = \underbrace{M \times \ldots \times M}_{n \text{ раз}}$.

По определению $M^1 = M$, $M^2 = M \times M$.

Множество $\mathbb{R}^n$ используется в многих областях математики. Его элементами являются всевозможные кортежи $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, составленные из действительных чисел.