Содержание

1 Аксиоматика множеств: отношения $\in$ и $\subseteq$

В теории множеств (Set) вводится исходное понятие отношения принадлежности.

- **Отношение принадлежности ($\in$):** Запись $x \in y$ означает, что объект x является элементом объекта y. Это отношение, вообще говоря, не транзитивно.
- **Отношение включения ($\subseteq$):** Объект u называется подмножеством объекта w (запись $u \subseteq w$), если каждый элемент u также является элементом w ($\forall x \in u \Rightarrow x \in w$). Если $u \subseteq w$ и $w \nsubseteq u$, то u называется строгим подмножеством w ($u \subset w$).

Отношение включения $\subseteq$ обладает следующими свойствами:

- **Рефлексивность:** $u \subseteq u$.
- **Антисимметричность:** $v \subseteq w$ и $w \subseteq v \Rightarrow v = w$ (это свойство является определением равенства объектов в Set).
- **Транзитивность:** $u \subseteq v$ и $v \subseteq w \Rightarrow u \subseteq w$.

2 Аксиоматика множеств: система аксиом ZF+C

Наиболее известной системой аксиом теории множеств является система Цермело-Френкеля (ZF), дополненная аксиомой выбора (C). В этой системе есть единственный тип объектов (множество) и единственный предикат ($\in$).

Основные аксиомы системы $ZF + C$:

- **ZF-1 (Аксиома экстенсиональности):** Два множества равны, если они содержат одни и те же элементы.
- **ZF-2 (Аксиома существования):** Существует пустое множество $\emptyset$, не содержащее элементов.
- **ZF-3 (Аксиома неупорядоченных пар):** Для любых x и y существует множество $\{x, y\}$.
- **ZF-4 (Аксиома объединения):** Для любого множества множеств y_α существует их объединение $z = \bigcup y_\alpha$.
- **ZF-5 (Аксиома бесконечности):** Существует множество ω, такое что $\emptyset \in \omega$ и $\forall x \in \omega \Rightarrow \{x, \{x\}\} \in \omega$.
- **ZF-6 (Аксиома подмножеств):** Для любого множества x и свойства P существует множество $y \subseteq x$, состоящее из всех элементов x, обладающих свойством P.
- **ZF-7 (Аксиома степени):** Для любого x существует множество ω, состоящее из всех подмножеств x ($y \in \omega \Leftrightarrow y \subseteq x$).
- **ZF-8 (Аксиома выбора, C):** Для любого объединения x непересекающихся непустых множеств x_α, существует подмножество $y \subseteq x$, которое пересекается с каждым x_α ровно по одному элементу.
- **ZF-9 (Аксиома регулярности):** Запрещает конструкции вида $x \in x$.

3 Аксиома упорядоченной пары и модель упорядоченной пары

Существование упорядоченной пары (x, y), в отличие от неупорядоченной $\{x, y\}$ (гарантируемой ZF-3), не следует напрямую из аксиом ZF.

- **Аксиома упорядоченной пары (OP):** Равенство $(x, y) = (u, v)$ имеет место тогда и только тогда, когда $x = u$ и $y = v$. Элемент x называется первой компонентой, y — второй.

- **Модель по Куратовскому:** В рамках ZF упорядоченная пара моделируется (определяется) как специфическое множество:

  $$(x, y) \triangleq \{\{x\}, \{x, y\}\}$$

  Эта модель удовлетворяет аксиоме OP.

4 Декартово произведение множеств

- **Прямое (декартово) произведение двух множеств** X и Y — это множество всех упорядоченных пар (x, y), где $x \in X$ и $y \in Y$:

  $$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

- **Декартово произведение конечного числа множеств** $X_1, \ldots, X_n$ — это множество упорядоченных списков (кортежей):

  $$X_1 \times \cdots \times X_n = \{(x_1, \ldots, x_n) : x_i \in X_i\}$$

Существование $X \times Y$ (при модели Куратовского) гарантируется аксиомами ZF.

5 Понятие бинарного отношения на множестве, примеры

Бинарное отношение между множествами X и Y — это тройка (X, Y, R), где R является подмножеством декартова произведения $X \times Y$ $(R \subseteq X \times Y)$.

Если $(x, y) \in R$, говорят, что x находится в отношении R с y, и пишут xRy. Если $X = Y$, говорят об отношении на X.

Примеры:

1. **Отношение принадлежности:** $xRX \Leftrightarrow x \in X$.

2. **Отношение вхождения (включения):** $ARB \Leftrightarrow A \subseteq B$.

3. **Отношение равенства:** $xRy \Leftrightarrow x = y$.

6 Композиция отношений, свойства отношений

Композиция отношений: Пусть $R \in Rel(X,Y)$ и $S \in Rel(Y,Z)$. Их композицией называется отношение $S \circ R \in Rel(X,Z)$, такое что:

$$S \circ R = \{(x,z) \in X \times Z : \exists y \in Y, (x,y) \in R \text{ и } (y,z) \in S\}$$

Основные свойства отношений (для $R \in Rel(X)$):

1. **Рефлексивность:** Отношение рефлексивно, если оно содержит диагональ $\Delta = \{(x,x) : x \in X\}$.
2. **Симметричность:** Отношение R симметрично, если оно совпадает со своим обратным R' (где R' определяется как $(x,y) \in R \Rightarrow (y,x) \in R'$).
3. **Транзитивность:** Отношение R транзитивно, если $R \circ R \subseteq R$.
4. **Антисимметричность:** Отношение R антисимметрично, если $R' \cap R = \Delta_X$.

7 Отображение множеств как бинарное отношение

Отображение (функция) — это бинарное отношение $F \in Rel(X,Y)$, обладающее особым свойством:

$$\forall x \in X \text{ существует } \textbf{единственный} y \in Y, \text{ такой что } xFy$$

Для отображений используют специальную запись: $F : X \to Y$ и $F(x) = y$.

- X называется **областью определения** (доменом) $D(F)$.
- Y называется **областью значений** (кообластью) $C(F)$.

8 Внутренний закон композиции и свойства элементов относительно закона

Внутренний закон композиции на множестве M — это отображение $M \times M \to M$. Композицию элементов (x,y) обозначают $x+y$, $x \cdot y$, $x \circ y$ и т.д..

Свойства элементов относительно закона $\circ$:

1. **Нейтральный элемент:**
   - *Левый* (e_L): $e_L \circ x = x$, $\forall x \in M$.
   - *Правый* (e_R): $x \circ e_R = x$, $\forall x \in M$.
   - Если существуют оба, они совпадают, и элемент e называется просто нейтральным.
2. **Идемпотентный элемент:** Элемент x идемпотентен, если $x \circ x = x$.
3. **Регулярный элемент:**
   - *Левый* (y_L): $y_L \circ x_1 = y_L \circ x_2 \Rightarrow x_1 = x_2$.
   - *Правый* (y_R): $x_1 \circ y_R = x_2 \circ y_R \Rightarrow x_1 = x_2$.

4. **Обратимый элемент:** (Требует наличия e)

   - *Левый обратный* (z_L): $z_L \circ x = e$.
   - *Правый обратный* (z_R): $x \circ z_R = e$.
   - Если закон ассоциативен, левый и правый обратные совпадают.

5. **Поглощающий элемент (θ):** $\forall x \in M, x \circ \theta = \theta \circ x = \theta$.

9 Свойства внутреннего закона композиции: ассоциативность, коммутативность

- **Ассоциативность:** Закон $\circ$ ассоциативен, если $\forall x, y, z \in M$ выполняется равенство $(x \circ y) \circ z = x \circ (y \circ z)$.

- **Коммутативность:** Элементы x, y называются перестановочными, если $x \circ y = y \circ x$. Если это верно для любой пары элементов, закон $\circ$ называется коммутативным.

10 Внешний закон композиции и его согласование с внутренним законом

Внешний закон композиции — это отображение $\Omega \times M \to M$, где Ω — множество операторов. Действие оператора $\alpha \in \Omega$ на $x \in M$ обозначают αx, $\alpha(x)$ и т.д..

Согласование: Пусть на M заданы внутренний закон $\circ$ и внешний закон (с операторами Ω). Пусть также на M задан *второй* внутренний закон $*$. Внешний закон согласован с внутренним ($\circ$), если $\forall x, y \in M, \alpha \in \Omega$ выполняется:

$$\alpha(x \circ y) = \alpha(x) * \alpha(y)$$

11 Основные структуры с одним законом композиции

1. **Магма:** Множество, наделенное (одним) внутренним законом композиции.

2. **Полугруппа:** Магма, закон композиции в которой ассоциативен.

3. **Моноид:** Полугруппа, содержащая нейтральный элемент.

12 Структура группы: определение и примеры

Группа — это непустое множество G с внутренним законом композиции ($G \times G \to G$), удовлетворяющее трем аксиомам:

- **G1 (Ассоциативность):** $\forall x, y, z \in G, (xy)z = x(yz)$.

- **G2 (Нейтральный элемент):** $\exists e \in G : \forall x \in G, xe = x = ex$.

- **G3 (Обратный элемент):** $\forall x \in G, \exists x^{-1} \in G : xx^{-1} = e = x^{-1}x$.

Если операция также коммутативна ($xy = yx$), группа называется **абелевой**.

Примеры:

- **Неабелевы:** Группа симметрий треугольника D_3, симметрическая группа S_n.
- **Абелевы:** Аддитивная группа целых чисел $(\mathbb{Z}, +)$; мультипликативная группа вещественных чисел $(\mathbb{R}^*, \cdot)$; булева группа $(2^X, \Delta)$ (симметрическая разность).

13 Гомоморфизм групп: основные определения и свойства

Гомоморфизм групп — это отображение $\sigma : G \to G'$, которое сохраняет структуру:

1. $\sigma(xy) = \sigma(x)\sigma(y)$
2. $\sigma(e_G) = e_{G'}$

Свойство: Гомоморфизм также сохраняет обратные элементы: $\sigma(x^{-1}) = \sigma(x)^{-1}$.
Основные определения:

- **Инъекция (вложение):** $f(x) = f(y) \Rightarrow x = y$.
- **Сюръекция:** $\forall y \in N, \exists x \in M : f(x) = y$.
- **Биекция:** Отображение, являющееся одновременно инъекцией и сюръекцией.
- **Изоморфизм:** Гомоморфизм σ, для которого существует обратный гомоморфизм χ. Группы G и G' в этом случае называются изоморфными ($G \simeq G'$).
- **Автоморфизм:** Изоморфизм группы на саму себя ($Aut(G)$).

14 Ядро и образ гомоморфизма. Сюрьективность и инъективность

Пусть $\sigma : G \to G'$ — гомоморфизм групп.

- **Ядро (Kernel):** Множество элементов G, которые отображаются в нейтральный элемент G':
$$\ker \sigma = \{g \in G : \sigma(g) = e'\}$$
Ядро $\ker \sigma$ само является группой.
- **Образ (Image):** Множество элементов G', которые "достижимы"из G:
$$Im\sigma = \{g' \in G' : \exists g \in G, \sigma(g) = g'\}$$
Образ $Im\sigma$ также является группой.

Связь с инъективностью/сюръективностью:

- **Инъективность:** Гомоморфизм σ инъективен $\iff$ его ядро тривиально ($\ker \sigma = \{e_G\}$).
- **Сюръективность:** Гомоморфизм σ сюръективен $\iff$ его образ совпадает со всей кообластью ($Im\sigma = G'$).

15 Подгруппа и смежные классы группы по подгруппе

- **Подгруппа:** H является подгруппой G ($H \leq G$), если $H \subseteq G$ и H сама имеет структуру группы, индуцированную законом G. (Тривиальная подгруппа $\{e\}$ и несобственная G).
- **Отношение эквивалентности:** Подгруппа H задает отношение $x \sim y \iff xy^{-1} \in H$. (Оно рефлексивно, симметрично и транзитивно).
- **Смежные классы:** Классы эквивалентности по этому отношению.
  - **Правый смежный класс:** $Hx = \{hx : h \in H\}$. Обозначается $[x]_R$.
  - **Левый смежный класс:** $xH = \{xh : h \in H\}$. Обозначается $[x]_L$.
- Смежные классы либо не пересекаются, либо совпадают.

16 Нормальная подгруппа. Фактор-группа

- **Нормальная подгруппа:** Подгруппа H называется нормальной ($H \triangleleft G$), если ее левые и правые смежные классы совпадают: $\forall x \in G, xH = Hx$.
  - Любая подгруппа абелевой группы нормальна.
  - Ядро любого гомоморфизма σ является нормальной подгруппой ($\ker \sigma \triangleleft G$).
- **Фактор-группа:** Если $H \triangleleft G$, то множество смежных классов G/H образует группу (называемую фактор-группой).
  - **Операция:** $\overline{x} \cdot \overline{y} = \overline{xy}$ (корректно определена из-за нормальности).
  - **Нейтральный элемент:** H (или $\overline{e}$).
  - **Обратный элемент:** $\overline{x}^{-1} = \overline{x^{-1}}$.

17 Канонический гомоморфизм. Теорема об изоморфизме

- **Канонический гомоморфизм:** Для $H \triangleleft G$ существует гомоморфизм $\varphi : G \to G/H$, определяемый как $\varphi(x) = \overline{x} = xH$.
  - Этот гомоморфизм сюръективен ($Im\varphi = G/H$).
  - Его ядро — $\ker \varphi = H$.
- **Теорема об изоморфизме:** Пусть $\sigma : G \to G'$ — гомоморфизм групп. Тогда:

$$G/\ker \sigma \simeq Im\sigma$$

(Фактор-группа по ядру изоморфна образу).

18 Согласование внутренних законов: дистрибутивность

Пусть на M задано два закона: $\circ$ и $*$.

- Закон $\circ$ называется **дистрибутивным слева** относительно $*$, если $\forall x, y, z \in M$:

$$x \circ (y * z) = (x \circ y) * (x \circ z)$$

- Закон $\circ$ называется **дистрибутивным справа** относительно $*$, если $\forall x, y, z \in M$:

$$(y * z) \circ x = (y \circ x) * (z \circ x)$$

19 Кольцо и подкольцо: определение и примеры

(Подразумевается ассоциативное коммутативное кольцо с единицей). **Кольцо** R — это множество с двумя операциями $(+, \cdot)$, удовлетворяющее аксиомам:

1. $(R, +)$ — **абелева группа:**
   - Ассоциативность сложения (A1).
   - Существование нуля (A2).
   - Существование противоположного (A3).
2. $(R, \cdot)$ — **коммутативный моноид:**
   - Ассоциативность умножения (M1).
   - Существование единицы (M2).
   - Коммутативность умножения (M3).
3. **Согласование (Дистрибутивность):** Умножение дистрибутивно относительно сложения (D1, D2).

Примеры:

- Целые числа $\mathbb{Z}$.
- Гауссово кольцо $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}, i^2 = -1\}$.
- Кольцо многочленов $\mathbb{Z}[x]$.

Подкольцо: $S \subseteq R$ называется подкольцом, если S является абелевой подгруппой $(R, +)$ и S содержит единицу 1_R.

20 Гомоморфизм колец: определение, ядро, образ

Гомоморфизм колец — это отображение $f : R \to R'$, сохраняющее *всю* структуру:

1. Сохранение сложения: $f(x + y) = f(x) + f(y)$.
2. Сохранение умножения: $f(xy) = f(x) \cdot f(y)$.
3. Сохранение единицы: $f(1_R) = 1_{R'}$.

- **Образ (Imf):** Является подкольцом в R'.
- **Ядро ($\ker f$):** Ядро f (элементы, отображающиеся в $0_{R'}$) является:
  1. Нормальной подгруппой $(R, +)$.
  2. Обладает поглощением: $\forall x \in R, \forall y \in \ker f \Rightarrow xy \in \ker f$. (т.е. ядро гомоморфизма колец — это идеал).

21 Идеал и фактор-кольцо. Кольцо вычетов кольца Z

- **Идеал:** J в кольце R — это аддитивная подгруппа $J \leq (R, +)$, обладающая свойством поглощения: $\forall x \in R, \forall y \in J \Rightarrow xy \in J$ (т.е. $RJ \subseteq J$).
- **Фактор-кольцо (R/J):** Идеал J порождает отношение эквивалентности $x \sim y \iff x - y \in J$.
  - Фактор-множество R/J (состоящее из классов $\overline{x} = x + J$) само образует кольцо.
  - Операции: $\overline{x} + \overline{y} = \overline{x + y}$ и $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$.
  - Нулевой элемент — класс $\overline{0} = J$.
- **Кольцо вычетов $\mathbb{Z}$:** Это фактор-кольцо $\mathbb{Z}$ по идеалу $(m) = m\mathbb{Z}$, обозначаемое $\mathbb{Z}/m\mathbb{Z}$. Его элементы — классы вычетов по модулю m: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

22 Делители нуля, нильпотенты и обратимые элементы в кольце

1. **Делитель нуля:** Элемент $x \neq 0$, для которого $\exists y \neq 0$ такой, что $xy = 0$. (Пример: $\overline{2}$ и $\overline{3}$ в $\mathbb{Z}/6\mathbb{Z}$).
2. **Нильпотент:** Элемент $z \neq 0$, для которого $\exists n \in \mathbb{N} : z^n = 0$. (Всякий нильпотент является делителем нуля, но не наоборот).
3. **Обратимый элемент (Единица):** Элемент $u \in R$, для которого $\exists v \in R : uv = 1$. Множество обратимых элементов R^* образует мультипликативную группу.

23 Малая теорема Ферма и теорема Эйлера

Эти теоремы следуют из конечности мультипликативной группы $\mathbb{Z}_m^*$.

- **Малая теорема Ферма:** Если p — простое число (тогда $|\mathbb{Z}_p^*| = p - 1$), то $\forall a \in \mathbb{N}$ (не делящемся на p), $a^{p-1} \equiv 1 \pmod{p}$.
- **Теорема Эйлера:** Если m составное (тогда $|\mathbb{Z}_m^*| = \varphi(m)$), $\forall a \in \mathbb{N}$ (взаимно простом с m), $a^{\varphi(m)} \equiv 1 \pmod{m}$.

24 Простой идеал. Область целостности

- **Область целостности:** Коммутативное кольцо, в котором нет делителей нуля. (Примеры: $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ для простого p).
- **Простой идеал:** Идеал $\mathfrak{p} \leq R$, который удовлетворяет двум условиям:
  1. $\mathfrak{p} \neq (1)$ (не совпадает со всем кольцом);
  2. $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ или $y \in \mathfrak{p}$.
- **Связь:** Идеал $\mathfrak{p}$ является простым $\iff$ фактор-кольцо $R/\mathfrak{p}$ является областью целостности.

25 Поле. Эквивалентные определения поля

- **Определение:** Поле $\daleth$ — это (коммутативное) кольцо, в котором каждый ненулевой элемент обратим.
- **Следствие:** Всякое поле является областью целостности.

Эквивалентные определения (для ненулевого кольца R):

1. R — поле.
2. В R нет идеалов, кроме (0) и (1).
3. Любой гомоморфизм из R в ненулевое кольцо инъективен.

26 Сумма и пересечение идеалов

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы кольца R.

- **Сумма идеалов:** $\mathfrak{a} + \mathfrak{b} = \{x + y : x \in \mathfrak{a}, y \in \mathfrak{b}\}$. Сумма идеалов также является идеалом.
- **Пересечение идеалов:** $\mathfrak{a} \cap \mathfrak{b} = \{x \in R : x \in \mathfrak{a}$ и $x \in \mathfrak{b}\}$. Пересечение идеалов также является идеалом.

Пример в $\mathbb{Z}$: $(m) + (n) = (gcd(m, n))$ и $(m) \cap (n) = (lcm(m, n))$.

27 Максимальный идеал. Поле как фактор-кольцо по максимальному идеалу

- **Максимальный идеал:** Идеал $\mathfrak{m}$ называется максимальным, если:
  1. $\mathfrak{m} \neq (1)$ (не совпадает со всем кольцом);
  2. Не существует другого идеала $\mathfrak{a}$, который бы строго лежал между $\mathfrak{m}$ и R (т.е. $\nexists \mathfrak{a} : \mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$).
- **Теорема:** Идеал $\mathfrak{m}$ кольца R является максимальным $\iff$ фактор-кольцо $R/\mathfrak{m}$ является полем.
- **Следствие:** Любой максимальный идеал является простым (так как любое поле — область целостности).

28 Комплексные числа: определение, алгебраическая форма

- **Определение:** Комплексное число z — это элемент декартова произведения $\mathbb{R} \times \mathbb{R}$, то есть $z = (a, b)$, где $a, b \in \mathbb{R}$. Множество $\mathbb{C}$ наделено двумя операциями:
  1. **Сложение:** $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$.
  2. **Умножение:** $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.
- Множество $\mathbb{C}$ с этими операциями образует **поле**. (Нейтральный по сложению $0_{\mathbb{C}} = (0, 0)$, по умножению $1_{\mathbb{C}} = (1, 0)$).
- **Алгебраическая форма:** $z = a + ib$.
  - i — **мнимая единица**, символ, обладающий свойством $i^2 = -1$.
  - $a = \Re z$ — вещественная часть.
  - $b = \Im z$ — мнимая часть.

29 Комплексная плоскость: тригонометрическая и показательная форма

- **Комплексная плоскость:** Интерпретация $z = (a, b)$ как точки на плоскости с вещественной (a) и мнимой (b) осями.
- Точку (a, b) можно также задать полярными координатами (ρ, ψ):
  - $a = \rho \cos \psi$, $b = \rho \sin \psi$.
  - $\rho = \sqrt{a^2 + b^2} = |z|$ — **модуль**.
  - $\psi = arg(z)$ — **аргумент** (угол от вещественной оси).
- **Тригонометрическая форма:** $z = \rho(\cos \psi + i \sin \psi)$.
- **Показательная форма:** $z = \rho e^{i\psi}$. (Формулы Эйлера связывают $e^{i\psi}$ с $\cos \psi$ и $\sin \psi$).

30 Определение кольца многочленов $\daleth[x]$

Пусть $\daleth$ — поле.

- **Многочлен** $p(x)$ — это формальная бесконечная сумма $p(x) = \sum_{n=0}^{\infty} a_n x^n$, где $a_i \in \daleth$ и лишь конечное число a_i не равны нулю.
- Множество $\daleth[x]$ образует **коммутативное ассоциативное кольцо** с операциями:
  1. **Сложение:** $h(x) = \sum c_k x^k$, где $c_k = a_k + b_k$.
  2. **Умножение:** $g(x) = \sum d_j x^j$, где $d_j = \sum_{i=0}^{j} a_i b_{j-i}$.
- **Степень** $deg(p)$ — максимальный n, при котором $a_n \neq 0$. Для $0(x)$ $deg(0) = -\infty$.

31 Делимость в $\daleth[x]$. Область главных идеалов

- **Теорема о делении с остатком:** $\forall p, q \in \daleth[x]$ $(q \neq 0)$, существуют **единственные** $g, r \in \daleth[x]$ такие, что $p = g \cdot q + r$ и $deg(r) < deg(q)$.
- **Делимость:** q делит p $(q|p)$, если $r = 0$, т.е. $\exists h : p = h \cdot q$. Эквивалентно: $p \in (q)$.
- **Область главных идеалов (PID):** Кольцо $\daleth[x]$ является областью главных идеалов.
  - Это следует из теоремы о делении: любой идеал J порождается многочленом $q \in J$ минимальной степени. Любой $p \in J$ при делении на q должен дать $r = 0$ (иначе $r \in J$ и $deg(r) < deg(q)$, что противоречит минимальности), значит $p = g \cdot q$ и $J = (q)$.

32 Разложение НОД в кольце многочленов

- Связь НОД и идеалов: $(p_1) + (p_2) = (d)$, где $d = gcd(p_1, p_2)$.
- **Теорема (Тождество Безу):** Так как $d \in (d)$, по определению суммы идеалов d можно представить в виде $d = q_1 p_1 + q_2 p_2$.
- **Формулировка:** Для $p_1, p_2 \in \daleth[x]$ и $d = gcd(p_1, p_2)$, существуют $q_1, q_2 \in \daleth[x]$ такие, что $p_1 q_1 + p_2 q_2 = d$.

33 Корень многочлена. Теоремы Виета и Безу

- **Корень:** $\alpha \in \daleth$ называется корнем $p \in \daleth[x]$ кратности m, если $p(x)$ делится на $(x - \alpha)^m$, но не делится на $(x - \alpha)^{m+1}$.
- **Теорема Безу:** Остаток от деления $p(x)$ на $(x - \alpha)$ равен $p(\alpha)$.
- **Следствие (Теорема о корне):** α является корнем $p(x) \iff (x - \alpha)|p(x)$.
- **Теорема Виета:** Устанавливает связь между коэффициентами многочлена $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ и его корнями $x_1, \ldots, x_n$.
  - Сумма корней: $x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n}$
  - Сумма попарных произведений: $x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n = \frac{a_{n-2}}{a_n}$
  - ...
  - Произведение всех корней: $x_1 x_2 \ldots x_n = (-1)^n \frac{a_0}{a_n}$

34 Кольцо матриц: определения и примеры

Множество прямоугольных $m \times n$ матриц с элементами из поля $\daleth$ обозначается $Mat_\neg(m, n)$.

- **Сложение матриц** (для $A, B \in Mat_\neg(m, n)$): $C = A + B$, где $c_{i,j} = a_{i,j} + b_{i,j}$. Относительно сложения $Mat_\neg(m, n)$ является абелевой группой.
- **Умножение матриц** (для $A \in Mat_\neg(m, p)$ и $B \in Mat_\neg(p, n)$): $C = A \cdot B$, где $c_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j}$. Умножение ассоциативно, но некоммутативно.

Множество **квадратных матриц** $Mat_{\neg}(n)$ с операциями сложения и умножения образует **ассоциативное некоммутативное кольцо**.

- **Единичная матрица** E является нейтральным элементом по умножению.
- **Нильпотентная матрица** N: квадратная матрица, для которой $N^m = \theta$ (нулевая матрица) для некоторого m, но $N^{m-1} \neq \theta$.
- **Обратимая матрица** A: квадратная матрица, для которой $\exists B, C$ такие, что $A \cdot B = E = C \cdot A$.

Пример: Существует изоморфизм $\sigma : \mathbb{C} \to Mat_{\mathbb{R}}(2)$, который сопоставляет $a + ib$ матрице вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

35 Определитель матрицы: определение и свойства

Определителем $det(A)$ квадратной матрицы A называется число, которое ставится ей в соответствие индуктивно (разложение Лапласа):

- $det(A_1) = a$.
- $det(A_2) = \det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$.
- $det(A_m) = \sum_{i=1}^{m} (-1)^{i+j} \cdot a_{i,j} \cdot M_{i,j}$ (разложение по j-му столбцу).

Здесь $M_{i,j}$ — **дополнительный минор**, т.е. определитель матрицы, полученной вычеркиванием i-ой строки и j-го столбца.

Свойства определителя:

- При перестановке строк (E1) определитель меняет знак.
- При умножении строки на $\lambda \neq 0$ (E2) определитель умножается на λ.
- При прибавлении к строке другой, умноженной на число (E3), определитель не меняется.
- Определитель с двумя одинаковыми строками равен нулю.
- $det(A \cdot B) = det(A) \cdot det(B)$.
- $det(A^T) = det(A)$ (определитель транспонированной матрицы равен исходному).

Критерий обратимости: Матрица A обратима ($\exists A^{-1}$) $\iff det(A) \neq 0$.

36 Система линейных уравнений: основные определения

Линейным алгебраическим уравнением (СЛАУ) с n неизвестными $(x_1, \dots, x_n)$ над полем ⅂ называется уравнение вида:

$$a_1x^1 + a_2x^2 + \cdots + a_nx^n = b$$

где $a_i \in$ ⅂ — коэффициенты, а $b \in$ ⅂ — свободный член.

Системой называется совокупность из m таких уравнений.

- **Решение СЛАУ:** Упорядоченный набор чисел $(x_0^1, \dots, x_0^n)$, который является решением каждого уравнения системы.
- **Совместная** система: имеет хотя бы одно решение.
- **Несовместная** система: не имеет решений.

Матричная форма: СЛАУ можно записать в виде $S \cdot X = B$, где S — матрица коэффициентов, X — столбец неизвестных, B — столбец свободных членов.

37 Расширенная матрица. Метод Гаусса

- **Матрица системы (S):** Матрица $m \times n$, составленная из коэффициентов a_{ij}.
- **Расширенная матрица ($\tilde{S}$):** Матрица S, к которой справа добавлен столбец свободных членов b_i.

Метод Гаусса — это алгоритм приведения расширенной матрицы к **ступенчатому виду** с помощью **элементарных преобразований строк**. Эти преобразования не меняют множества решений системы.

Элементарные преобразования:

1. Прибавление к одной строке другой, умноженной на число.
2. Перестановка двух строк.
3. Умножение строки на число, отличное от нуля.

Ступенчатая матрица — это матрица, где:

- Номера ведущих (первых ненулевых) элементов ее ненулевых строк строго возрастают.
- Нулевые строки, если они есть, стоят в конце.

Анализ решения (по ступенчатому виду): Пусть r — ранг (число ненулевых строк) матрицы S, $\tilde{r}$ — ранг расширенной матрицы $\tilde{S}$, n — число неизвестных.

- Если $\tilde{r} = r+1$ (ведущий элемент в столбце свободных членов), система **несовместна**.
- Если $\tilde{r} = r = n$, система имеет **единственное решение**.
- Если $\tilde{r} = r < n$, система имеет **множество решений** (есть $n - r$ свободных переменных).