

Нехаев И.Н., доцент Поволжского государственного технологического университета

Колчев А.А., доцент Казанского Федерального Университета

**Курс Волгатеха (ПГТУ) «Линейная алгебра и геометрия»
для направления «Программная инженерия»**

■ ТЕМА

Введение в общую алгебру



Ключевые вопросы лекции

- Что такое множество и какие существуют операции над множествами?
- Какие бывают отношения и какими свойствами они обладают?
- Что такое алгебраическая структура (АС) с одной или с двумя операциями?
- Чем различаются группоид, моноид, группа, кольцо и поле?
- Как определить тип АС по описанию?

План уроков темы

- ❑ Описание множеств. Операции над множествами.
- ❑ Отношения. Свойства отношений.
- ❑ Функция. Отображение. Операции.
- ❑ Алгебраические системы и их изоморфизм.
- ❑ Группы, кольца, поля. Примеры

Множества

- **Множество** – совокупность любых объектов, называемых элементами множества.
- **Примеры множеств:** множество жителей данного города, множество целых чисел, множество студентов данной группы и т. д.
- Важные обозначения:
- $x \in A$ принадлежит A
- $x \notin A$ не принадлежит A
- \emptyset – пустое множество

Способы задания множеств

1) Перечислением всех элементов

- $A = \{\text{Петр, Сергей, Юлия, Ольга}\}$
- $B = \{1, 3, 5, 7, 9\}$

Способы задания множеств

1) Перечислением всех элементов

- $A = \{\text{Петр, Сергей, Юлия, Ольга}\}$
- $B = \{1, 3, 5, 7, 9\}$

2) Характеристическим предикатом, который описывает СВОЙСТВО ВСЕХ ЭЛЕМЕНТОВ, ВХОДЯЩИХ В МНОЖЕСТВО.

- $\{x | P(x)\}$ (или $\{x: P(x)\}$) - множество всех элементов x , для которых высказывание $P(x)$ истинно".

Способы задания множеств

1) Перечислением всех элементов

- $A = \{\text{Петр, Сергей, Юлия, Ольга}\}$
- $B = \{1, 3, 5, 7, 9\}$

2) Характеристическим предикатом, который описывает СВОЙСТВО ВСЕХ ЭЛЕМЕНТОВ, ВХОДЯЩИХ В МНОЖЕСТВО.

- $\{x | P(x)\}$ (или $\{x: P(x)\}$) - множество всех элементов x , для которых высказывание $P(x)$ истинно".
- $A = \{x: x^2 + 3x - 2 = 0, x \in R\}$ - множество корней уравнения;
- $A = \{x: x \leq 10, x \in N\}$ множество натуральных чисел от 1 до 10.

Сравнение множеств

- Множество **A** называется **подмножеством** множества **B**, если все элементы **A** содержатся в **B**.

$$A \subset B \Leftrightarrow \forall a \in A \Rightarrow a \in B$$

- Два множества называются **равными**, если они содержат одинаковые наборы элементов.

$$A = B \Leftrightarrow A \subset B \text{ и } B \subset A$$

Сравнение множеств

- Множество **A** называется **подмножеством** множества **B**, если все элементы **A** содержатся в **B**.

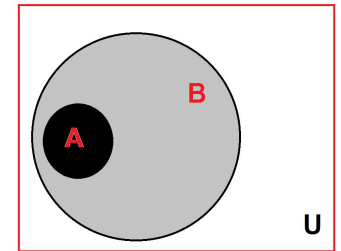
$$A \subset B \Leftrightarrow \forall a \in A \Rightarrow a \in B$$

- Два множества называются **равными**, если они содержат одинаковые наборы элементов.

$$A = B \Leftrightarrow A \subset B \text{ и } B \subset A$$

- Универсальное** множество (универсум) **U**

— множество, включающее все элементы и все множества, участвующие в рассматриваемой задаче.



- Булеан** множества **U** – это множество всех подмножеств **U** (2^U)
- Пустое** множество \emptyset является подмножеством всех множеств.
- Любое множество является подмножеством Универсального множества **U**:

$$A \subset U \Leftrightarrow A \in 2^U$$

Алгебра множеств

- **Алгебра множеств** в [теории множеств](#) — это непустая система подмножеств, [замкнутая](#) относительно операций [дополнения \(разности\)](#) и [объединения \(суммы\)](#).

Семейство S подмножеств множества U ($S \subset 2^U$) называется алгеброй, если оно удовлетворяет следующим свойствам:

1. $\emptyset \in S$
2. Если $A \in S$, то и его дополнение $U \setminus A \in S$
3. Если $A, B \in S$, то и объединение $A \cup B \in S$

(Статья из википедии:)

Операции над множествами

Основные операции, определяемые над множествами:

- **Пересечение** : $A \cap B := \{x : x \in A \text{ и } x \in B\}$
- **Объединение**: $A \cup B := \{x : x \in A \text{ или } x \in B\}$.

Если множества A и B не пересекаются, то $A \cap B = \emptyset$.

- **Разность**: $A \setminus B := \{x : x \in A \text{ и } x \notin B\}$.
- **Симметрическая разность**:

$$A \Delta B := \{x : (x \in A \text{ и } x \notin B) \text{ или } (x \notin A \text{ и } x \in B)\}.$$

- **Дополнение**: $\overline{A} := \{x : x \notin A\}$

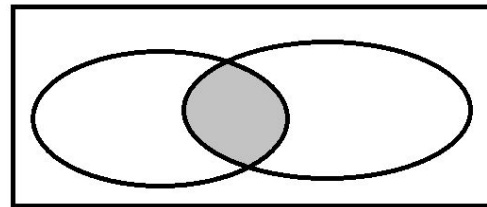
Операции над множествами.

Примеры

Пусть $A = \{К, А, Т, Я\}$, $B = \{Н, И, К, О, Л, А, Й\}$

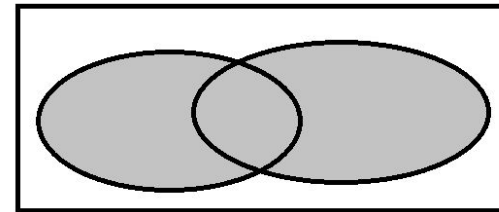
Пересечение :

- $A \cap B := \{А, К\}$



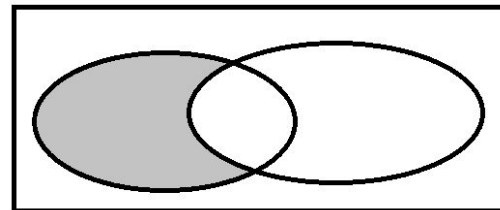
Объединение:

- $A \cup B := \{А, И, Й, К, Л, Н, О, Т, Я\}$.



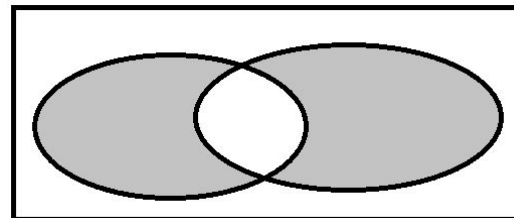
Разность:

- $A \setminus B := \{Т, Я\}$;



Симметрическая разность:

- $A \Delta B := \{И, Й, Л, Н, О, Т, Я\}$.



Свойства операций над множествами

- 1) Коммутативность.
- 2) Ассоциативность.
- 3) Дистрибутивность.
- 4) Свойство нуля.
- 5) Свойство единицы
- 6) Закон поглощения
- + Идемпотентность,
инволютивность,
закон де Моргана

Декартово произведение

Декартово или прямое произведение:

- $A \times B = \{ (a, b) : a \in A, b \in B \}$.

ПРИМЕР : $A = \{ 6, 5, 7 \}$; $B = \{ 11, 14, 12 \}$

- $A \times B = \{ (6, 11), (6, 14), (6, 12), (5, 11), (5, 14), (5, 12), (7, 11), (7, 14), (7, 12), \}$.

- Прямое произведение множеств – операция **многочестная**

$$A_1 \times A_2 \times \dots \times A_n = \prod_{i=1}^n A_i$$

- В результате получаются множества, состоящие из упорядоченной последовательности вида

$$(a_1, a_2, \dots, a_n) \text{ , где } a_1 \in A_1; a_2 \in A_2; \dots; a_n \in A_n .$$

• .

Декартово произведение

- **Декартово или прямое произведение:**

- $A \times B = \{ (a, b) : a \in A, b \in B \}$.

- ПРИМЕР : $A = \{ 6, 5, 7 \}$; $B = \{ 11, 14, 12 \}$

- $A \times B = \{ (6, 11), (6, 14), (6, 12), (5, 11), (5, 14), (5, 12), (7, 11), (7, 14), (7, 12), \}$.

- Прямое произведение множеств – операция **многочестная**

$$A_1 \times A_2 \times \dots \times A_n = \prod_{i=1}^n A_i$$

- В результате получаются множества, состоящие из упорядоченной последовательности вида

$$(a_1, a_2, \dots, a_n), \text{ где } a_1 \in A_1; a_2 \in A_2; \dots; a_n \in A_n.$$

- Такие последовательности называются **кортежами** или **векторами**. Сами элементы при этом называются **компонентами** (координатами) кортежа.

- **Степенью множества** называется декартово произведение множества A само на себя n раз:

- $A^n = A \times A \times A \dots \times A$ – n раз

- ПРИМЕР: $A = \{ 2, 7 \}$

- $A^2 = A \times A = \{ (2, 2), (2, 7), (7, 2), (7, 7) \}$.

План уроков темы

- ❑ Описание множеств. Операции над множествами.
- ❑ Отношения. Свойства отношений.
- ❑ Функция. Отображение. Операции.
- ❑ Алгебраические системы и их изоморфизм.
- ❑ Группы, кольца, поля. Примеры

Отношения

- **Опр. N -местным (n -арным) отношением**, заданным на множествах M_1, M_2, \dots, M_n называется любое подмножество декартова произведения $M_1 \times M_2 \times \dots \times M_n$
- Отношение обычно обозначается буквой **R** (Relation - отношение).
- Говорят, что a_1, a_2, \dots, a_n находятся в отношении **R**, если $(a_1, a_2, \dots, a_n) \in R$

Отношения

- **Опр. N -местным (n -арным) отношением**, заданным на множествах M_1, M_2, \dots, M_n называется любое подмножество декартова произведения $M_1 \times M_2 \times \dots \times M_n$
- Отношение обычно обозначается буквой **R** (Relation - отношение).
- Говорят, что a_1, a_2, \dots, a_n находятся в отношении **R**, если $(a_1, a_2, \dots, a_n) \in R$
- Бинарное отношение **R** на множестве A - любое подмножество $A \times A$.
- **Примеры отношений:** « x -спортсмен», « x работает в компании y », « x - y нравится y », « $z=x+y$ »
- Для бинарных отношений: xRy (« $x < y$ », « $x = y$ »)

Способы задания отношения

- **Перечислением всех элементов**
 - $M1 = \{\text{Петр, Сергей, Мирон}\}$
 - $M2 = \{\text{Юлия, Ольга}\}$
 - R - «Нравится», $R \subset M1 \times M2$
 - $R = \{(\text{Петр, Юлия}), (\text{Сергей, Ольга}), (\text{Мирон, Ольга}), (\text{Сергей, Юлия})\}$

Способы задания отношения

Таблично (перечислением всех элементов)

- $M1 = \{\text{Петр, Сергей, Мирон, Юлия, Ольга}\}$
- $M2 = \{x: x \in N, x < 200\}$
- $M3 = \{\text{Йошкар – Ола, Ульяновск, Набережные Челны, Саранск, Нижний Новгород, ...}\}$

- R - « x имеет возраст y и живет в городе z »,

$$R \subset M1 \times M2 \times M3$$

- $R1$ - « x имеет возраст y »
- $R2$ - « x живет в городе z »

Способы задания отношения

Предикатом, который описывает свойство всех n -к элементов, входящих в отношение.

- $\{(a_1, a_2, \dots, a_n): P(a_1, a_2, \dots, a_n)\}$ - множество всех кортежей (a_1, a_2, \dots, a_n) , для которых высказывание $P(a_1, a_2, \dots, a_n)$ истинно".
- Пример. R - «не больше»:
$$R = \{(x, y): x < y \text{ ИЛИ } x = y\}$$

Способы задания отношения

Графический способ задания отношений

- $M = \{\text{Петр, Сергей, Мирон, Юлия, Ольга}\}$
- $R = \{(\text{Петр, Юлия}), (\text{Юлия, Петр}), (\text{Мирон, Ольга}), (\text{Ольга, Мирон}), (\text{Сергей, Юлия}), (\text{Юлия, Сергей}), (\text{Ольга, Юлия}), (\text{Юлия, Ольга})\}$

Матрица бинарного отношения

$M = \{\text{Петр, Сергей, Мирон, Юлия, Ольга}\}$
 $R = \{(\text{Петр, Юлия}), (\text{Юлия, Петр}), (\text{Мирон, Ольга}),$
 $(\text{Ольга, Мирон}), (\text{Сергей, Юлия}), (\text{Юлия, Сергей}),$
 $(\text{Ольга, Юлия}), (\text{Юлия, Ольга})\}$

Бинарному отношению $R \in M \times M$,
где $M = (a_1, a_2, \dots, a_n)$ –
конечное множество
мощности n , соответствует
квадратная матрица C
порядка n , в которой элемент
 c_{ij} , стоящий на пересечении
 i -и строки и j -го столбца,
равен 1, если между a_i и a_j
имеет место отношение R ,
или 0, если оно отсутствует

Свойства бинарного отношения

Пусть R – отношение на множестве M , $R \in M \times M$.

Тогда отношение R :

- **рефлексивно**, если $\forall a \in M: a R a$
(главная диагональ матрицы рефлексивного отношения содержит только единицы);

Свойства бинарного отношения

Пусть R – отношение на множестве M , $R \in M \times M$.

Тогда отношение R :

- **рефлексивно**, если $\forall a \in M: a R a$;
- **антирефлексивно**, если $\forall a \in M: \neg (a R a)$
(главная диагональ матрицы антирефлексивного отношения содержит только нули);

Свойства бинарного отношения

Пусть R – отношение на множестве M , $R \in M \times M$.

Тогда отношение R :

- **симметрично**, если $\forall a, b \in M: a R b \Rightarrow b R a$
(матрица такого отношения симметрична относительно главной диагонали,
т.е. $c_{ij} = c_{ji}$);

Свойства бинарного отношения

Пусть R – отношение на множестве M , $R \in M \times M$.

Тогда отношение R :

- **симметрично**, если $\forall a, b \in M: a R b \Rightarrow b R a$;
-
- **антисимметрично**, если $\forall a, b \in M: a R b$ и $b R a \Rightarrow a = b$

(в матрице такого отношения отсутствуют единицы, симметричные относительно главной диагонали);

Свойства бинарного отношения

Пусть R – отношение на множестве M , $R \in M \times M$.

Тогда отношение R :

- **транзитивно**, если $\forall a, b, c \in M: a R b$ и $b R c \Rightarrow a R c$

Примеры транзитивного отношения: “>”, “=”, “есть путь”, “есть функция”, «является подмножеством»

- Пример нетранзитивного отношения: “общается с”, “нравится”

Отношения эквивалентности

Если отношение R на множестве M рефлексивно, симметрично и транзитивно одновременно, то это отношение **ЭКВИВАЛЕНТНОСТИ**.

Примеры отношения эквивалентности.

- $M1 = \{x: x \in N, x < 100\}$. $R1$ - отношение "оканчиваться на одну цифру".
- Пусть $M2 = \mathbf{Z}$ (множество целых чисел). $R2$ - отношение «имеют одинаковый остаток от деления на 3».
- (отношение конгруэнтности, подобия, ...)

Отношения эквивалентности

Ключевое свойство отношения эквивалентности:

- множество **A** разбивается на **непересекающиеся классы эквивалентности**, элементы внутри такого класса эквивалентны друг друга с точки зрения рассматриваемого отношения.

Примеры разбиения

- Для **R1** - отношение "оканчиваться на одну цифру" множество **M1** делится на 10 классов эквивалентности например $K_5 = \{5, 15, 25, \dots, 95\}$, $K_9 = \{9, 19, 29, \dots, 99\}$.
- Для **R2** - отношение «имеет одинаковый остаток от деления на 3» множество **M2** делится на 3 класса $K_0 = \{0, \pm 3, \pm 6, \dots\}$, $K_1 = \{\dots, -2, 1, 4, 7, \dots\}$, $K_2 = \{\dots, -1, 2, 5, 8, \dots\}$.

Отношения порядка

- **Связное (полное) отношение** – отношение R , в котором для любой пары a, b из условия $a \neq b$ следует aRb или bRa .

Примером **связного (полного) отношения** является отношение «**быть выше по росту**», заданное на множестве студентов некоторой группы.

Отношения порядка

- **Связное (полное) отношение** – отношение R , в котором для любой пары a, b из условия $a \neq b$ следует aRb или bRa .

- **Отношение частичного порядка** – отношение, которое рефлексивно, антисимметрично и транзитивно.

Пример: отношение «является подмножеством» (\subset), заданное на булеане U , отношение «доминирует» на R^2 .

- **Отношение линейного порядка** – отношение частичного порядка, которое связно.

Пример: является отношением \geq , заданное на множестве вещественных чисел.

Отношения порядка

- **Связное (полное) отношение** – отношение R , в котором для любой пары a, b из условия $a \neq b$ следует aRb или bRa .
- **Отношение строгого порядка** – отношение, которое антирефлексивно, антисимметрично и транзитивно.
- **Отношение строгого линейного порядка** – связное отношение строгого порядка.

Применение отношений

- **Описание смысла подмножеств**

$\mathbf{R} = \{(\text{Петр}, \text{Юлия}), (\text{Юлия}, \text{Петр}), (\text{Мирон}, \text{Ольга}), (\text{Ольга}, \text{Мирон}),$
 $(\text{Сергей}, \text{Юлия}), (\text{Юлия}, \text{Сергей}), (\text{Ольга}, \text{Юлия}), (\text{Юлия}, \text{Ольга})\}, \mathbf{R} = ?$

Применение отношений

- **Описание смысла подмножеств**

$R = \{(\text{Петр}, \text{Юлия}), (\text{Юлия}, \text{Петр}), (\text{Мирон}, \text{Ольга}), (\text{Ольга}, \text{Мирон}), (\text{Сергей}, \text{Юлия}), (\text{Юлия}, \text{Сергей}), (\text{Ольга}, \text{Юлия}), (\text{Юлия}, \text{Ольга})\}$, $R = ?$

- **Формирование новых множеств с использованием свойств отношений:**

R_1 – “выше чем” (транзитивно). $R_1 = \{(\text{Иван}, \text{Вася}), (\text{Вася}, \text{Саша})\}$

$R_2 = \overline{R_1}$ (транзитивное замыкание), $R_2 = R_1 \cup (\text{Иван}, \text{Саша})$

Применение отношений

- **Описание смысла подмножеств**

$R = \{(\text{Петр, Юлия}), (\text{Юлия, Петр}), (\text{Мирон, Ольга}), (\text{Ольга, Мирон}), (\text{Сергей, Юлия}), (\text{Юлия, Сергей}), (\text{Ольга, Юлия}), (\text{Юлия, Ольга})\}$, $R = ?$

- **Формирование новых множеств с использованием свойств отношений:**

R_1 – “выше чем” (транзитивно). $R_1 = \{(\text{Иван, Вася}), (\text{Вася, Саша})\}$

$R_2 = \overline{R_1}$ (транзитивное замыкание), $R_2 = R_1 \cup (\text{Иван, Саша})$

- **Конструирование предикатов для описания множеств**

$$M = \{x: x \in N \text{ И } x \leq 10\}, \quad M = \{(x, y): y = f(x)\}$$

$$M = \{x: x^2 - 1 = 0, x \in R\} \rightarrow M = \{-1, +1\} \quad (\text{и наоборот})$$

План уроков темы

ТЕМА
Введение
в общую алгебру

- ❑ Описание множеств. Операции над множествами.
- ❑ Отношения. Свойства отношений.
- ❑ Функция. Отображение. Операции.
- ❑ Алгебраические системы и их изоморфизм.
- ❑ Группы, кольца, поля. Примеры

Соответствие

- **Соответствие** между множествами **A** и **B** – это множество, представляющее собой некоторое подмножество их декартова произведения: $P \subset A \times B$ или $P: A \rightarrow B$.
A-начало, B – конец соответствия
- Если $(a, b) \in P$ то говорят, что **b** соответствует **a** в соответствии **P**
- **Образ элемента a в множестве B при соответствии P** – множество всех **b**, соответствующих элементу **a**.
Обозначается: $b = P(a)$.
- **Прообраз элемента b в множестве A при соответствии P** – множество всех **a**, соответствующих элементу **b**.
Обозначается $a = P^{-1}(b)$.

Соответствие

- **Область определения соответствия P (обозначается $D(P)$)** – множество таких a , для которых существует образ.
- **Область значений соответствия P (обозначается $E(P)$)** – множество таких b , для которых существует прообраз.

Виды соответствий

- **Всюду определенное соответствие** : $D(P) = A$. В противном случае соответствие называется **частичным**.
- **Сюръективное соответствие (сюръекция)**:
 $E(P) = B$.

Виды соответствий

- **Инъективное соответствие (инъекция)** – соответствие, при котором прообразом любого элемента из множества $E(P)$ является единственный элемент из множества $D(P)$.
- **Функциональное соответствие (функция)** – соответствие, при котором образом любого элемента из множества $D(P)$ является единственный элемент из множества $E(P)$.

Виды соответствий

- **Взаимнооднозначное соответствие** – соответствие, которое функционально и инъективно.
- **Биекция (1-1 соответствие)** – соответствие, которое всюду определено, сюръективно, функционально и инъективно.
- **Отображение A в B** – соответствие, которое всюду определено и функционально.
- **Отображение A на B** – соответствие, которое всюду определено, функционально и сюръективно.

Алгебраические операции

- Под **алгебраической операцией** понимается отображение, которое одному или нескольким элементам множества (аргументам) ставит в соответствие другой элемент (значение).
- Операции классифицируются по присущим им специфическим свойствам и по количеству аргументов аргности).
- **Унарная** операция на множестве **A** это отображение
$$f : A \rightarrow A.$$
- Примерами унарных операций могут служить операции перехода от множества к его дополнению, изменение знака числа. Унарную операцию называют **оператором**.
- **Нульарная операция** на множестве **A** - произвольный фиксированный элемент множества **A**. Нульарные операции позволяют фиксировать элементы множества **A**, обладающие некоторыми специальными свойствами. Примером нульарной операции является, например, фиксирование нуля в множестве целых чисел с операцией сложения.

Бинарная операция

Пусть A, B, C тройка непустых множеств.

- **Бинарной операцией f** на паре множеств A и B со значениями в C называется отображение $f : A \times B \rightarrow C$, которое ставит в соответствие упорядоченной паре $(a, b) \in A \times B$ некоторый элемент множества C .

Если $A = B = C$, то бинарная операция называется внутренней, в противном случае - внешней.

Бинарную операцию принято обозначать знаком действия, который ставится между операндами (инфиксная форма записи). Например, для произвольной бинарной операции $(*)$ результат её применения к двум элементам a и b записывается в виде $a * b$.

- Говорят, что множество A **замкнуто** относительно операции $*$, если $a_1 * a_2 \in A$ для любых $a_1, a_2 \in A$.

Свойства (типы) бинарных операций

Рассмотрим бинарную операцию на множестве A , обозначив ее звездочкой $(*)$. Эту операцию называют:

- 1) **ассоциативной**,
если $(a * b) * c = a * (b * c) \quad \forall a, b, c \in A;$
- 2) **коммутативной**,
если $a * b = b * a \quad \forall a, b \in A;$
- 3) **идемпотентной**,
если $a * a = a \quad \forall a \in A.$

Пусть (\circ) и $(*)$ - две бинарные операции, заданные на множестве A . Операция $(*)$ называется **дистрибутивной** относительно операции (\circ) , если

$$(a \circ b) * c = (a * c) \circ (b * c), \quad c * (a \circ b) = (c * a) \circ (c * b) \quad \forall a, b, c \in A.$$

Нулевой элемент

- Элемент $\mathbf{0}$ множества \mathbf{A} называют левым (правым) нулем относительно данной операции $*$, если $\mathbf{0} * a = \mathbf{0}$ ($a * \mathbf{0} = \mathbf{0}$) для любого $a \in \mathbf{A}$.
- Если $\mathbf{0}'$ — левый нуль и $\mathbf{0}''$ — правый нуль существуют, то они совпадают, так как $\mathbf{0}' = \mathbf{0}' * \mathbf{0}'' = \mathbf{0}''$. В этом случае говорят просто о **нуле относительно операции**, при этом он единственен и для него одновременно выполнены оба равенства $\mathbf{0} * x = \mathbf{0}$ и $x * \mathbf{0} = \mathbf{0}$.

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ d & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ d & 1 \end{pmatrix}.$$

Нейтральный элемент

- Элемент e множества A называют левым (правым) нейтральным элементом относительно операции $(*)$, если $e*a=a$ ($a*e=a$) для любого элемента $a \in A$.

Для левого e' и правого e'' нейтральных элементов, если они оба существуют, выполнены равенства $e' = e' * e'' = e''$, следовательно, они совпадают. В этом случае элемент e называют **нейтральным элементом**.

Нейтральным элементом относительно операции умножения на множестве натуральных чисел является число 1. На множестве целых чисел нейтральным элементом относительно операции сложения будет число 0.

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}.$$

Алгебраические операции

- Пусть $*$ - бинарная операция на множестве A , обладающая нейтральным элементом e . Элемент a' называется симметричным к элементу $a \in A$ относительно операции $*$, если $a'*a = e = a*a'$.

- **Аддитивные операции.** Если операция на множестве **коммутативна и ассоциативна**, то ее часто обозначают знаком $+$ и называют **сложением**.

При этом нейтральный элемент, если он существует, обозначается 0 и называется нулем, а (единственный) симметричный элемент к элементу a обозначается через $-a$ и называется противоположным к a элементом.

- **Мультипликативные операции.** Если операция на множестве **ассоциативна**, то ее часто обозначают знаком \cdot и называют **умножением**.

При этом нейтральный элемент, если он существует, обозначается 1 и называется единицей, а (единственный) симметричный элемент к элементу a обозначается через a^{-1} и называется обратным к a элементом.

План уроков темы

- ❑ Описание множеств. Операции над множествами.
- ❑ Отношения. Свойства отношений.
- ❑ Функция. Отображение. Операции.
- ❑ Алгебраические системы и их изоморфизм.
- ❑ Группы, кольца, поля. Примеры

Алгебраические структуры

- **Опр.** Непустое множество A , вместе с одной или несколькими алгебраическими операциями, определенными на этом множестве называют **алгебраической структурой (системой)**.

Обозначения:

- $(A, *)$ – пример обозначения алгебраической структуры с одной алгебраической операцией;
- $(A, *, \circ)$ – алгебраическая структура с двумя операциями
- и т.п. .

Алгебраические структуры (АС)

- **Опр.** Непустое множество \mathbf{A} , вместе с одной или несколькими алгебраическими операциями, определенными на этом множестве называют **алгебраической структурой (системой)**.

Примеры:

- $(\mathbf{R}, +)$ – множество вещественных чисел с операцией $+$;
- $(\mathbf{R}, +, *)$ – множество вещественных чисел с операциями $+$ и $*$;
- $(M_n(\mathbf{R}), +)$, $(M_n(\mathbf{R}), +, \times)$ – множество квадратных матриц n -го порядка, определенных на множестве действительных чисел с операциями матричного сложения $(+)$ и умножения (\times) .

Группоид

- **Опр.** Непустое множество A , в котором определена только одна бинарная операция, называется **группоидом**.

В группоиде на бинарную операцию нет никаких ограничений.

Полугруппа

- **Опр.** Непустое множество A , в котором определена только одна бинарная операция, называется **группоидом**.

В группоиде на бинарную операцию нет никаких ограничений.

- **Опр.** Алгебраическая структура $(A, *)$ называется **полугруппой**, если операция $*$ является **ассоциативной**.

Если операция $*$ является **коммутативной**, то полугруппа $(A, *)$ называется **коммутативной полугруппой**.

Примеры: $((\mathbf{N}, +), (\mathbf{N}, \cdot))$.

Моноид

- **Опр.** Полугруппа A , в которой существует **единичный элемент**, называется полугруппой с единицей, или **МОНОИДОМ**.

Примеры:

- Аддитивная полугруппа $(M_n(\mathbf{R}), +)$ - это коммутативный моноид (единичный элемент - нулевая матрица).
- Мультипликативная полугруппа $(M_n(\mathbf{R}), \times)$ - это некоммутативный моноид (единичный элемент - единичная матрица E)

Группа

- **Опр.** Моноид \mathbf{G} , в котором для любого элемента существует **симметричный или противоположный элемент**, называется **группой**.

Т.о., для операции группы выполняются следующие свойства:

- А1. Операция $*$ **ассоциативна**:

$$\forall x, y, z \in \mathbf{G} \quad x * (y * z) = (x * y) * z;$$
- А2. операция $*$ обладает **нейтральным элементом** e :

$$\exists e \in \mathbf{G} : \forall x \in \mathbf{G} \quad x * e = e * x = x;$$
- А3. все элементы множества \mathbf{G} **обратимы** относительно операции $*$:

$$\forall x \in \mathbf{G} \exists x' \in \mathbf{G} \quad x * x' = x' * x = e.$$

Абелева группа

- **Опр.** Группа $(G, *)$ называется **абелевой**, если операция $*$ в ней коммутативна.

Примеры:

- $(V, +)$, V - множество n -к чисел:
- $(Z, +)$. Z - множество целых чисел относительно операции $+$

Абелева группа

- **Опр.** Группа $(G, *)$ называется **абелевой**, если операция $*$ в ней коммутативна.

Примеры:

- $(V, +)$, V - множество n -к чисел:
- $(Z, +)$. Z - множество целых чисел относительно операции $+$
- Группа G , содержащая конечное число элементов, называется **конечной**, а число её элементов называется порядком и обозначается $|G|$. В противном случае группа называется бесконечной.
- Группу относительно сложения называют **аддитивной** группой. Группу относительно умножения называют **мультипликативной** группой.

Свойства групп

- Утверждение 1. **Нейтральный элемент единственен:**

Если e_1, e_2 — нейтральные, то $e_1 * e_2 = e_1, e_2 * e_1 = e_2 \Rightarrow e_2 = e_1$.

- Утверждение 2. **Для каждого элемента a обратный элемент a' единственен.**

Пусть для элемента a существуют два обратных элемента a_1' и a_2' . Тогда ...

•

Свойства групп

- Утверждение 3. **Верны законы сокращения:**
 $c * a = c * b \Leftrightarrow a = b, a * c = b * c \Leftrightarrow a = b.$

Действительно, пусть $c * a = c * b$, e – единичный элемент группы и c' – обратный к c элемент. Тогда ...

- Утверждение 4. **Группа содержит единственное решение x любого уравнения $x * c = b$ или $c * x = b$.**

Доказательство. Решением уравнения $a * x = b$ в группе A называется такой элемент $c \in A$, что $a * c = b$. Возьмем $c = a' * b$, где a' – обратный к a элемент.

Тогда ...

.

Свойства групп

- Обратный элемент к нейтральному есть сам нейтральный элемент: $e^{-1} = e$.
- $(ab)^{-1} = b^{-1}a^{-1}$.
- $(a^{-1})^{-1} = a$.
- $e^n = e$, для любого $n \in \mathbb{Z}$.

АС с двумя операциями: кольцо

- *Опр. Кольцо* — это непустое множество M , на котором заданы две бинарные операции: $+$ и \times (называемые **сложение** и **умножение**), со следующими свойствами:
 - 1)-4) $(M, +)$ – абелева группа;
 - 5) $(M, *)$ – полугруппа;
 - 6) дистрибутивность умножения относительно сложения:
$$a \times (b + c) = a \times b + a \times c$$
$$(b + c) \times a = b \times a + c \times a$$

Пример: $(\mathbf{Z}, +, *)$

Кольцо многочленов — кольцо, образованное многочленами от одной или нескольких переменных с коэффициентами из другого кольца.

Многочленом от одной переменной над кольцом K называется выражение

$$f = f(x) = a_0 + a_1x + \dots + a_nx^n = \sum_{i=0}^n a_ix^i, \quad a_i \in K,$$

где x — некоторая переменная из кольца K .

Если $a_n \neq 0$, то a_n называется старшим коэффициентом многочлена f , а n — степенью многочлена f (обозначение: $n = \deg f$)

Нулевому многочлену 0 степень не приписывается. Два многочлена равны, если равны коэффициенты при одинаковых степенях x . Множество всех многочленов от x над кольцом K будем обозначать символом $K[x]$. На множестве $K[x]$ определим операции сложения и умножения:

$$\sum_{i=0}^n a_ix^i + \sum_{i=0}^n b_ix^i = \sum_{i=0}^n (a_i + b_i)x^i,$$

$$\sum_{i=0}^n a_ix^i \cdot \sum_{j=0}^m b_jx^j = \sum_{k=0}^{n+m} c_kx^k, \quad \text{где } c_k = \sum_{i+j=k} a_ib_j,$$

при определении операции сложения мы добавляем нулевые слагаемые с тем, чтобы получить записи с одинаковыми степенями x .

АС с двумя операциями: поле

• **Опр.** Кольцо F называется **полем**, если множество его ненулевых элементов $F \setminus \{0\}$, **непусто и образует абелеву группу**. Эта группа называется **мультипликативной группой** поля.

• 1)-4) $(F, +)$ – абелева группа;

• 5)-8) $(F \setminus \{0\}, *)$ – абелева группа;

• 9) дистрибутивность умножения относительно сложения:

$$a \times (b + c) = a \times b + a \times c$$

$$(b + c) \times a = b \times a + c \times a$$

Примеры: $(\mathbf{Q}, +, *)$, $(\mathbf{R}, +, *)$, $\mathbf{Z}_p = \{0, 1, 2, \dots, p-1\}$ с операциями "сложения по модулю p " и "умножения по модулю p " является **полем для любого простого числа p** . Поля, состоящие из конечного числа элементов называются полями Галуа.

- Изоморфизм алгебраических структур одного вида позволяет результаты в одной АС переносить в другую АС:

$$(R^+, *) \leftrightarrow (R, +)$$

$$\ln(a * b) = \ln(a) + \ln(b)$$