АЛГЕБРА-1

МОДУЛЬ 1. ТЕОРИЯ ДЕЛИМОСТИ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ. ТЕОРИЯ ДЕЛИМОСТИ.

МОДУЛЬ 2. МНОЖЕСТВА И ОТНОШЕНИЯ. АЛГЕБРЫ И АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ. ОСНОВНЫЕ ЧИСЛОВЫЕ СИСТЕМЫ.

МОДУЛЬ 3. МАТРИЦЫ И ОПРЕДЕЛИТЕЛИ.

МОДУЛЬ-1

«Теория делимости целых чисел. Теория сравнений»

§1. Отношение делимости целых чисел и его свойства

О.1. Пусть $a, b \in \mathbb{Z},\ b \neq 0$. Говорят, что a *делится на* b и пишут $a \vdots b$, если существует $c \in \mathbb{Z}$, такое что $a = bc$. Можно также говорить, что b *делит* a и записывать $b|a$.

Число a называется *кратным* числа b, b *– делителем* числа a, c *– частным* от деления a на b.

Рассмотрим несколько важных свойств делимости.

Св-во 1 (рефлексивность). $a \vdots a$, $\forall a \in \mathbb{Z}\backslash\{0\}$.

Св-во 2 (транзитивность). Пусть $a, b, c \in \mathbb{Z}$.

Если $a \vdots b$, $b \neq 0$, и $b \vdots c$, $c \neq 0$, то $a \vdots c$.

Св-во 3. Если $a \vdots c$ и $b \vdots c$, $c \neq 0$, то $a \pm b \vdots c$.

Св-во 4. Если $a \vdots c$, $c \neq 0$, то $\forall b \in \mathbb{Z}$: $ab \vdots c$.

Св-во 5. Если $a_1, a_2, \dots, a_m, c, d \in \mathbb{Z}$, $a_i \vdots d$, $\forall i = \overline{1, m}$ и $a_1 + a_2 + \cdots + a_m \pm c \vdots d$, $d \neq 0$, то $c \vdots d$.

Св-во 6. $0 \vdots b$, $\forall b \in \mathbb{Z} \backslash \{0\}$.

Св-во 7. $a \vdots 1$, $\forall a \in \mathbb{Z}$.

Св-во 8. Если $a \vdots b$, $a \neq 0, b \neq 0$, то $|a| \geq |b|$.

Св-во 9. Если $a \vdots b$ и $b \vdots a$, $a \neq 0, b \neq 0$, то $|a| = |b|$.

§2. Теорема о делении с остатком

Т.1 (о делении с остатком). Пусть $a, b \in \mathbb{Z},\ b \neq 0$. Тогда $\exists q, r \in \mathbb{Z}$: $a = bq + r$, причем $0 \leq r < |b|$. Кроме того, числа q и r определены однозначно.

О.1. Число q называется неполным частным, а r – остатком от деления a на b.

Пр.1. Выполнить деление с остатком $a = 95$ на $b = 17$.

§3. Наибольший общий делитель (НОД) и его свойства

О.1. Пусть $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Число $\delta \in \mathbb{Z}\backslash\{0\}$ называется *общим делителем* этих чисел, если $a_i \vdots \delta$, $\forall i = 1,2, \ldots, n$.

О.2. Число $d \in \mathbb{Z}\backslash\{0\}$ называют *наибольшим общим делителем* чисел $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, если:

(1) d – общий делитель этих чисел;

(2) d делится на любой общий делитель этих чисел.

Обозн-ся: $d = \text{НОД}(a_1, a_2, \ldots, a_n)$ или $d = (a_1, a_2, \ldots, a_n)$.

Рассмотрим несколько важных свойств НОД.

Св-во 1. Если $d_1 = \text{НОД}(a, b)$ и $d_2 = \text{НОД}(a, b)$, то $|d_1| = |d_2|$.

3.1. Так как все НОД отличаются друг от друга только знаками, условимся считать под НОД натуральное значение.

Св-во 2. Если $a \vdots b$, $b \neq 0$, то $(a, b) = |b|$.

Св-во 3. Если $a = bq + r$, где $a, b, r \neq 0$, то $(a, b) = (b, r)$.

§4. Алгоритм Евклида. Линейное представление НОД.

Алгоритм Евклида описывает способ нахождения НОД двух $a, b \in \mathbb{N}$.

Пусть $a \neq 0$, $b = 0$. Так как $0 : a$, то по св-ву 2 §4 $\text{НОД}(a, 0) = a$.

Пусть $a \neq 0$, $b \neq 0$. Далее будем действовать по шагам:

(1) Выполним деление a на b с остатком:

$$a = bq_0 + r_1, \text{ где } 0 \leq r_1 < b.$$

Если $r_1 = 0$, т.е. $a \vdots b$, то по св-ву 2 §4 $\text{НОД}(a, b) = b$, т.е. процесс нахождения $\text{НОД}(a, b)$ закончится на первом шаге.

Пусть $r_1 \neq 0$. Тогда по св-ву 3 §4 $\text{НОД}(a, b) = \text{НОД}(b, r_1)$.

(2) Выполним деление b на r_1 с остатком:

$$b = r_1 q_1 + r_2, \text{ где } 0 \leq r_2 < r_1 < b.$$

Если $r_2 = 0$, т.е. $b : r_1$, то по св-ву 2 §4 то $\text{НОД}(a, b) = \text{НОД}(b, r_1) = r_1$ (последний ненулевой остаток).

Пусть $r_2 \neq 0$. Тогда по св-ву 3 §4 $\text{НОД}(a, b) = \text{НОД}(b, r_1) = \text{НОД}(r_1, r_2)$.

(3) Выполним деление r_1 на r_2 с остатком и т.д. Этот процесс не может продолжаться до бесконечности, т.к. все остатки от деления убывают и положительны.

В результате получим систему равенств вида:

$$(1)\begin{cases} a = bq_0 + r_1, \\ b = r_1q_1 + r_2, \\ r_1 = r_2q_2 + r_3, \\ \dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, \\ r_{n-1} = r_nq_n. \end{cases}$$

Последний ненулевой остаток $r_n = \text{НОД}(a, b)$.

Пр.1. Найти $\text{НОД}(a, b)$, если $a = 95$, $b = 35$.

Т.1 (о линейном представлении НОД). Пусть $a, b \in \mathbb{Z}$ и $d = \text{НОД}(a, b)$. Тогда $\exists x, y \in \mathbb{Z}$: $d = xa + yb$ – линейное представление $\text{НОД}(a, b)$.

Пр.2. Найти линейное представление $\text{НОД}(a, b)$, если

$$a = 95, b = 35.$$

§5. Взаимно простые числа.

О.1. Пусть $a, b \in \mathbb{Z}$. Эти числа будем называть взаимно простыми и записывать $(a, b) = 1$, если НОД$(a, b) = 1$.

Например, $(2,15) = 1$.

Т.1. Пусть $a, b \in \mathbb{Z}$. Тогда

$$(a, b) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z}: xa + yb = 1.$$

Т.2. Пусть $a, b, \text{c} \in \mathbb{Z}$. Если $ab \vdots c$, $c \neq 0$, $(a, c) = 1$, то $b \vdots c$.

Сл.1. Пусть $a, b, c \in \mathbb{Z}$. Если $a \vdots b$, $b \neq 0$, и $a \vdots c$, $c \neq 0$, где $(b, c) = 1$, то $a \vdots bc$.

Пр.1. $876 \vdots 2,\ 876 \vdots 3,\ (2,3) = 1 \Longrightarrow 876 \vdots 6.$

Т.3. Пусть $a, b, c \in \mathbb{Z}$. Если $(a, b) = 1$ и $(b, c) = 1$, то $(ab, c) = 1$.

§6. Наименьшее общее кратное (НОК)

О.1. Пусть $a_1, a_2, \dots, a_n \in \mathbb{Z}\backslash\{0\}$. Число $M \in \mathbb{Z}$ называется *общим кратным* этих чисел, если $M \vdots a_i$, $\forall i = 1,2, \dots n$.

О.2. Число $m \in \mathbb{Z}$ называют *наименьшим общим кратным* чисел $a_1, a_2, \dots, a_n \in \mathbb{Z}\backslash\{0\}$, если:

(1) m – общее кратное этих чисел;

(2) любое общее кратное этих чисел делится на m.

Обозн-ся: $m = \text{НОК}(a_1, a_{2,} \dots, a_n)$ или $m = [a_1, a_{2,} \dots, a_n]$.

Св-во 1. Если $m_1 = \text{НОК}(a, b)$ и $m_2 = \text{НОК}(a, b)$, то $|m_1| = |m_2|$.

3.1. В дальнейшем будем выбирать положительное значение НОК.

Т.1. Пусть $a, b \in \mathbb{N}$. Тогда $[a, b] = \frac{ab}{(a,b)}$.

§7. Простые числа. Решето Эратосфена.

О.1. Натуральное число $n > 1$ называется *простым*, если оно делится либо на само себя, либо на 1, а других делителей у него нет. Числа, которые не являются простыми, называются *составными*.

Т.о. $\mathbb{N} = \{1\} \cup \{\text{простые числа}\} \cup \{\text{составные числа}\}$.

Т.1. Пусть $n \in \mathbb{N}$ и p – простое число. Тогда либо $n \vdots p$, либо $(n, p) = 1$.

Т.2. Пусть $n_1, n_2, \ldots, n_k \in \mathbb{N}$ и p – простое число. Если $n_1 n_2 \ldots n_k \vdots p$, то хотя бы один из множителей $n_s \vdots p$, $s \in \{1,2, \ldots, k\}$.

Т.3. Если n – составное число, p – его наименьший простой делитель, то $p \leq \sqrt{n}$.

3.1. Если n не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то $n -$ простое. В противном случае - $n -$ составное.

Пр.1. Является ли $n = 137$ простым числом?

В III в. до н.э. греческий математик Эратосфен открыл способ выделения простых чисел из отрезка 1, 2, …, n натурального ряда путем вычеркивания числа 1; всех чисел, кратных 2 (кроме 2); затем всех чисел, кратных 3 (кроме 3); и т.д., всех чисел, кратных $p \leq \sqrt{n}$.

Пр. 2. Найти все простые числа, не превосходящие 30.

§8. Разложение составных чисел на простые множители

Т.1 (основная теорема арифметики). Всякое натуральное число $n > 1$ либо является простым, либо может быть представлено ив виде произведения простых чисел. Кроме того, это представление единственно с точностью до порядка записи множителей.

О.1. Рассмотрим разложение числа n на простые множители. Упорядочим это разложение и соберем одинаковые степени:

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k},$$

где $p_1, p_2, \ldots, p_k$ – различные простые числа, $\alpha_i \in \mathbb{N}$, $\forall\, i = 1,2, \ldots, k$.

Такое представление числа n называют *каноническим.*

Пр.1. Найти каноническое представление числа $n = 180$.

3.1. Пусть $a, b \in \mathbb{N}$ и

$$a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_s}^{\alpha_s},\ b = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_s}^{\beta_s},$$

где $p_1, p_2, \dots, p_s$ – различные простые числа; $\alpha_i,\ \beta_i \in \mathbb{N} \cup \{0\}$, $i = 1,2, \dots, s$. Тогда

$$(a, b) = {p_1}^{\gamma_1} {p_2}^{\gamma_2} \dots {p_s}^{\gamma_s},$$

где $\gamma_i = \min\{\alpha_i, \beta_i\},\ i = 1,2, \dots, s.$

$$[a, b] = {p_1}^{\lambda_1} {p_2}^{\lambda_2} \dots {p_s}^{\lambda_s},$$

где $\lambda_i = \max\{\alpha_i, \beta_i\}$, $i = 1,2, \dots, s$.

Пр.2. Найти НОД(a, b) и НОК(a, b), используя канонические представления чисел a и b, если

$$a = 2^3 \cdot 3^4 \cdot 5 \cdot 7^4 \text{ и } b = 2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2.$$

§9. Бесконечность множества простых чисел.

Т.1 (Евклид). Множество простых чисел бесконечно.

Т.2 (об интервалах). Для любого $n \in \mathbb{N}$ существуют интервалы длины n, в которых нет ни одного простого числа.

§10. Сравнения и их свойства

О.1. Пусть $a, b \in \mathbb{Z}$. Числа a и b будем называть *сравнимыми по модулю* m ($m \in \mathbb{N}, m \neq 1$), если они имеют при делении на m один и тот же остаток r. Обозначается: $a \equiv b (mod\ m)$.

Если остатки от деления a и b на m разные, будем записывать: $a \not\equiv b (mod\ m)$.

Т.1. Пусть $a, b \in \mathbb{Z}$. Тогда $a \equiv b (mod\ m) \Leftrightarrow a - b \vdots m$.

Рассмотрим несколько важных свойств сравнений.

Св-во 1.

1) (рефлексивность) $a \equiv a(mod\ m)$;
2) (симметричность) если $a \equiv b(mod\ m)$, то $b \equiv a(mod\ m)$;
3) (транзитивность) если $a \equiv b(mod\ m)$ и $b \equiv c(mod\ m)$, то $a \equiv c(mod\ m)$.

Св-во 2. Если $a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$, то

1) $a + c \equiv b + d(mod\ m)$,
2) $a - c \equiv b - d(mod\ m)$,
3) $ac \equiv bd(mod\ m)$.

Сл.1. Если $a \equiv b(mod\ m)$, то

$$a + k \equiv b + k(mod\ m),\ \forall k \in \mathbb{Z}.$$

Сл. 2. Если $a \equiv b(mod\ m)$, то $a^n \equiv b^n(mod\ m)$, $\forall n \in \mathbb{N}$.

Сл. 3. Члены сравнения можно переносить из одной части в другую с противоположным знаком.

Сл. 4. К обеим частям сравнения можно прибавлять (отнимать) число, кратное модулю.

Св-во 3. Если $a \equiv b(mod\ m)$, то

$$ka \equiv kb(mod\ m), \forall k \in \mathbb{Z}.$$

Св-во 4. Если $ka \equiv kb(mod\ m)$ и $(k, m) = 1$, то

$$a \equiv b(mod\ m).$$

3.1. Сокращать обе части сравнения на число, не взаимно простое с модулем, нельзя. Сравнение может получиться как верным, так и нет.

Например, $30 \equiv 6(mod\ 6),\ |:2,\ \ (2,6) \neq 1,$

$15 \equiv 3(mod\ 6)$ – верное сравнение.

НО $30 \equiv 6(mod\ 6),\ |:3,\ \ (3,6) \neq 1,$

$10 \equiv 2(mod\ 6)$ – неверное сравнение.

Св-во 5. Если $a \equiv b(mod\ m)$, то

$$ka \equiv kb(mod\ km), \quad \forall k \in \mathbb{N}.$$

Св-во 6. Если $ka \equiv kb(mod\ km)$, то

$$a \equiv b(mod\ m), \forall k \in \mathbb{N}.$$

§11. Классы вычетов по данному модулю

Множество $\mathbb{Z}$ можно разбить на m непересекающихся подмножеств в зависимости от остатка при делении на m. Эти подмножества называются *классами вычетов* по модулю m. Все числа (*вычеты*) принадлежащие одному классу имеют одинаковые остатки при делении на m (сравнимы по модулю m).

С помощью этих остатков и будем обозначать классы вычетов:

Остатки от деления на m: $0, 1, \dots, m-1$.

(представители классов вычетов)

Классы вычетов по модулю m: $\bar{0}, \bar{1}, \dots, \overline{m-1}$.

Заметим, что $x \in \bar{a} \Leftrightarrow x \equiv a (mod\ m)$,

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b\ (mod\ m).$$

Обозначим $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ – множество классов вычетов по модулю m будем обозначать.

Определим на множестве $\mathbb{Z}_m$ операции сложения и умножения по правилам: $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{ab}$.

Пр.1. Построить таблицы + и * в $\mathbb{Z}_5$.

§12. Полная система вычетов

О.1. *Полной системой вычетов* (ПСВ) по модулю m называется совокупность m целых чисел, содержащая по одному представителю из каждого класса вычетов по модулю m.

Обычно в качестве представителей берутся:

наименьшие неотрицательные $0, 1, \dots, m-1,$

наименьшие положительные $1, 2, \dots, m$

или наименьшие по абсолютной величине

$$-\frac{m-1}{2}, \dots, -1, 0, 1, \dots, \frac{m-1}{2}$$

вычеты.

Пр.1. Пусть $m = 5$

ПСВ	
наименьших неотрицательных вычетов	0, 1, 2, 3,4
наименьших положительных вычетов	1, 2, 3, 4,5
наименьших по абсолютной величине вычетов	–2,–1, 0, 1, 2

Т.1. Любая совокупность m чисел $x_1, x_2, \dots, x_m$ (1), попарно не сравнимых по модулю m, образует ПСВ по модулю m.

Т.2. Пусть $(a, m) = 1$, $b \in \mathbb{Z}$. Если $x_1, x_2, \dots, x_m$ – ПСВ по модулю m, то $ax_1 + b, ax_2 + b, \dots, ax_m + b$ (2) – ПСВ по модулю m.

§13. Приведенная система вычетов

Л.1. Все числа из $\bar{a} \in \mathbb{Z}_m$ имеют с m один и тот же НОД, т.е. если $a \equiv b(mod\ m)$, то $(a, m) = (b, m)$.

З.1. В виду Л.1 вместо (a, m) можно писать $(\bar{a}, m)$.

О.1. Если $(\bar{a}, m) = 1$, то класс вычетов $\bar{a}$ называется классом вычетов, взаимно простым с m.

О.2. *Приведенной системой вычетов* (ПрСВ) по модулю m называется совокупность вычетов по модулю m, взятых по одному из каждого взаимно простого с m класса вычетов.

Чтобы составить ПрСВ по модулю m нужно выписать ПСВ по модулю m и выбрать из нее вычеты, взаимно простые с m.

Пр.1. Пусть $m = 5$.

	ПСВ		ПрСВ
наименьших неотрицательных вычетов	0, 1, 2, 3,4	$\overrightarrow{\text{Взаимно простые}}$ с $m = 5$	1, 2, 3,4
наименьших положительных вычетов	1, 2, 3, 4,5	$\overrightarrow{\text{Взаимно простые}}$ с $m = 5$	1, 2, 3, 4
наименьших по абсолютной величине вычетов	-2,–1, 0, 1, 2	$\overrightarrow{\text{Взаимно простые}}$ с $m = 5$	-2,–1, 1, 2

Пусть число классов, взаимно простых с m равно k.

Т.1. Любая совокупность k чисел $x_1, x_2, \dots, x_k$ (1), попарно не сравнимых по модулю m и взаимно простых с m, есть ПрСВ по модулю m.

Т.2. Пусть $(a, m) = 1$. Если $x_1, x_2, \dots, x_k$ – ПрСВ по модулю m, то $ax_1, ax_2, \dots, ax_k$ (2) – ПрСВ по модулю m.

§14. Обратимые элементы во множестве классов вычетов

О.1. Элемент $\bar{a} \in \mathbb{Z}_m$ называется *обратимым*, если

$$\exists \bar{b} \in \mathbb{Z}_m: \quad \bar{a}\bar{b} \equiv \bar{1}.$$

Т.1. Элемент $\bar{a} \in \mathbb{Z}_m$ обратим $\Leftrightarrow (\bar{a}, m) = 1$.

3.1. Множество всех обратимых элементов $\mathbb{Z}_m$ совпадает с множеством всех классов, взаимно простых с m, и обозначается $\mathbb{Z}_m{}^*$.

Пр.1. Найти $\mathbb{Z}_5{}^*$.

§15. Функция Эйлера.

О.1. Обозначим через $\varphi(m)$ число классов вычетов по модулю m, взаимно простых с m, т.е. число элементов ПрСВ по модулю m. Функцию $\varphi(m)$ называют функцией Эйлера.

Выберем в качестве представителей наименьшие положительные вычеты $1,2,\dots,m$. Тогда $\varphi(m)-$ число натуральных чисел, не превосходящих m и взаимно простых с m.

Т.1. Если p – простое число, то

$$\varphi(p) = p - 1.$$

Т.2. Если $n = p^{\alpha}$, где p – простое число и $\alpha \in \mathbb{N}$, то

$$\varphi(n) = \varphi(p^{\alpha}) = p^{\alpha-1}(p - 1).$$

Т.3. Если $(m,n)=1$, то $\varphi(mn)=\varphi(m)\varphi(n)$.

Т.4. Если $m={p_1}^{\alpha_1}\cdot{p_2}^{\alpha_2}\cdot\ldots\cdot{p_k}^{\alpha_k}$ – каноническое представление числа m, то

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right).$$

Пр.1. Вычислить $\varphi(18)$.

§16. Теоремы Эйлера и Ферма.

Т.1 (Эйлера). Для любого $a \in \mathbb{Z},\ (a, m) = 1$, верно

$$a^{\varphi(m)} \equiv 1 (mod\ m).$$

Т.2 (Ферма). Пусть $a \in \mathbb{Z}$, p – простое число, $(a, p) = 1$. Тогда

$$a^{p-1} \equiv 1 (mod\ p).$$

Сл.1. Пусть $a \in \mathbb{Z}$, p – простое число. Тогда

$$a^{p} \equiv a (mod\ p).$$

Пр.1. Найти остаток от деления 317^{259} на 15.

МОДУЛЬ-2

«Множества и отношения. Алгебры и алгебраические системы. Основные числовые системы»

§17. Множество. Подмножество. Пустое множество.

О.1. Под множеством понимается любая совокупность объектов, называемых элементами множества.

Множества обозначаются большими латинскими буквами $(A, B, C, \ldots)$, а их элементы – малыми $(a, b, c, \ldots)$.

Если элемент a принадлежит множеству A, пишут $a \in A$. В противном случае будем писать $a \notin A$.

Стандартные обозначения множеств:

$\mathbb{N}$ – множество всех натуральных чисел,

$\mathbb{Z}$ – множество всех целых чисел,

$\mathbb{Q}$ – множество всех рациональных чисел,

$\mathbb{R}$ – множество всех действительных чисел.

О.2. Два множества A и B называются равными, если они содержат одни и те же элементы, т.е.

1) если $x \in A$, то $x \in B$, $\forall x \in A$

2) если $x \in B$, то $x \in A$, $\forall x \in B$

Обозначается $A = B$.

О.3. Если каждый элемент множества A является элементом множества B, т.е.

$$\text{если } x \in A, \text{ то } x \in B, \forall x \in A,$$

то говорят, что A есть подмножество множества B.

Обозначается: $A \subseteq B$.

Множество A называется собственным подмножеством B, если $A \subseteq B$ и $A \neq B$. Обозначается: $A \subset B$.

О.4. Множество называется конечным, если оно содержит конечное число элементов. Число элементов конечного множества A называется его мощностью и обозначается $|A|$.

Множество, не содержащее ни одного элемента, называется пустым и обозначается $\emptyset$. Очевидно, что для любого множества A: $\emptyset \subseteq A$, $A \subseteq A$.

Способы задания множеств:

1) Перечисление элементов (только для конечных множеств).

$$M = \{m_1, m_2, \dots, m_k\}$$

2) Указание свойств.

$$M = \{x | \text{условие, которому удовлетворяет } x\}$$

обозначение произвольного элемента из M

Пр.1. $M -$ множество натуральных чисел, не превосходящих 6. Тогда

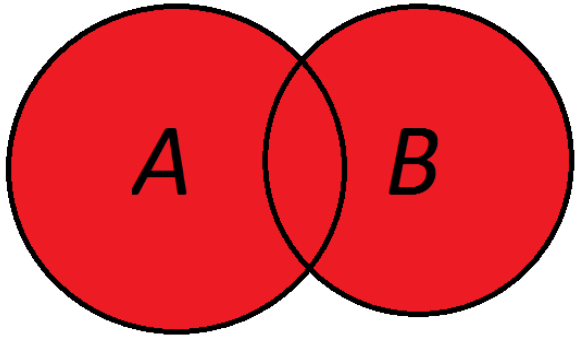
1) $M = \{1,2,3,4,5,6\},\ |M| = 6.$

2) $M = \{x | x \in \mathbb{N},\ x \leq 6\},\ |M| = 6.$

§18. Операции над множествами и их свойства

Рассмотрим операции над множествами и их свойства.

О.1. Объединением множеств A и B называется множество $A \cup B$, содержащее элементы, каждый из которых принадлежит хотя бы одному из множеств A или B.



$$A \cup B = \{x | x \in A \text{ или } x \in B\}$$

Свойства объединения:

1) $A \subseteq A \cup B$;

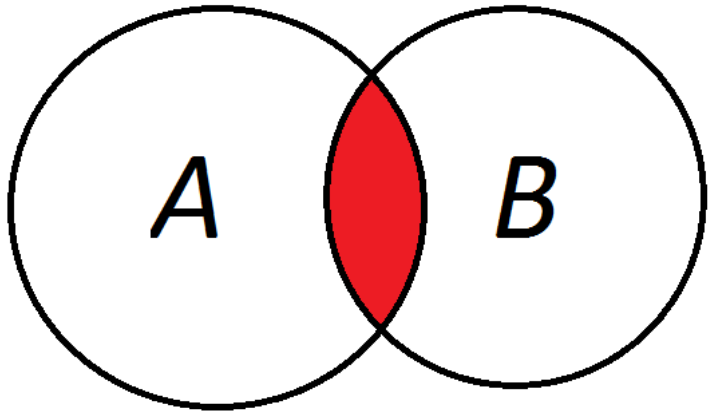
2) $B \subseteq A \cup B$;

3) $A \cup \emptyset = A$.

Пр.1. Пусть $A = \{1,9,18\},\ B = \{1,5,9\}$.

Найти $A \cup B$.

О.2. Пересечением множеств A и B называется множество $A \cap B$, содержащее элементы, каждый из которых принадлежит и множеству A и множеству B.



$$A \cap B = \{x | x \in A \text{ и } x \in B\}$$

Свойства пересечения:

1) $A \cap B \subseteq A$;

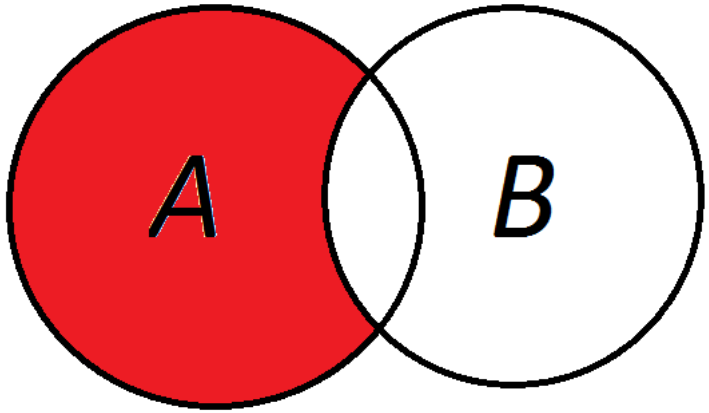
2) $A \cap B \subseteq B$;

3) $A \cap \emptyset = \emptyset$.

Пр.2. Пусть $A = \{1,9,18\},\ B = \{1,5,9\}$.

Найти $A \cap B$.

О.3. Разностью множеств A и B называется множество $A\backslash B$, содержащее элементы, каждый из которых принадлежит множеству A и не принадлежит множеству B.



$$A\backslash B = \{x | x \in A \text{ и } x \notin B\}$$

Свойства разности:

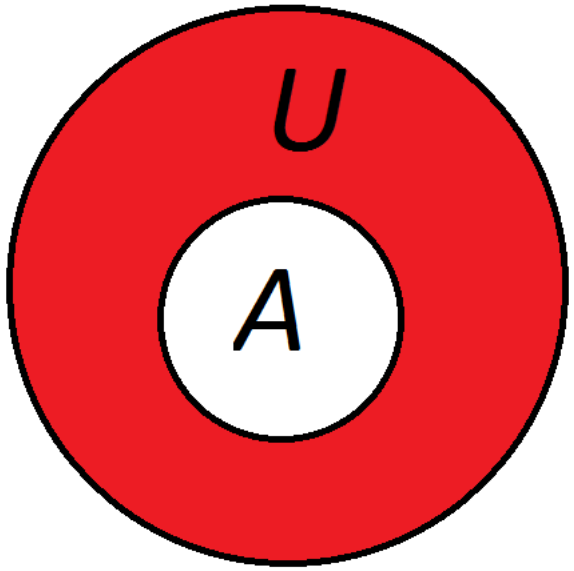
1) $A \backslash A = \emptyset$;

2) $A \backslash \emptyset = A$;

Пр.3. Пусть $A = \{1,9,18\},\ B = \{1,5,9\}.$

Найти $A \backslash B$.

О.4. Если $A \subseteq U$, то разность $U \backslash A = \bar{A}$ называется дополнением множества A в U.



$$\bar{A} = \{x | x \in U \text{ и } x \notin A\}$$

Свойства дополнения:

1) $A \cap U = A$;

2) $A \cup U = U$;

3) $A \cup \bar{A} = U$;

4) $A \cap \bar{A} = \emptyset$.

Дополнение $\bar{A}$ в U обозначается $\bar{\bar{A}} = U \backslash \bar{A}$.

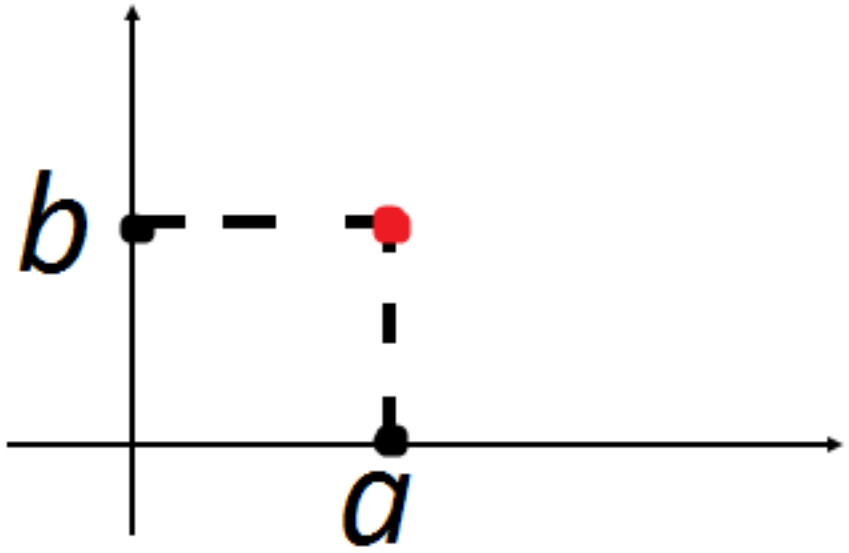
О.5. Пусть A и B – множества. Пару

$$(a, b), \text{ где } a \in A, b \in B,$$

будем называть упорядоченной парой и считать

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ и } b = d.$$

О.6. Декартовым (прямым) произведением множеств A и B называется множество $A \times B$, содержащее все упорядоченные пары (a, b), где $a \in A$, $b \in B$.



$$A \times B = \{(a, b) | a \in A \text{ и } b \in B\}$$

Пр. 4. Пусть $A = \{0,1,2\},\ B = \{3,5\}.$

Найти $A \times B$.

Т.1. Имеют место следующие свойства операций над множествами:

(1) $A \cup A = A, A \cap A = A -$ идемпотентность $\cup$ и $\cap$

(2) $A \cup B = B \cup A,$

$A \cap B = B \cap A -$ коммутативность $\cup$ и $\cap$

(3) $A \cup (B \cup C) = (A \cup B) \cup C,$

$A \cap (B \cap C) = (A \cap B) \cap C -$ ассоциативность $\cup$ и $\cap$

(4) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) -$

дистрибутивность ∪ относительно ∩ и ∩ относительно ∪

(5) $\bar{\bar{A}} = A$,

(6) $\overline{A \cup B} = \bar{A} \cap \bar{B}$,

$\overline{A \cap B} = \bar{A} \cup \bar{B} -$ законы де Моргана

Пр. 5. Докажите тождество, проиллюстрируйте его с помощью диаграмм Эйлера-Венна.

$$A \cap \bar{B} = A \setminus B$$

§19. Бинарные отношения

О.1. Бинарным отношением на множестве A называется любое подмножество R декартового произведения $A \times A$.

Если R – бинарное отношение на A и $(a, b) \in R$, то говорят, что a находится в отношении R к b. Обозначается: aRb.

О.2. Множество всех первых элементов пар из R называется областью определения отношения R и обозначается

$$DomR = \{x|\exists y: (x, y) \in R\}.$$

Множество всех вторых элементов пар из R называется областью значений отношения R и обозначается

$$ImR = \{y|\exists x: (x, y) \in R\}.$$

Пр.1. Пусть $M = \{2,3,4,5,6,7,8\}$,

$R -$ отношение делимости на M, т.е.

$$(a,b) \in R \text{ или } aRb \Leftrightarrow \ b \vdots a.$$

О.3. Бинарные отношения R и S называются равными, если они равны как множества, т.е.

$$\forall (x, y): \quad (x, y) \in R \Leftrightarrow (x, y) \in S.$$

О.4. Пусть R и S – бинарные отношения. Множество всех пар (x, y), таких что для некоторого z

$$(x, z) \in S \text{ и } (z, y) \in R$$

называется композицией отношений R и S и обозначается

$$R \circ S = \{(x, y) | \exists z: (x, z) \in S \text{ и } (z, y) \in R\}$$

Пр.2. Пусть $R = \{(1,3), (2,6), (3,9), (4,12)\}$,

$$S = \{(1,2), (2,4), (3,6)\}.$$

Т.1. Для любых бинарных отношений R, S, T верно:

$$(R \circ S) \circ T = R \circ (S \circ T).$$

О.5. Обратным к бинарному отношению R называется множество

$$R^{-1} = \{(x, y) | (y, x) \in R\}.$$

Пр.3. Пусть $R = \{(2,5), (8,15), (4,1)\}$.

Т.2. Для любых бинарных отношений R, S верно:

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}.$$

§20. Отношения эквивалентности и порядка

О.1. Бинарное отношение R на множестве A называется:

1) рефлексивным, если

$$\forall a \in A: \ \ aRa.$$

3) симметричным, если

$$\forall a, b \in A: \text{ если } aRb, \text{ то } bRa.$$

4) транзитивным, если

$$\forall a, b, c \in A: \text{ если } aRb \text{ и } bRc, \text{ то } aRc.$$

5) антисимметричным, если

$$\forall a, b \in A: \text{ если } aRb \text{ и } bRa, \text{ то } a = b.$$

Пр.1. Отношение:

1) делимости на $\mathbb{N}$:

рефлексивно ($a \vdots a, \forall a \in \mathbb{N}$),

антисимметрично (если $a \vdots b$ и $b \vdots a$, то $a = b, \forall a, b \in \mathbb{N}$)

транзитивно (если $a \vdots b$ и $b \vdots c$, то $a \vdots c$, $\forall a, b, c \in \mathbb{N}$)

2) сравнения по модулю m на $\mathbb{Z}$ рефлексивно, симметрично и транзитивно (св-во 1 §11).

О.2. Бинарное отношение называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Т.1. Если $R -$ отношение эквивалентности на A, то A распадается на непересекающиеся подмножества, такие что $\forall a, b \in A$: a, b принадлежат одному подмножеству $\Leftrightarrow aRb$.

Пр.2. $\mathbb{Z} -$ объединение непересекающихся классов вычетов по модулю m.

О.3. Бинарное отношение называется отношением частичного порядка, если оно рефлексивно, антисимметрично и транзитивно.

Множество с заданным на нем отношением частичного порядка называют частично упорядоченным (чум).

Пр.3. Отношение частичного порядка:

1) отношение делимости на $\mathbb{N}$ (см. пример 1)
2) отношение $\subseteq$ на множестве $P(A)$ всех подмножеств множества A
3) отношение $\leq$ на множестве $\mathbb{R}$

О.4. Наибольшим элементом чум A называется элемент

$$n \in A\colon\ aRn, \forall a \in A.$$

Максимальным элементом – элемент

$$m \in A\colon\ \text{если}\ mRa, \text{то}\ m = a.$$

Аналогично определяются наибольший и минимальные элементы.

З.1. Наибольший элемент является максимальным, обратное не верно. Максимальных элементов может быть много, а наибольший, если существует, единственный.

Пр.4. Пусть $M = \mathbb{N}\backslash\{1\}$,

$R -$ отношение делимости на M, т.е. $aRb \Leftrightarrow \ b \vdots a$.

§21. Отображения и их свойства. Композиция отображений

О.1. Пусть A и $B-$ произвольные множества. Отображением множества A в множество B называют всякое правило f, по которому каждому элементу множества A сопоставляют единственный элемент множества B. Обозначается: $f: A \to B$.

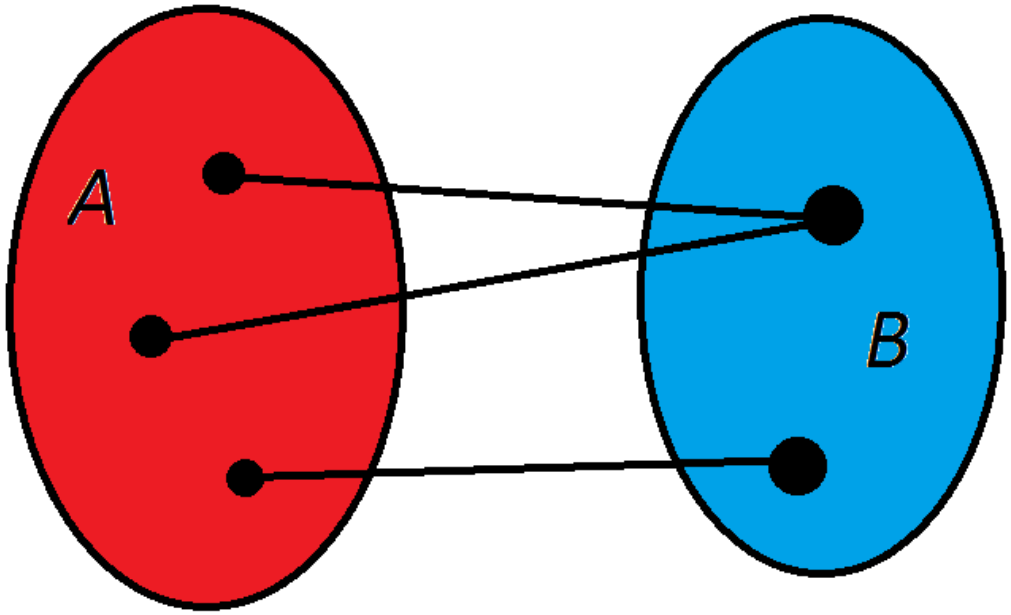
Если элементу $a \in A$ сопоставлен элемент $b \in B$, то b называют образом элемента a, а $a -$ прообразом элемента b, при отображении f и обозначают $f(a) = b$.

3.1. Из О.1. следует, что $\forall a \in A$ существует единственный образ. Но для $b \in B$ прообразов может быть много или не быть совсем.

О.2. Отображение $f: A \to B$ называется:

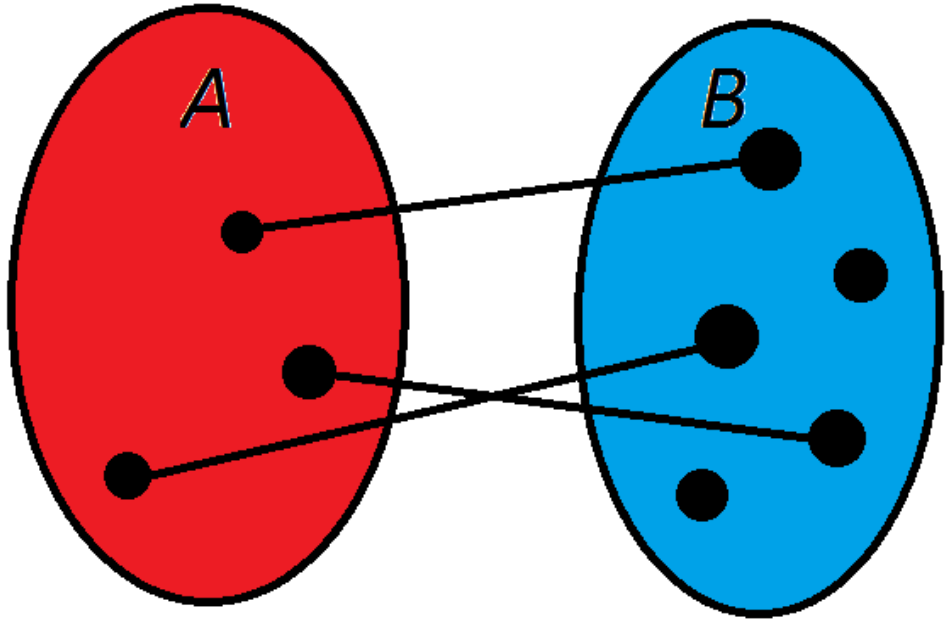
1) сюръективным (или сюръекцией), если каждый элемент из B является образом хотя бы одного элемента из A, т.е.

$$\forall b \in B \ \ \exists a \in A: \ f(a) = b \ \text{ или } f(A) = \{f(a) | a \in A\} = B$$



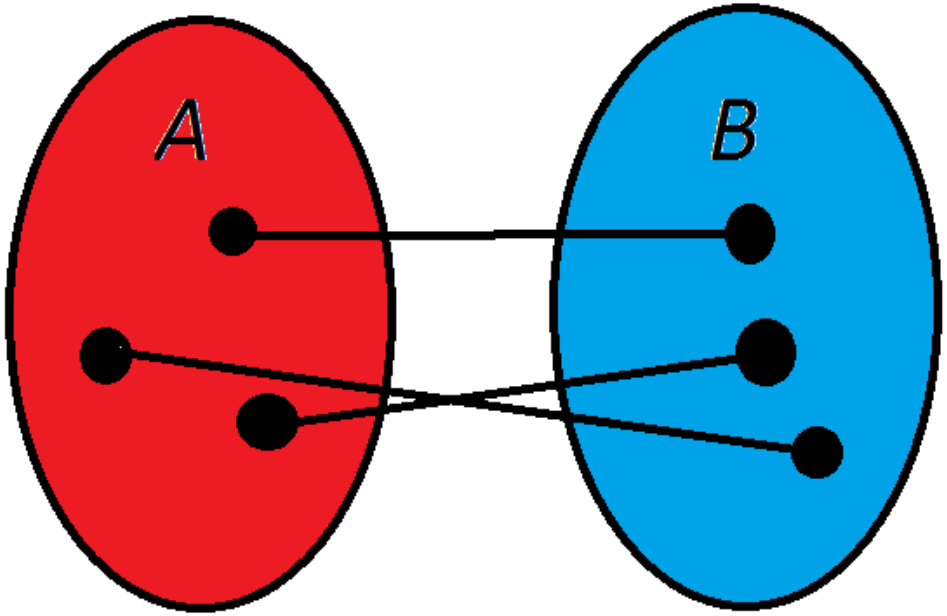
2) инъективным (или инъекцией), если образы различных элементов множества A являются различными элементами множества B, т.е.

если $a_1 \neq a_2$, то $f(a_1) \neq f(a_2), a_1, a_2 \in A, f(a_1), f(a_2) \in B$



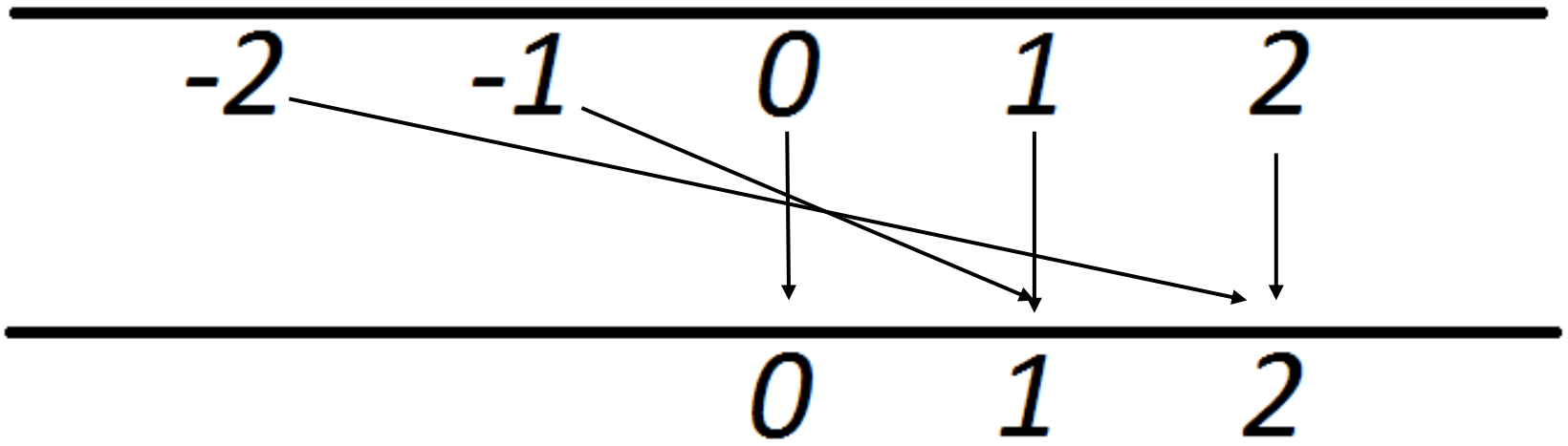
3) биективным (или биекцией), или взаимно однозначным отображением A на B, если оно сюръективно и инъективно, т.е.

$$\forall b \in B \ \exists! a \in A\colon \ f(a) = b$$



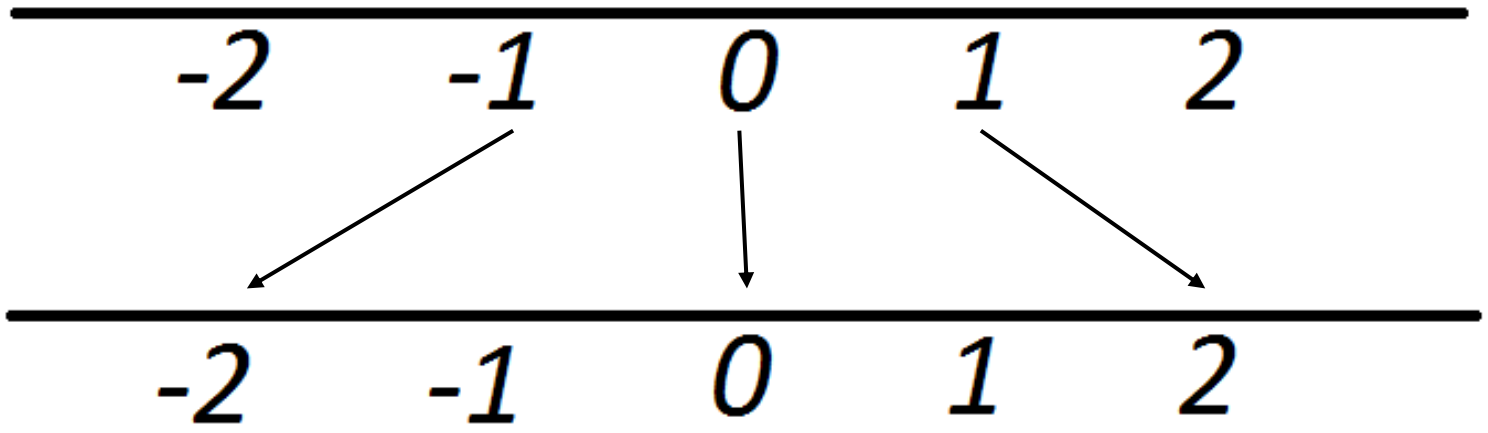
Пр.1.

1) $f_1: \mathbb{Z} \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ по правилу $f_1(a) = |a|, \forall a \in \mathbb{Z}$



f_1 −сюръекция, но не инъекция

2) $f_2: \mathbb{Z} \to \mathbb{Z}$ по правилу $f_2(a) = 2a, \forall a \in \mathbb{Z}$



$f_2 -$ инъекция, но не сюръекция

3) $f_3 : A \to A$ по правилу $f_3(a) = a, \forall a \in A$

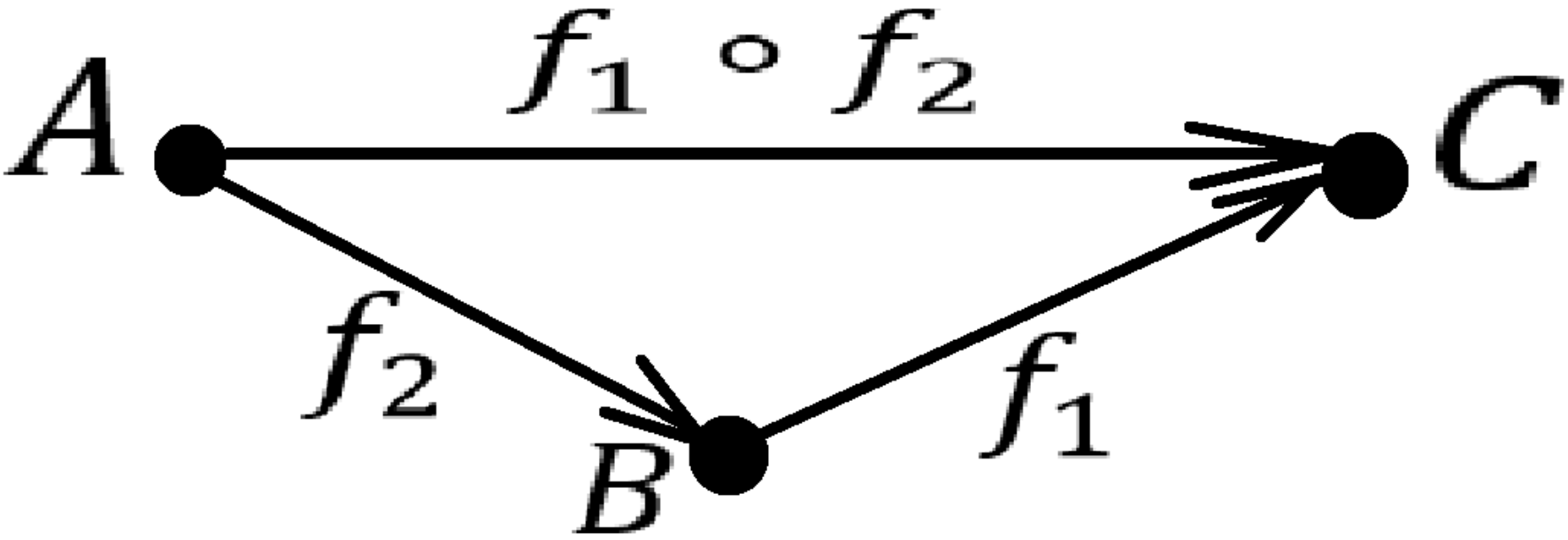
$f_3 -$ биекция и обозначается $f_3 = \varepsilon_A$.

О.3. Отображения $f_1: A \to B$ и $f_2: A \to B$ называются равными, если

$$f_1(a) = f_2(a), \forall a \in A.$$

О.4. Композицией отображений $f_1: B \to C$ и $f_2: A \to B$ называется отображение $f_1 \circ f_2: A \to C$, такое что

$$(f_1 \circ f_2)(a) = f_1\big(f_2(a)\big), \forall a \in A$$



Св-во 1. Если $f_1: A \to B$, $f_2: B \to C$, $f_3: C \to D$, то

$$(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$$

Св-во 2. Если $f_1: A \to B$, $f_2: B \to C$ сюръективны (инъективны/биективны), то $\varphi = f_2 \circ f_1$ сюръективно (инъективно/биективно).

Св-во 3. Пусть $\varphi = f_2 \circ f_1$. Если φ сюръективно, то f_2 сюръективно; если φ инъективно, то f_1 инъективно.

О.5. Отображение $f: A \to B$ называется обратимым, если

$$\exists\, f^{-1}: B \to A: \quad f \circ f^{-1} = \varepsilon_B \text{ и } f^{-1} \circ f = \varepsilon_A.$$

Отображение f^{-1} называется обратным для f.

Т.1. Отображение $f: A \to B$ обратимо $\Leftrightarrow$ $f -$ биекция

§22. Подстановки

О.1. Пусть $M = \{1,2, \dots, n\}$.

Обозначим через $S_n -$ множество всех биекций множества M на себя. Элементы из S_n называются подстановками степени n.

Подстановки удобно записывать в виде таблицы, состоящей из двух строк, заключенных в скобки. В первой строке записываются элементы множества M, во второй – соответствующие им образы.

Итак, пусть $\pi \in S_n$, тогда

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \pi(i_1) & \pi(i_2) & \dots & \pi(i_n) \end{pmatrix},$$

где $\{i_1, i_2, \dots, i_n\} = M,\ \{\pi(i_1), \pi(i_2), \dots, \pi(i_n)\} = M.$

Отметим, что поскольку при перестановке любых двух столбцов таблицы отображение множества M на себя не изменится, то в дальнейшем будем рассматривать подстановки с упорядоченной по возрастанию первой строкой, т.е.

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix},$$

где $\{\pi(1), \pi(2), \dots, \pi(n)\} = M$.

Т.1. Число различных подстановок степени n равно $n!$, т.е.

$$|S_n| = n!$$

Пр.1. Множество S_3 всех подстановок степени 3.

О.2. Пусть $\pi_1, \pi_2 \in S_n$. Произведением подстановок π_1 и π_2 называется отображение $\pi_1\pi_2$: $M \longrightarrow M$ по правилу:

$$\pi_1\pi_2(m) = \pi_1\big(\pi_2(m)\big), \forall m \in M.$$

Так как $\pi_1, \pi_2 -$ биекции, то по свойству 2 §22 $\pi_1\pi_2 \in S_n$.

Пр.2. Пусть

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3.$$

Найти $\pi_1\pi_2$.

Св-во 1. $\forall\ \pi_1, \pi_2, \pi_3 \in S_n$:

$$(\pi_1\pi_2)\pi_3 = \pi_1(\pi_2\pi_3)$$

Св-во 2. При $n > 2$: $\pi_1\pi_2 \neq \pi_2\pi_1$.

О.3. Подстановка

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n$$

называется единичной или тождественной.

О.4. Подстановка

$$\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n$$

называется обратной к подстановке π.

§23. Четная и нечетная подстановки. Транспозиции. Разложение подстановки в произведение транспозиций

О.1. Рассмотрим подстановку

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

где $j_1 = \pi(1), j_2 = \pi(2), \dots, j_n = \pi(n)$.

Вторая строка $j_1, j_2, \ldots, j_n$ этой подстановки образует перестановку на n символах. Будем говорить, что j_k и j_m образуют инверсию $< j_k, j_m >$, если:

$j_k > j_m$ и j_k стоит в перестановке раньше j_m.

Подстановка называется нечетной, если она имеет нечетное число инверсий; четной – четное число инверсий. Тождественную подстановку, которая имеет 0 инверсий, считают четной.

Пр.1. Определить четность подстановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

О.2. Подстановка, в которой меняются местами только два элемента, а все остальные остаются в естественном порядке

$$\begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & k & k+1 & \dots & n \\ 1 & 2 & \dots & i-1 & k & i+1 & \dots & i & k+1 & \dots & n \end{pmatrix}$$

называется транспозицией.

Обозначается: (ik).

Пр.2.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$$

Т.1. Число инверсий в любой транспозиции равно

$$2s + 1,$$

где s – число символов, расположенных между i и k.

Т.о. любая транспозиция является нечетной подстановкой.

Т.2. Подстановка, обратная к транспозиции, совпадает с ней самой.

Пр.3. Разложить в произведение транспозиций и определить четность

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

§24. Разложение подстановки в произведение независимых циклов

О.1. Рассмотрим подстановку

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

Будем выписывать последовательное перемещение символов в этой подстановке, начиная с 1 до тех пор, пока снова не получим 1:

$$1 \to \pi(1) \to \pi\big(\pi(1)\big) \to \cdots \to 1.$$

Если множество всех символов, входящих в эту последовательность, совпадет с $\{1, 2, \ldots, n\}$, то подстановка π называется циклом.

В противном случае выбираем наименьшее натуральное число $k \in \{1,2,\dots,n\}$, но не принадлежащее последовательности, и, начиная с k, построим новую последовательность:

$$k \to \pi(k) \to \pi\big(\pi(k)\big) \to \cdots \to k.$$

Такие перемещения символов будем называть *циклами*, а число различных элементов в каждом цикле – *длиной цикла*.

Так как любые два цикла не содержат общих элементов, то их называют *независимыми*. Любую подстановку можно однозначным образом разложить в произведение независимых циклов.

О.2. Пусть $\pi \in S_n$ и $s -$ число независимых циклов в π. Число $d = n - s$ называется декрементом подстановки π.

Несложно показать, что четность числа d совпадает с четностью самой подстановки, и d равен минимальному числу множителей в разложении этой подстановки в произведение транспозиций.

Пр.1. Определить четность подстановки, используя декремент. Разложить в произведение минимального числа транспозиций.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 6 & 5 & 1 & 8 & 7 \end{pmatrix}.$$

§25. Бинарная алгебраическая операция

О.1. Пусть M – множество. Говорят, что на M задана *бинарная алгебраическая операция* φ, если задано отображение $\varphi: M \times M \to M$, т. е. любой упорядоченной паре (a, b) элементов из M соответствует однозначно определенный элемент $c = \varphi(a, b) \in M$.

Части вместо $\varphi(a, b) = c$ пишут $c = a\varphi b$, еще чаще бинарную операцию (б.о.) обозначают специальным символом: $*$, $\circ$, $+$, $\cdot$ и т.д.

Пр.1. Является ли б.о. закон

$$a \circ b = a^b$$

на множестве $M = \mathbb{N}$? На множестве $M = \{1, 2\}$?

Б.о. на конечном множестве удобно записывать в виде таблицы.

$\circ$	a	b	…	v
a	$a\circ a$	$a\circ b$	…	$a\circ v$
b	$b\circ a$	$b\circ b$	…	$b\circ v$
⋮	…	…	…	…
v	$v\circ a$	$v\circ b$	…	$v\circ v$

Таблицы такого вида называются *таблицами Кэли*.

О.2. Б.о. $\circ$ на множестве M называется *ассоциативной*, если $\forall\, a, b, c \in M$:

$$(a \circ b) \circ c \;=\; a \circ (b \circ c),$$

и *коммутативной,* если $\forall a, b \in M$:

$$a \circ b \;=\; b \circ a.$$

Пр.2. Является ли б.о.

$$a \circ b \;=\; a^b$$

на множестве $\mathbb{N}$ коммутативной? Ассоциативной?

3.1. Если б.о. задана с помощью таблицы Кэли, то коммутативность операции легко извлечь из симметричности таблицы.

§26. Нейтральный и симметричный элементы множества. Группоид. Полугруппа. Моноид

О.1. Пусть M – непустое множество и $\circ$ – б.о. на M. Элемент $e_{\text{л}} \in M$ $(e_{\text{п}} \in M)$ называется *левым* (*правым*) *нейтральным элементом* относительно б.о. $\circ$ на M, если

$$\forall a \in M\colon e_{\text{л}} \circ a = a \,(a \circ e_{\text{п}} = a).$$

О.2. Если некоторый элемент $e \in M$ является одновременно левым и правым нейтральным элементом относительно б.о. $\circ$ на M, т. е.

$$e \circ a = a \circ e = a, \forall a \in M,$$

то его называют *нейтральным элементом*.

Пр.1. Найти правый и левый нейтральные элементы относительно б.о. $\circ$ на $\mathbb{N}$, если

$$a \circ b = a^b, \forall a, b \in \mathbb{N}.$$

Т.1. Если множество M обладает левым и правым нейтральными элементами относительно б.о. $\circ$ на M, то они совпадают между собой. В частности, если в M существует нейтральный элемент относительно б.о. $\circ$, то он в M единственен.

О.3. Пусть M – непустое множество и e – нейтральный элемент относительно б.о. $\circ$ на M.

Элемент $a_{\text{п}} \in M$ $(a_{\text{л}} \in M)$ называется *правым* (*левым*) *симметричным элементом* для $a \in M$, если

$$a \circ a_{\text{п}} = e \quad (a_{\text{л}} \circ a = \text{e}).$$

Т.2. Пусть M – непустое множество, e – нейтральный элемент в M относительно б.о. $\circ$ и операция $\circ$ ассоциативна на M. Если элемент $a \in M$ имеет в M правый и левый симметричные элементы относительно б.о. $\circ$, то они совпадают между собой. В частности, если для элемента $a \in M$ в M существует симметричный элемент относительно б.о. $\circ$, то он в M единственен.

Пр.2. Найти симметричные элементы для всех элементов множества $\mathbb{N}$ относительно б.о. $\circ$ на $\mathbb{N}$, заданной по правилу:

$$x \circ y = max(x, y), \forall x, y \in \mathbb{N}.$$

О.4. Непустое множество M с заданной на нем б.о. $\circ$ называется *группоидом*. Обозначается: $(M,\circ)$.

О.5. Если $(M,\circ)$ является группоидом и б.о. $\circ$ ассоциативна на M, то группоид M называется *полугруппой*.

О.6. Если $(M,\circ)$ является полугруппой и M обладает нейтральным элементом относительно б.о. $\circ$, то полугруппа M называется *моноидом*.

Пр.3.

(1) Пусть $M = \mathbb{N}$ с заданной на нем б.о. $\circ$:

$$a \circ b = a^b, \forall a, b \in M.$$

Тогда $(M, \circ)$ является группоидом,

$(M, \circ)$ не является полугруппой, т.к. б.о. $\circ$ не ассоциативна.

(2) Пусть $M = \mathbb{N}$ с заданной на нем б.о. $\circ$:

$$a \circ b = max(a, b), \forall a, b \in M.$$

Тогда $(M,\circ)$ является группоидом,

$(M,\circ)$ является полугруппой,

$(M,\circ)$ является моноидом.

Т.1. В полугруппе $(M, \cdot)$ произведение n элементов, где $n \geq 3$, не зависит от расстановки скобок и, значит, их вообще можно опустить.

§27. Группа. Примеры групп. Порядок элемента группы

О.1. Непустое множество G, с заданной на нем бинарной операцией $\circ$, называется *группой*, если выполняются следующие условия (аксиомы):

1) операция $\circ$ ассоциативна на множестве G, т. е.

$$\forall a, b, c \in G\colon\ (a \circ b) \circ c = a \circ (b \circ c);$$

2) в G существует нейтральный элемент e, т. е.

$$\exists e \in G\quad \forall a \in G\colon\ e \circ a = a \circ e = a;$$

3) каждый элемент в G обладает симметричным элементом в G, т. е.

$$\forall a \in G\quad \exists a' \in G\colon\ a' \circ a = a \circ a' = e.$$

Вместо общей формы записи операции $\circ$ в теории групп принято использовать обозначения операций:

$+$ – сложение (аддитивная форма записи) и

$\cdot$ – умножение (мультипликативная форма записи).

$(G,+)$	$(G,\cdot)$
1) ассоциативность: $\forall a,b,c \in G$: $(a + b) + c = a + (b + c)$	1) ассоциативность: $\forall a,b,c \in G$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2) нейтральный элемент обозначают 0 и называют *нулевым* (*нулем*): $\exists 0 \in G \quad \forall a \in G$: $0 + a = a + 0 = a$.	2) нейтральный элемент обозначают 1 и называют *единичным* (*единицей*): $\exists 1 \in G \quad \forall a \in G$: $1 \cdot a = a \cdot 1 = a$.

3)симметричный элемент обозначают $-a$ и называют *противоположным*:

$$\forall a \in G \quad \exists -a \in G:$$

$$-a + a = a + (-a) = 0.$$

G – *аддитивная*

группа.

3)симметричный элемент обозначают a^{-1} и называют *обратным*:

$$\forall a \in G \quad \exists a^{-1} \in G:$$

$$a^{-1} \cdot a = a \cdot a^{-1} = 1.$$

G – *мультипликативная*

группа.

О.2. Если б.о. $\circ$ коммутативна на G, то группу $(G,\circ)$ называют *абелевой*.

О.3. Если множество G состоит из конечного числа элементов, то группа $(G,\circ)$ называется *конечной*. Число элементов конечной группы G будет обозначать $|G|$ и называть *порядком* этой группы. Если множество G бесконечно, то группу $(G,\circ)$ называют *бесконечной*.

Пр.1.

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ – бесконечные аддитивные абелевы группы.

(2) Множество $\mathbb{Z}_m$ всех классов вычетов по модулю m – конечная аддитивная абелева группа ($|\mathbb{Z}_m| = m$):

1) Б.о. + ассоциативна на $\mathbb{Z}_m$;
2) $\bar{0}$ – нулевой элемент в $\mathbb{Z}_m$;
3) $-\bar{a} \in \mathbb{Z}_m$ – противоположный для $\bar{a} \in \mathbb{Z}_m$;
4) Б.о. + коммутативна на $\mathbb{Z}_m$.

(3) Множество S_n всех подстановок степени n – конечная мультипликативная группа ($|S_n| = n!$):

1) Б.о. $\cdot$ ассоциативна на S_n;

2) $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ – единичный элемент в S_n;

3) $\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$ – обратный элемент для $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} \in S_n$.

Группу S_n называют симметрической группой степени n.

S_n не абелева, т.к. б.о. $\cdot$ не коммутативна.

В дальнейшем, если не оговорено противное, будем рассматривать мультипликативную форму записи и обозначение операции $\cdot$ опускать.

О.4. Пусть a – элемент группы. Если существует $n \in \mathbb{N}$, такой что

$$\underbrace{aa \dots a}_{n \text{ раз}} = a^n = 1,$$

причем n является наименьшим натуральным числом с таким свойством, то n называют порядком элемента a и обозначают $|a| = n$.

Если такого натурального числа n не существует, то a называется элементом бесконечного порядка и обозначают: $|a| = \infty$.

Полагаем, что $a^0 = 1$ и $(a^{-1})^k = a^{-k}$.

Несложно доказать, что $\forall m, n \in \mathbb{Z}$:

$$a^m a^n = a^{m+n} \text{ и } (a^m)^n = a^{mn}.$$

Пр.2.

(1) $\mathbb{Z}$ – аддитивная абелева группа, $k \in \mathbb{Z}$.

(2) $\mathbb{Z}_6$ – аддитивная абелева группа.

(3) S_8 –симметрическая группа 8 степени.

Порядок подстановки равен НОК длин циклов в разложении этой подстановки.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 5 & 3 & 8 & 1 & 6 \end{pmatrix} \in S_8.$$

О.5. Элементы второго порядка в группах называют *инволюциями*.

§28. Подгруппа. Критерий подгруппы. Изоморфизм групп

О.1. Пусть $G -$ группа и $\emptyset \neq H \subseteq G$. Если H является группой относительно той же операции, которая задана на G, то H называется подгруппой группы G и обозначается $H \leq G$.

Если $H \neq G$, то подгруппу H называют собственной подгруппой в G и обозначают $H < G$.

Отметим, что каждая группа G обладает единичной подгруппой $E = \{1\}$ и подгруппой G. Эти подгруппы называют *тривиальными*.

3.1. Очевидно, что не всякое $\emptyset \neq H \subseteq G$ является подгруппой в G. Например, $G = \mathbb{Z} -$ группа, $H_1 = 2\mathbb{Z} < G$, но $H_2 = 2\mathbb{Z} + 1 \not\leq G$.

Т.1. (критерий подгруппы). Пусть G – группа и $\emptyset \neq H \subseteq G$. Тогда H является *подгруппой* в $G \Leftrightarrow$ выполняются следующие условия:

$$(1)\ \forall h_1, h_2 \in H\colon \quad h_1 h_2 \in H,$$

$$(2)\ \forall h \in H\colon \ h^{-1} \in H.$$

Пр.1. Множество A_n всех четных подстановок образуют подгруппу симметрической группы S_n.

Группу A_n будем называть знакопеременной группой.

$$|A_n| = \frac{n!}{2}.$$

3.2. Нечетные подстановки в произведении дают четную подстановку, поэтому множество нечетных подстановок не является подгруппой группы S_n.

О.3. Пусть заданы две группы $(G_1,\circ)$ и $(G_2,*)$. Группы G_1 и G_2 будем называть *изоморфными* и записывать $G_1 \cong G_2$, если существует биективное отображение φ: $G_1 \to G_2$, называемое *изоморфизмом*, для которого сохраняется операция, т. е.

$$\varphi(a \circ b) = \varphi(a) * \varphi(b), \forall a, b \in G_1.$$

Пр.2. Пусть $G_1 = \mathbb{Z},\ G_2 = 5\mathbb{Z}$.

Тогда $G_1 \cong G_2$.

§29. Кольцо. Подкольцо. Критерий подкольца. Характеристика кольца. Обратимые элементы кольца

О.1. Непустое множество K с заданными на нем б.о. + и $\cdot$ называется кольцом, если выполняются следующие условия (аксиомы):

1) $K -$ аддитивная абелева группа (аддитивная группа кольца);

2) б.о. $\cdot$ дистрибутивна на K относительно +, т.е.

$\forall a, b, c \in K: a(b + c) = ab + ac$ и $(a + b)c = ac + bc$.

Следствия из аксиом кольца:

Сл.1. $a0 = 0a = 0, \forall a \in K.$

Сл.2. $a(-b) = (-a)b = -ab, \forall a, b \in K.$

Сл.3. $a(b - c) = ab - ac$ и $(a - b)c = ac - bc,$

$\forall a, b, c \in K.$

О.2. Кольцо K называется коммутативным, если б.о. $\cdot$ коммутативна на K, т.е.

$$\forall a, b \in K: ab = ba.$$

Кольцо K называется ассоциативным, если б.о. $\cdot$ ассоциативна на K, т.е.

$$\forall a, b, c \in K: (ab)c = a(bc).$$

О.3. Кольцо K называется кольцом с единицей, если

$$\exists 1 \in K \quad \forall a \in K: a1 = 1a = a.$$

Также, как и для мультипликативной группы, доказывается, что в кольце не может быть двух различных единиц (но может не быть ни одной).

О.4. Говорят, что кольцо K имеет делители нуля, если

$$\exists a, b \in K, a \neq 0, b \neq 0: \; ab = 0.$$

Если таких элементов нет, то K – кольцо без делителей нуля.

О.5. Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется областью целостности.

Пр.1.

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ — области целостности относительно б.о. + и $\cdot$.

(2) Множество $\mathbb{Z}_m$ всех классов вычетов по модулю m – коммутативное и ассоциативное кольцо с единицей.

1) $\mathbb{Z}_m$ — аддитивная абелева группа; (см. §28)

2) операция $\cdot$ дистрибутивна относительно $+$;

3) операция $\cdot$ коммутативна и ассоциативна;

4) $\bar{1} \in \mathbb{Z}_m$ — единица кольца $\mathbb{Z}_m$.

$\bar{a} \in \mathbb{Z}_m$ обратим $\Leftrightarrow (a, m) = 1$ (см. §16)

О.6. Пусть $K-$ коммутативное ассоциативное кольцо с единицей. Если существует $n \in \mathbb{N}$, такой что

$$\underbrace{1+1+\cdots+1}_{n \text{ раз}} = 1n = 0,$$

причем n является наименьшим натуральным числом с таким свойством, то n называют характеристикой кольца K и обозначают $charK = n$.

Если такого числа n не существует, то говорят, что кольца K имеет характеристику 0 и пишут: $charK = 0$.

Пр.2. Найти:

(1) $char\mathbb{Z}, char\mathbb{Q}, char\mathbb{R}.$

(2) $char\mathbb{Z}_6$.

О.7. Пусть $K -$ кольцо и $\emptyset \neq K_1 \subseteq K$. Если K_1 является кольцом относительно тех же операций, которые заданы на K, то K_1 называется подкольцом кольца K.

Т.1. (критерий подкольца). Пусть $K -$ кольцо и $\emptyset \neq K_1 \subseteq K$. Тогда K_1 является подкольцом в $K \Leftrightarrow$ выполняются следующие условия:

$$(1)\ \forall a, b \in K_1 :\ \ a + (-b) \in K_1,$$

$$(2)\ \forall a, b \in K_1 :\ \ ab \in K_1.$$

О.8. Пусть $K -$ коммутативное и ассоциативное кольцо с единицей. Элемент $a \in K$ называется обратимым, если

$$\exists a^{-1} \in K: \ \ aa^{-1} = a^{-1}a = 1.$$

Пр.3. Найти обратимые элементы:

(1) кольца $\mathbb{Z}.$

(2) кольца $\mathbb{Z}_6$.

Т.2. Множество обратимых элементов коммутативного и ассоциативного кольца K с единицей образует мультипликативную абелеву группу K^*.

§30. Поле. Подполе. Критерий подполя. Характеристика поля

О.1. Непустое множество P с заданными на нем б.о. + и $\cdot$ называется полем, если выполняются следующие условия (аксиомы):

1) $P -$ аддитивная абелева группа;

2) $P\backslash\{0\} -$ мультипликативная абелева группа;

3) б.о. $\cdot$ дистрибутивна на P относительно +, т.е.

$$\forall a, b, c \in P\colon\ a(b + c) = ab + ac.$$

О.2. Полем называется коммутативное ассоциативное кольцо с единицей, содержащее не менее двух элементов, в котором всякий ненулевой элемент обратим.

Св-во 1. Любое поле P содержит по крайней мере два различных элемента: 0 и 1.

Св-во 2. Любое поле P не имеет делителей нуля.

Пр. 1.

(1) $\mathbb{Q}, \mathbb{R} -$ поля;

$\mathbb{Z}$ не является полем.

(2) $\mathbb{Z}_m -$ поле $\Leftrightarrow$ $m -$ простое число. Если $m -$ составное число, то в $\mathbb{Z}_m$ есть делители нуля.

О.3. Пусть $P -$ поле. Если существует $n \in \mathbb{N}$, такой что

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = 1n = 0,$$

причем n является наименьшим натуральным числом с таким свойством, то n называют характеристикой поля P и обозначают $charP = n$.

Если такого числа n не существует, то P называют полем нулевой характеристики и пишут: $charP = 0$.

Т.1. Если $charP = n \neq 0$, то $n -$ простое число.

О.4. Пусть $P -$ поле и $\emptyset \neq P_1 \subseteq P$. Если P_1 является полем относительно тех же операций, которые заданы на P, то P_1 называется подполем поля P.

Т.2. (критерий подполя). Пусть $P -$ поле и $\emptyset \neq P_1 \subseteq P$. Тогда P_1 является подполем поля $P \Leftrightarrow$ выполняются следующие условия:

$$(1)\ \forall a, b \in P_1 \colon\ a + (-b) \in P_1,$$

$$(2)\ \forall a, b \in P_1, b \neq 0 \colon\ ab^{-1} \in P_1.$$

§31. Поле комплексных чисел

О.1. Комплексными числами называются упорядоченные пары (a, b), $a, b \in \mathbb{R}$, для которых:

I. $(a, b) = (c, d) \Leftrightarrow \begin{cases} a = c, \\ b = d. \end{cases}$

II. $(a, b) + (c, d) = (a + c, b + d)$.

III. $(a, b)(c, d) = (ac - bd, ad + bc)$.

IV. $(a, 0) = a$.

Т.1. Множество $\mathbb{C} = \{(a, b) | a, b \in \mathbb{R}\}$ с заданными на нем операциями + и ·, определенными равенствами II-III, является полем.

О.2. Построенное поле $\mathbb{C}$ называют полем комплексных чисел, а его элементы – комплексными числами.

Т.2. Поле $\mathbb{C}$ содержит подполе, изоморфное полю $\mathbb{R}$.

§32. Алгебраическая форма записи комплексного числа

О.1. Обозначит $(0,1) = i$. Тогда

$$(a, b) = (a, 0) + (0, b) =$$

$$(a, 0) + (b, 0)(0,1) = a + bi,$$ где

$$i^2 = (0,1)(0,1) = (0 - 1,0 + 0) = (-1,0) = -1$$

Выражение $a + bi$ называется алгебраической формой записи комплексного числа (a, b).

Пусть $z = a + bi$. Тогда

a называется действительной частью числа z и обозначается Rez,

b называется мнимой частью числа z и обозначается Imz,

i называется мнимой единицей.

Операции над комплексными числами в алгебраической форме:

1) Сложение

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

2) Умножение

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Пр.1. Записать $z_1 = (2, -3)$ и $z_2 = (-5,7)$ в алгебраической форме, найти

$$Rez_1, Rez_2, Imz_1, Imz_2, z_1 + z_2, z_1 z_2.$$

Т.1. Пусть $z_1, z_2 \in \mathbb{C}$. Тогда существует единственное

$$z = (-z_1) + z_2 \in \mathbb{C}:\ z_1 + z = z_2\ .$$

Обозначается: $z = z_2 - z_1$.

В алгебраической форме:

$$(a + bi) - (c + di) = (a - c) + (b - d)i$$

Пр.2. Пусть $z_1 = 2 - 4i$ и $z_2 = -7 + 6i$.

Найти $z_1 - z_2$.

Т.2. Пусть $z_1, z_2 \in \mathbb{C}, z_2 \neq 0$. Тогда существует единственное

$$z = z_1 {z_2}^{-1} \in \mathbb{C}\colon\ z_2 z = z_1\ .$$

Обозначается: $z = \frac{z_1}{z_2}$.

В алгебраической форме:

$$\frac{a+bi}{c+di} = (a+bi)(c+di)^{-1} =$$

$$= \left(\frac{ac}{c^2+d^2} + \frac{bd}{c^2+d^2}\right) + \left(\frac{-ad}{c^2+d^2} + \frac{bc}{c^2+d^2}\right) i$$

О.2. Комплексное число $a - bi$ называется сопряженным числу $z = a + bi$. Обозначается:

$$\bar{z} = a - bi.$$

Вычисление $\frac{z_1}{z_2}$ есть умножение числителя z_1 и знаменателя z_2 на число $\overline{z_2}$, сопряженное знаменателю.

Пр.3. Пусть $z_1 = 1 + 3i$ и $z_2 = 1 + i$.

Найти $\frac{z_1}{z_2}$.

Т.3. Для любых $z_1, z_2 \in \mathbb{C}$ верно:

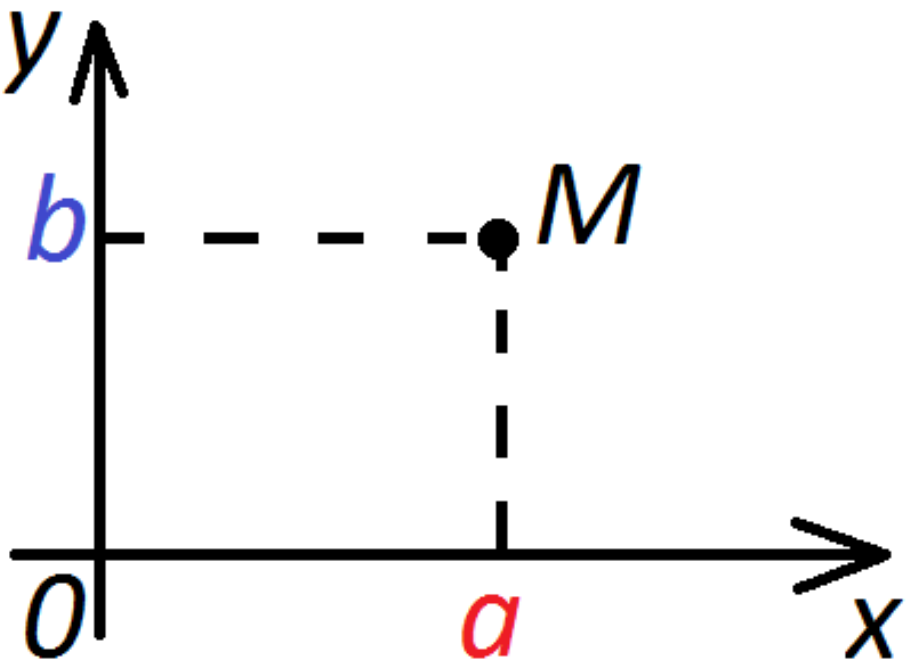
(1) $\overline{\overline{z_1}} = z_1;$

(2) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2};$

(3) $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$

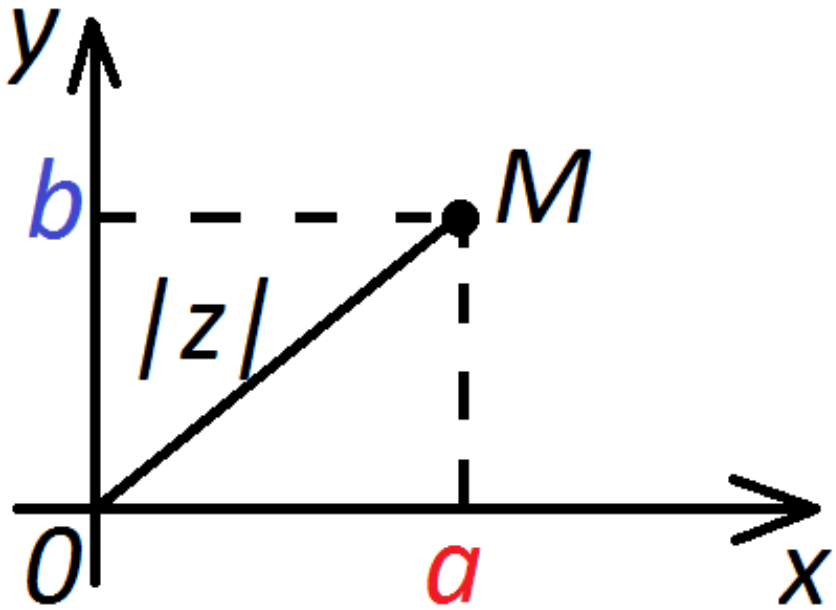
§33. Тригонометрическая форма записи комплексного числа

О.1. Возьмем на плоскости декартову систему координат и изобразим на ней комплексное число $z = a + bi$ точкой $M(a, b)$.



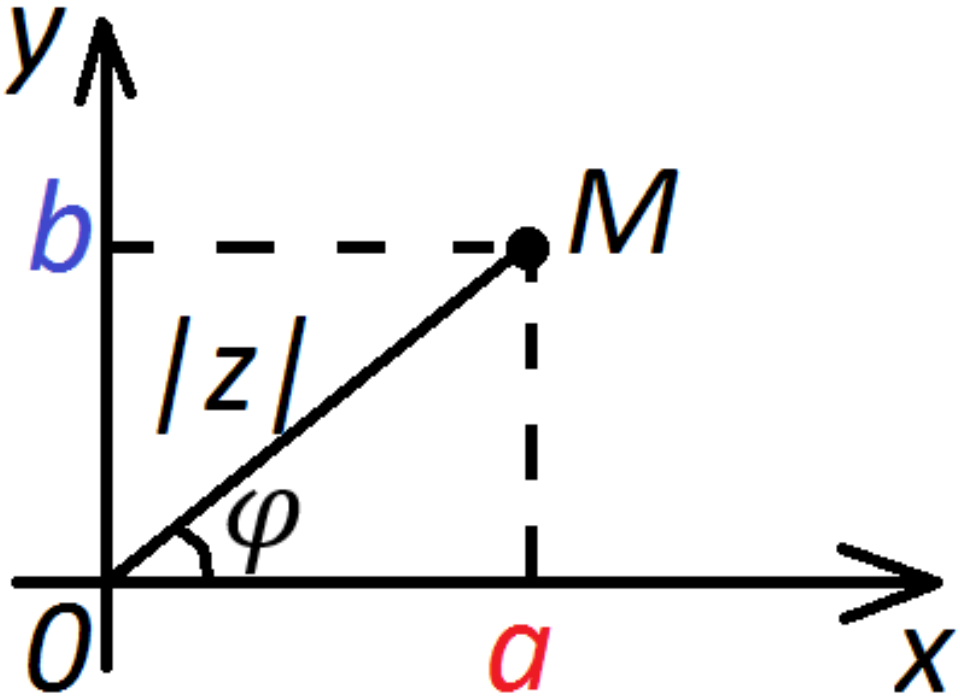
Плоскость, на которой изображаются комплексные числа, называется комплексной. Ось абсцисс называется действительной осью, а ось ординат – мнимой.

О.2. Длина отрезка OM называется модулем комплексного числа z и обозначается $|z|$.



$$|z| = \sqrt{a^2 + b^2}.$$

О.3. Угол φ, на который нужно повернуть ось OX до совпадения ее направления с направление вектора OM, называется аргументом числа z и обозначается $argz = \varphi$.



$$cos\varphi = \frac{a}{\sqrt{a^2 + b^2}} = \frac{a}{|Z|}$$

$$sin\varphi = \frac{b}{\sqrt{a^2 + b^2}} = \frac{b}{|Z|}$$

3.1. Аргумент комплексного числа определен неоднозначно, т.е. угол φ может быть отсчитан несколькими способами.

Пусть $\varphi_0 -$ наименьшее положительное значение аргумента. Получим все значения φ:

1) в положительном направлении:

$$\varphi = \varphi_0 + 2\pi m, m \in \mathbb{Z}.$$

2) в отрицательном направлении:

$$\varphi = -(2\pi - \varphi_0) + 2\pi n, n \in \mathbb{Z}.$$

Т.о. все возможные значения аргумента:

$$\varphi = \varphi_0 + 2\pi k, k \in \mathbb{Z}.$$

Если необходимо выбрать определенное значение, накладываем ограничения:

$$0 \leq \varphi < 2\pi \text{ или } -\pi < \varphi \leq \pi.$$

О.4. Пусть $z = a + bi$,

$$|z| = \sqrt{a^2 + b^2},\ cos\varphi = \frac{a}{|z|},\ sin\varphi = \frac{b}{|z|}.$$

Тогда $z = |z|(cos\varphi + isin\varphi)$.

Такая форма числа $z \in \mathbb{C}$ называется тригонометрической.

Пр.1. Записать числа в тригонометрической форме.

(1) $z = 1,$

(2) $z = -1 + i,$

(3) $z = -i.$

§34. Операции над комплексными числами в тригонометрической форме

О.1. Рассмотрим умножение комплексных чисел в тригонометрической форме.

Пусть $z_1 = |z_1|(cos\varphi_1 + isin\varphi_1)$,

$z_2 = |z_2|(cos\varphi_2 + isin\varphi_2)$. Тогда

$$z_1 z_2 = |z_1||z_2|(\cos(\varphi_1 + \varphi_2) + isin(\varphi_1 + \varphi_2)).$$

Т.о. при умножении комплексных чисел в тригонометрической форме их модули умножаются, а аргументы складываются.

О.2. Пусть $z = |z|(cos\varphi + isin\varphi), n \in \mathbb{N}, n \neq 1.$

Тогда

$$z^n = |z|^n(cosn\varphi + isinn\varphi).$$

Если $z = 1$, то имеем формулу Муавра:

$$(cos\varphi + isin\varphi)^n = cosn\varphi + isinn\varphi.$$

Пр.1. Выразить $cos2x$ и $sin2x$ через $cosx$ и $sinx$.

О.3. Рассмотрим деление комплексных чисел в тригонометрической форме.

Пусть $z_1 = |z_1|(cos\varphi_1 + isin\varphi_1)$,

$z_2 = |z_2|(cos\varphi_2 + isin\varphi_2)$. Тогда

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + isin(\varphi_1 - \varphi_2)).$$

Т.о. при делении комплексных чисел в тригонометрической форме их модули делятся, а аргументы вычитаются.

Пр.2. Записать числа

$$z_1 = -1 + i, \;\; z_2 = \sqrt{3} + i$$

в тригонометрической форме и найти:

(1) $z_1 z_2$,

(2) $\dfrac{z_1}{z_2}$,

(3) z_1^{20}.

§35. Извлечение корней из комплексных чисел

Пусть $z = |z|(cos\varphi + isin\varphi) \in \mathbb{C},\ n \in \mathbb{N}, n \neq 1.$

Тогда

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(cos\frac{\varphi+2\pi k}{n} + isin\frac{\varphi+2\pi k}{n}\right),$$

$$k \in \mathbb{Z}.$$

Т.1. Пусть $z \in \mathbb{C}, \quad n \in \mathbb{N}, n \neq 1.$ Тогда $\sqrt[n]{z}$ имеет n различных значений, которые находятся по формуле:

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(cos\frac{\varphi+2\pi k}{n} + isin\frac{\varphi+2\pi k}{n}\right),$$

$$k = 0,1, \dots, n-1.$$

3.1. Все значения $\sqrt[n]{z}$ лежат на окружности с центром в начале координат радиуса $\sqrt[n]{|z|}$ и делят окружность на n равных частей.

Пр.1. Найти $\sqrt[4]{-16i}$.

МОДУЛЬ-3

«Матрицы и определители»

§36. Матрицы. Операции сложения матриц и умножения матрицы на число.

О.1. Матрицей размера $m \times n$ (или $m \times n$-матрицей) над полем P называется прямоугольная таблица чисел, содержащая m строк и n столбцов.

Матрицы обозначаются заглавными латинскими буквами, а их элементы – малыми с двумя индексами: первый – номер строки, второй – номер столбца, в котором расположен элемент.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

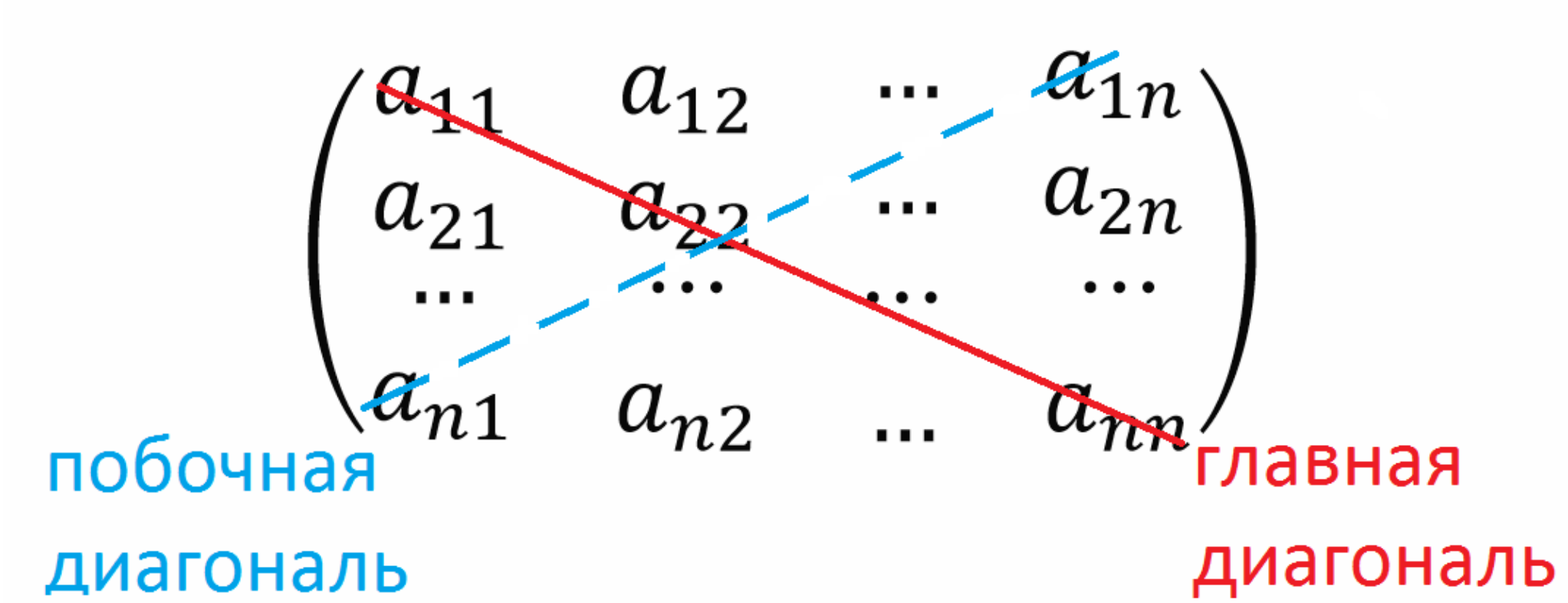
или кратко $A = (a_{ij})_{m\times n},\ a_{ij} \in P,$

$$i = 1,2,\ldots,m, j = 1,2,\ldots,n.$$

О.2. Матрицы $A = \left(a_{ij}\right)_{m\times n}$ и $B = \left(b_{ij}\right)_{m\times n}$ называются равными, если $a_{ij} = b_{ij}, \quad i = 1,2,\dots,m,\ j = 1,2,\dots,n.$ Обозначается: $A = B$.

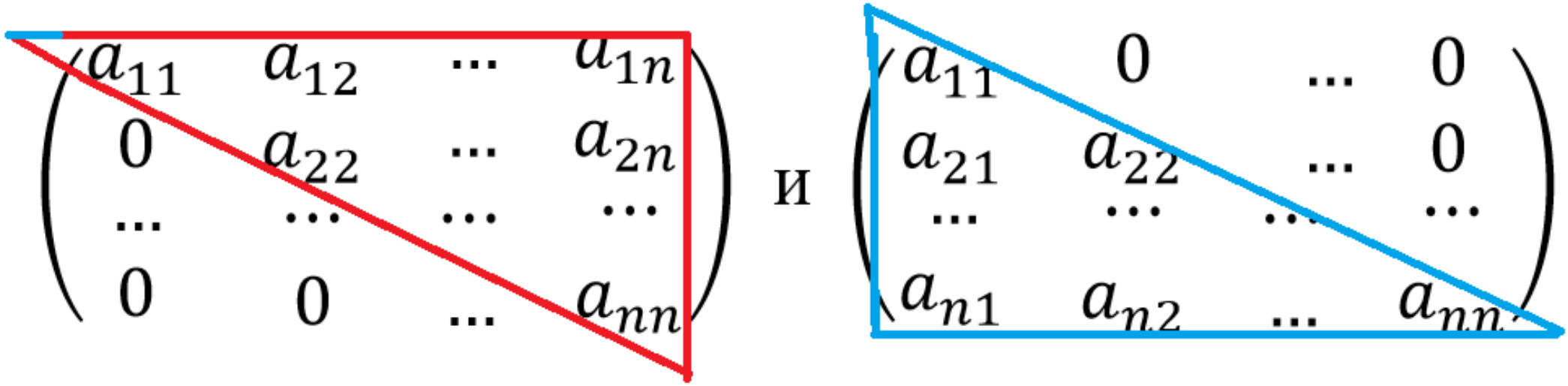
О.3. Матрица размера $n \times n$ называется квадратной матрицей n-го порядка.

Квадратная матрица имеет две диагонали:



О.4. Матрица размера $1 \times n$ называется матрицей-строкой; размера $n \times 1$ – матрицей-столбцом.

О.5. Квадратные матрицы, у которых ниже (выше) главной диагонали все элементы равны нулю, называются соответственно верхне- и нижнетреугольными.



О.6. Квадратная матрица называется диагональной, если все ее элементы, находящиеся вне главной диагонали, равны нулю.

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

О.7. Диагональная матрица называется единичной, если все ее элементы на главной диагонали равны 1.

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Матрицы любого размера называется нулевой, если все ее элементы равны 0.

$$O = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

О.8. Суммой матриц $A = (a_{ij})_{m\times n}$ и $B = (b_{ij})_{m\times n}$ называется матрица $C = (c_{ij})_{m\times n}$, в которой

$$c_{ij} = a_{ij} + b_{ij},\ i = 1,2,\dots,m,\ j = 1,2,\dots,n.$$

Обозначается: $A + B = C$.

О.9. Произведением матрицы $A = (a_{ij})_{m\times n}$ на элемент $k \in P$ называется матрица $B = (b_{ij})_{m\times n}$, в которой

$$b_{ij} = ka_{ij}\ i = 1,2,\dots,m, j = 1,2,\dots,n.$$

Обозначается: $kA = B$.

Пр.1. Дано:

$$A = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 5 & 6 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 4 \\ 2 & 5 & 1 \end{pmatrix}.$$

Найти: 1) $A + B$,

2) $5A$.

Т.1. Пусть $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$, $O = (0)_{m\times n}$. Тогда операции сложения матриц и умножения матрицы на число обладают следующими свойствами:

1) $A + B = B + A$ (коммутативность +);

2) $(A + B) + C = A + (B + C)$ (ассоциативность +);

3) $A + O = A$;

4) $A + (-1)A = O$;

5) $k(A + B) = kA + kB$;

6) $(\lambda + \mu)A = \lambda A + \mu A$;

7) $(\lambda\mu)A = \lambda(\mu A)$; 8) $1A = A$.

Сл.1. Множество $M_{m\times n}(P)$ всех матриц размерности $m \times n$ над полем P является аддитивной абелевой группой.

§37. Операция умножения матриц

О.1. Произведением матрицы $A = (a_{ij})_{m\times n}$ на матрицу $B = (b_{ij})_{n\times k}$ называется матрица $C = (c_{ij})_{m\times k}$, в которой

$$c_{ij} = (a_{i1}\ a_{i2}\ \dots\ a_{in})\begin{pmatrix} b_{1j} \\ b_{2j} \\ \dots \\ b_{nj} \end{pmatrix} =$$

i-ая строка A

j-ый столбец B

$$= a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{s=1}^{n} a_{is}b_{sj},$$

$$i = 1,2,\dots,m, j = 1,2,\dots,n.$$

Обозначается: $AB = C$.

3.1. Согласно этому определению перемножать можно только те матрицы, в которых число столбцов первой матрицы равно числу строк второй матрицы. Если это условие нарушено, то перемножать матрицы нельзя.

Пр.1. Найти AB, BA, AA, если

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 3 & -1 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 1 & -2 \\ 2 & 3 \\ -1 & 0 \end{pmatrix}.$$

Св-во 1. Обобщенный закон дистрибутивности:

$$k\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} ka_i$$

Св-во 2.

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{k} a_{ij}\right) = \sum_{j=1}^{k}\left(\sum_{i=1}^{m} a_{ij}\right)$$

Т.1. Если существуют AB и BC, то $(AB)C = A(BC)$ – ассоциативность умножения матриц.

Т.2. Пусть $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$, $C = (c_{ij})_{n\times k}$. Тогда $(A + B)C = AC + BC$ – дистрибутивность умножения относительно сложения.

Сл.1. Множество $M_{n\times n}(P)$ квадратных матриц над полем P является ассоциативным кольцом с единицей.

§38. Транспонирование матриц. Основные свойства транспонирования

О.1. Транспонированием матрицы $A = \left(a_{ij}\right)_{m\times n}$ называется преобразование матрицы A в матрицу $A^T = \left({a_{ij}}^T\right)_{n\times m}$, в которой строки и столбцы поменялись местами с сохранением порядка, т.е.

$${a_{ij}}^T = a_{ji},\ i = 1,2,\dots,m, j = 1,2,\dots,n.$$

Матрица A^T называется транспонированной относительно A.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}_{m \times n}$$

Строки пишем столбцами

$$A^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}_{n \times m}$$

Пр.1. Найти A^T, если $A = \begin{pmatrix} 4 & 2 \\ 3 & -1 \\ 1 & 2 \\ 0 & 8 \end{pmatrix}$.

Рассмотрим основные свойства операции транспонирования.

Св-во 1. $(A^T)^T = A$.

Св-во 2. $(A + B)^T = A^T + B^T$.

Св-во 3. $(kA)^T = kA^T$.

Св-во 4. $(AB)^T = B^T A^T$.

§39. Понятие перестановки. Четные и нечетные перестановки. Теорема о четности перестановки

О.1. Пусть $M -$ конечное множество, элементы которого пронумеруем. Располагая элементы этого множества некоторым образом, получим расположение номеров

$$j_1, j_2, \dots, j_n.$$

Это расположение будем обозначать $I = (j_1, j_2, \dots, j_n)$ и называть перестановкой степени n.

Т.1. Число P_n всех перестановок степени n равно $n!$.

О.2. Перемена местами любых двух элементов в перестановке называется транспозицией этих элементов.

О.3. Пусть $I = (j_1, j_2, \dots, j_n) -$ перестановка степени $n > 1$. Пара чисел j_r и j_s образуют инверсию, если $j_r > j_s$ и j_r стоит в перестановке раньше j_s.

Обозначается: $< j_r, j_s >$, число инверсий $\sigma(I)$.

О.4. Перестановка называется нечетной, если число инверсий в ней нечетно; и четной, если число инверсий в ней четно или равно 0.

Пр.1. Определить число инверсий и четность перестановки.

$$I = (5,3,4,2,1).$$

Т.1. При любой транспозиции меняется четность подстановки.

Сл.1. При $n > 1$ число четных подстановок степени n равно число нечетных, и равно $\frac{n!}{2}$.

Т.2. Пусть в перестановке I символ j находится на i-ом месте и $I_1 -$ перестановка, полученная из I удалением символа j.

$$\text{Тогда } (-1)^{\sigma(I)} = (-1)^{\sigma(I_1)+i+j},$$

т.е. перестановки имеют одинаковую четность, если $i + j$ четно; и противоположные четности, если $i + j$ нечетно.

§40. Определители n-го порядка. Миноры и алгебраические дополнения. Разложение определителей по строке (столбцу)

О.1. Определителем n-го порядка матрицы $A = (a_{ij})_{n\times n}$ над полем P называется элемент поля P(число), равный сумме $n!$ членов вида

$$(-1)^{\sigma(I)} a_{1j_1} a_{2j_2} \dots a_{nj_n} \ (1),$$

где $I = (j_1, j_2, \dots, j_n)$.

Обозначается:

$$\Delta = |A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

$$|A| = \sum_I (-1)^{\sigma(I)} a_{1j_1} a_{2j_2} \ldots a_{nj_n},$$

где (1) – члены определителя и суммирование ведется по всем $I \in P_n$.

Пусть $n = 2$, тогда

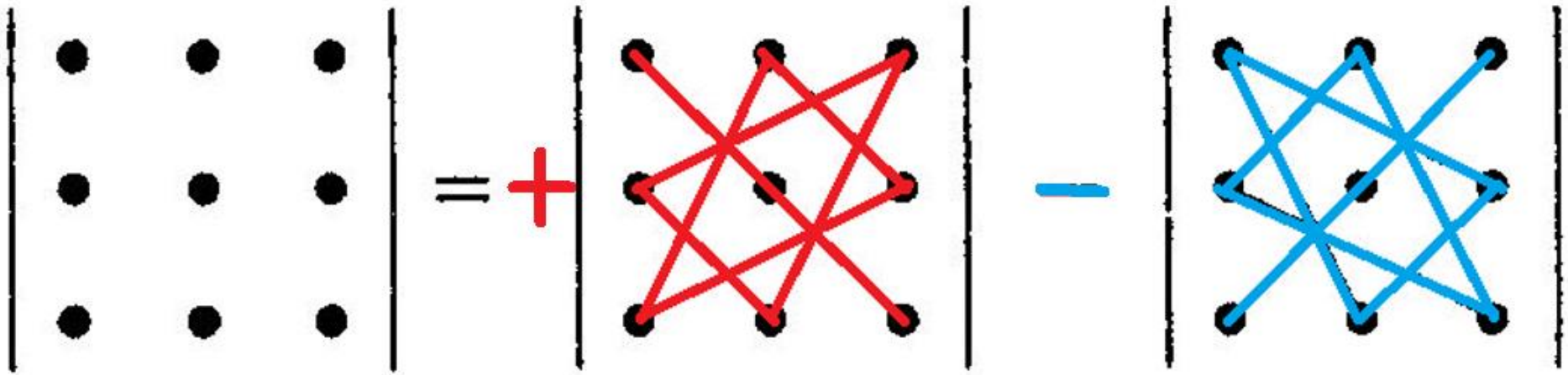
$$\Delta = |A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Пусть $n = 3$, тогда

$$\Delta = |A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$

$$-a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32},$$



(основания равнобедренных треугольников параллельны главной диагонали)

(основания треугольников параллельны побочной диагонали)

3.1. Как первые индексы, задающие номера строк, так и вторые индексы, задающие номера столбцов, составляют перестановки. Значит, при составлении членов вида (1) берется в точности по одному элементу из каждой строки и каждого столбца.

Пр.1. Вычислить:

1) $\begin{vmatrix} 1 & 2 \\ 3 & -1 \end{vmatrix}$

2) $\begin{vmatrix} 1 & 0 & -1 \\ 2 & 1 & 0 \\ -1 & 0 & 0 \end{vmatrix}$.

О.2. Пусть a_{ij} — элемент матрицы A n-го порядка, $|A| = \Delta$. Сгруппируем в Δ все слагаемые содержащие a_{ij} и вынесем a_{ij} за скобки. В скобке получим число A_{ij}, которое называется алгебраическим дополнением к a_{ij} в Δ.

Т.1. Определитель квадратной матрицы равен сумме произведений всех элементов какой-либо ряда (столбца или строки) на их алгебраические дополнения, т.е.

(2) $\Delta = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} -$

разложение определителя по i-ой строке;

(3) $\Delta = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} -$

разложение определителя по j-ому столбцу.

О.3. Пусть $\Delta -$ определитель n-го порядка, $a_{ij} -$ его элемент. Вычеркнем в Δ i-ую строку и j-ый столбец. Получим определитель $(n-1)$-го порядка, который будем обозначать M_{ij} и называть минором элемента a_{ij}.

Т.2. $$A_{ij} = (-1)^{i+j} M_{ij},$$

$$i = 1,2,\dots,n, j = 1,2,\dots,n.$$

Пр.2. Вычислить:

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{vmatrix}$$

§41. Основные свойства определителя

Св-во 1. Если определитель содержит нулевую строку (столбец), то он равен 0.

Св-во 2. Если все элементы некоторой строки (столбца) умножить на одно и тоже число k, то и определитель умножится на число k, т.е. общий множитель строки (столбца) можно вынести за знак определителя.

Св-во 3. От перестановки любых двух строк (столбцов) определитель лишь меняет знак.

Св-во 4. Если определитель имеет две равных строки (столбца), то он равен 0.

Св-во 5. Определитель, содержащий две пропорциональные строки (столбца), равен 0.

Св-во 6.

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ b_1 + c_1 & b_2 + c_2 & \dots & b_n + c_n \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ b_1 & b_2 & \dots & b_n \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_n \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Св-во 7. Определитель не изменится, если к элементам какой-либо строки (столбца) прибавить элементы другой строки (столбца), умноженные на некоторое число.

Св-во 8. Определитель не меняется при транспонировании.

Св-во 9. Определитель диагональной матрицы равен произведению ее элементов, стоящих на главной диагонали.

Св-во 10. Определитель треугольной матрицы равен произведению ее элементов, стоящих на главной диагонали.

Пр.1. Вычислить:

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 1 \\ 3 & 3 & 1 & 1 & 1 \\ 4 & 4 & 4 & 1 & 1 \\ 5 & 5 & 5 & 5 & 1 \end{vmatrix}$$

§42. Обратимые матрицы

О.1. Пусть $A = (a_{ij})_{n\times n}$. Если существует ${A^{-1}}_{n\times n}$, такая что

$$AA^{-1} = A^{-1}A = E,$$

то A^{-1} называется обратной к матрице A,

а матрица A – обратимой.

Т.1. Если в разложении определителя по строке (столбцу)

$$\Delta = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}$$

аалгебраические дополнения A_{ij} заменить на алгебраические дополнения $A_{sj}, s \neq i,$ любой другой строки (столбца), то

$$a_{i1}A_{s1} + a_{i2}A_{s2} + \cdots + a_{in}A_{sn} = 0$$

Т.2. Пусть $A = \left(a_{ij}\right)_{n\times n}$. Если $|A| \neq 0$, то A обратима.

О.2. Квадратная матрица называется невырожденной, если ее определитель не равен нулю.

Св-во 1. Если A обратима, то A^{-1} единственна.

Св-во 2. Если A и B обратимы, то AB обратима и

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Св-во 3. Если A обратима, то A^{-1} обратима и

$$(A^{-1})^{-1} = A.$$

Св-во 4. Если A обратима, то A^T обратима и

$$(A^T)^{-1} = (A^{-1})^T.$$

Пр.1. Найти A^{-1}, если

$$A = \begin{pmatrix} 3 & -1 & 0 \\ -2 & 1 & 1 \\ 2 & -1 & 4 \end{pmatrix}$$

§43. Элементарные матрицы и их свойства

О.1. Рассмотрим $E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & \dots & & \\ 0 & 0 & \dots & 1 \end{pmatrix}$ и применим к ней элементарные преобразования:

(1) умножение любой строки (столбца) матрицы на ненулевой число.

(2) прибавление к любой строке (столбцу) любой другой строки, умноженной на ненулевое число.

Матрицы, полученные в результате этих преобразований, называются элементарными.

После (1):

$$E_{\lambda(i)} = \begin{pmatrix} 1 & 0 & \dots & & & 0 \\ & \dots & & & & \\ 0 & 0 & \dots & \lambda & \dots & 0 \\ & & & & & \\ 0 & 0 & \dots & & & 1 \end{pmatrix} \; i - \text{ая строка}$$

После (2):

$$E_{(i)+\lambda(j)} = \begin{pmatrix} 1 & 0 & \dots & & 0 \\ & \dots & & & \\ 0 & 0 & \dots 1 & \lambda \cdots & 0 \\ & & & & \\ 0 & 0 & \dots & & 1 \end{pmatrix}$$

j-ый столбец

$i-$ая строка

1 на главной диагонали,

λ на месте ij,

0 все остальные элементы.

Свойства элементарных матриц.

Св-во 1. Любая элементарная матрица обратима.

Св-во 2. Произведение любого числа элементарных матриц есть обратимая матрица.

Св-во 3. Пусть $A = (a_{ij})_{n\times n}$. Любое элементарное преобразование строк матрицы можно записать как умножение матрицы A слева на некоторую элементарную матрицу.

Пр.1. Пусть $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

1) Выполним элементарные преобразования.

2) Запишем преобразования через умножение элементарных матриц.

§44. Ранг матрицы. Нахождение обратной матрицы с помощью элементарных преобразований

О.1. Пусть $A = (a_{ij})_{m\times n}$. Вычеркиванием каких-либо строк и столбцов можно вычленить квадратные подматрицы k-го порядка ($k \leq \min(m,n)$). Определители таких подматриц называются минорами k-го порядка матрицы A.

О.2. Рангом матрицы $A_{m\times n}$ называется наивысший порядок отличных от нуля миноров этой матрицы.

Обозначается: $r(A)$.

Пр.1. Найти ранг матрицы

$$A = \begin{pmatrix} 1 & 3 & 0 & 4 \\ 3 & 2 & 0 & 1 \\ 2 & -1 & 0 & -3 \end{pmatrix}$$

3.1. Вычисление ранга матрицы по О.2 слишком трудоемко, поэтому будем использовать элементарные преобразования:

1) умножение всех элементов строки (столбца) на ненулевое число;

2) изменение порядка строк (столбцов);

3) прибавление к строке (столбцу) другой строки (столбца), умноженной на некоторое число;

4) транспонирование матрицы.

Т.1. Ранг матрицы не изменится при элементарных преобразованиях матрицы.

С помощью элементарных преобразований приведем матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

к ступенчатому виду.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22}^{*} & \dots & a_{2n}^{*} \\ \dots & \dots & \dots & \dots \\ 0 & 0 \dots & a_{rr}^{*} & a_{rn}^{*} \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Ранг ступенчатой матрицы равен числу ее ненулевых строк r (найдется минор r-го порядка отличный от нуля).

Пр.2. Привести матрицу к ступенчатому виду и найти ее ранг.

$$A = \begin{pmatrix} 4 & 0 & -8 & 0 \\ 2 & 0 & -4 & 0 \\ 3 & 0 & -6 & 0 \\ 1 & 0 & -2 & 0 \end{pmatrix}$$

Т.2. Пусть $A = (a_{ij})_{n\times n}$ и $r(A) = n$. Тогда с помощью элементарных преобразований матрицу A можно привести к единичной матрице.

Т.2. Пусть $A = (a_{ij})_{n\times n}$ и $r(A) = n$. Тогда матрица A обратима.

Сл. 1. Если какая-нибудь цепочка элементарных преобразований приводит A к E, то эта же цепочка приводит E к A^{-1}.

Пр.3. Найти A^{-1}, если

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 1 & -2 \\ 1 & 0 & 1 \end{pmatrix}.$$

§45. Определитель произведения матриц

Т.1. Если $E_\varphi -$ элементарные матрицы $n \times n$,

$B = (b_{ij})_{n\times n}$, то

$$\left|E_\varphi \cdot B\right| = |E_\varphi| \cdot |B|.$$

Сл.1. Если $E_1, E_2, \ldots, E_n$ – элементарные $(n \times n)$-матрицы, то

$$|E_1 \cdot E_2 \cdot \ldots \cdot E_n| = |E_1| \cdot |E_2| \cdot \ldots \cdot |E_n|.$$

Сл.2. $|E_1 \cdot E_2 \cdot \ldots \cdot E_n \cdot B| = |E_1| \cdot |E_2| \cdot \ldots \cdot |E_n| \cdot |B|.$

Т.2. Пусть $A = (a_{ij})_{n\times n}$, $B = (b_{ij})_{n\times n}$, то

$$|A \cdot B| = |A| \cdot |B|.$$

Сл. 3. Если матрица A обратима, то

$$|A^{-1}| = \frac{1}{|A|}.$$

Сл. 4. Матрица $A = (a_{ij})_{n\times n}$ является невырожденной $\Leftrightarrow r(A) = n$.

Пр.1. Множество $GL_n(P) = \{A \in M_n(P) || A| \neq 0\}$ всех квадратных невырожденных матриц n-го порядка с элементами из поля P является мультипликативной группой, которую называют *полной или общей линейной группой* степени n над полем P.

Пр.2. Матрицы с единичными определителями образуют группу $SL_n(P) = \{A \in GL_n(P) || A| = 1\}$, которая называется *специальной линейной группой* степени n над полем P.