Алгебра. ИТМО. 1 курс, 2024-25

# Глава 0. Основные понятия

1. Кольцо, поле, типы колец.

Кольцо и поле

• Пусть K — множество, элементы которого мы будем называть числами. На множестве K определены две операции + : K × K → K и · : K × K → K.

1) Ассоциативность + ∀a, b, c ∈ K (a + b) + c = a + (b + c).

2) Коммутативность + ∀a, b ∈ K a + b = b + a.

3) Ноль ∃ 0 ∈ K : a + 0 = a.

4) Обратный элемент по + ∀a ∈ K ∃ (−a) ∈ K : a + (−a) = 0.

5) Дистрибутивность ∀a, b, c ∈ K (a + b)c = ac + bc и a(b + c) = ab + ac.

6) Ассоциативность · ∀a, b, c ∈ K (ab)c = a(bc).

7) Коммутативность · ∀a, b ∈ K ab = ba.

8) Единица · ∃ 1 ∈ K : a · 1 = 1 · a = a.

9) Обратный элемент по · ∀a ∈ K \ {0} ∃ (a) −1 ∈ K : a · (a)−1 = (a)−1 · a = 1.

• Выполнено 1 − 6: K — **кольцо**.

• Выполнено 1 − 7: K — **коммутативное кольцо.**

• Выполнено 1 − 6 и 8: K — **кольцо с 1.**

• Выполнено 1 − 6, 8 и 9 : K — **тело**.

• Выполнено 1 − 9 : K — **поле**.

1. Свойства 0, 1 и обратных элементов. Вычитание и деление.

Свойство 1

Ноль в кольце K единственен.

*Доказательство.*

Пусть есть два ноля: 01 и 02. Тогда: 01 = 01 + 02 = 02 + 01 = 02.

Свойство 2

Для любого a ∈ K, обратный элемент по + единственен.

*Доказательство.*

Пусть есть два обратных элемента по + для a ∈ K: b1 и b2. Тогда: b1 = b1 + 0 = b1 + (a + b2) = (b1 + a) + b2 = 0 + b2 = b2.

Свойство 3

∀a ∈ K − (−a) = a.

*Доказательство.*

a = a + ((−a) + (−(−a))) = (a + (−a)) + (−(−a)) = (−(−a)).

Свойство 4

В кольце не более одной единицы.

*Доказательство.*

Пусть есть две единицы: 11 и 12. Тогда: 11 = 11 · 12 = 12.

Определение

Пусть K — кольцо с 1. Элемент a ∈ K обратимый, если существует a−1 ∈ K.

• В поле все ненулевые элементы обратимы.

Свойство 5

Пусть K — кольцо с 1. Тогда для любого a ∈ K существует не более чем один обратный элемент по ·. *Доказательство.*

Пусть есть два обратных элемента по · для a ∈ K: b1 и b2. Тогда: b1 = b1 · 1 = b1 · (a · b2) = (b1 · a) · b2 = 1 · b2 = b2.

Свойство 6

Пусть K — кольцо с 1. Тогда для любого обратимого a ∈ K выполнено (a−1)−1 = a.

*Доказательство.*

a = a · 1 = a · (a−1 · (a−1)−1) = = (a · a−1) · ((a−1)−1 = 1 · (a−1)−1 = (a−1)−1.

Свойство 7

−0 = 0.

*Доказательство*. Следует из 0 + 0 = 0.

Свойство 8

Если K — кольцо с 1, то 1−1 = 1.

*Доказательство.* Следует из 1 · 1 = 1.

Определение

• **Вычитание** — это прибавление обратного элемента по + : a − b := a + (−b).

• **Деление** на обратимый элемент b — это умножение на b−1 : a÷b := a · b−1.

1. Подкольцо и подполе.

Определение

• Пусть K ⊂ L, причем оба они — кольца с одними и теми же операциями + и ·. Тогда K — **подкольцо** L, а L — **надкольцо** K.

• Пусть K ⊂ L, причем оба они — поля с одними и теми же операциями + и ·. Тогда K — **подполе** L, а L — **надполе** K.

Лемма 1

Пусть L — кольцо, K ⊂ L. Пусть выполнены следующие условия:

1 ◦ Замкнутость по + ∀ a, b ∈ K a + b ∈ K.

2 ◦ Замкнутость по · ∀ a, b ∈ K a · b ∈ K.

3 ◦ Существование обратного элемента по + ∀ a ∈ K ∃ − a ∈ K.

Тогда K — кольцо, а значит, подкольцо L. Если L — коммутативно, то K тоже.

*Доказательство.*

• Условия 1◦ и 2◦ означают, что + и · корректно определены в K.

• Ассоциативность и коммутативность +, ассоциативность ·, коммутативность · (если есть) наследуются из L. Рассмотрим любой элемент a ∈ K. Тогда −a ∈ K, а значит a − a = 0 ∈ K.

Лемма 2

Пусть L — поле, K ⊂ L. Пусть выполнены следующие условия:

1 ◦ Замкнутость по + ∀ a, b ∈ K a + b ∈ K.

2 ◦ Замкнутость по · ∀ a, b ∈ K a · b ∈ K.

3 ◦ Существование обратного элемента по + ∀ a ∈ K ∃ − a ∈ K.

4 ◦ Существование обратного элемента по · ∀ a ∈ K, a ̸= 0, ∃ (a) −1 ∈ K.

Тогда K — поле, а значит, подполе L.

Доказательство.

• По Лемме 1, K — коммутативное подкольцо L.

• Остается проверить существование 1 в K. Рассмотрим любой ненулевой элемент a ∈ K. Тогда a−1 ∈ K, а значит, a · a−1 = 1 ∈ K.

1. Гомоморфизмы колец. Ядро и образ гомоморфизма.

Определение

• Пусть K, L — кольца. Отображение f : K → L называется **гомоморфизмом**, если ∀ a, b ∈ K:

f (a + b) = f (a) + f (b) и f (ab) = f (a)f (b).

**Ядро** гомоморфизма f — это Ker(f ) = {x ∈ K : f (x) = 0}.

**Образ** гомоморфизма f — это Im(f ) = {y ∈ L : ∃x ∈ K : f (x) = y}.

Свойство 1

Если f : K → L гомоморфизм, то f (0K ) = 0L.

Доказательство.

f (0K) = f (0K + 0K) = f (0K ) + f (0K ). Вычитая из левой и правой частей f (0K), получаем f (0K) = 0L.

Свойство 2

Если f : K → L гомоморфизм, то f (−a) = −f (a).

Доказательство.

0L = f (0K ) = f (a + (−a)) = f (a) + f (−a). Вычитая из левой и правой частей f (a), получаем −f (a) = f (−a).

Лемма 3

Пусть K, L — кольца, f : K → L — гомоморфизм колец. Тогда:

1) Ker(f ) — подкольцо K.

2) Im(f ) — подкольцо L.

*Доказательство.*

Достаточно проверить условия из Леммы 1.

1. • Пусть a, b ∈ Ker(f ). Тогда f (a + b) = f (a) + f (b) = 0 + 0 = 0, следовательно, a + b ∈ Ker(f ).

• f (ab) = f (a)f (b) = 0 · 0 = 0, следовательно, ab ∈ Ker(f ).

• f (−a) = −f (a) = −0L = 0L.

1. • Пусть y, y ′ ∈ Im(f ), а x, x ′ ∈ K таковы, что f (x) = y и f (x ′ ) = y ′ .

• Тогда y + y ′ = f (x) + f (x ′) = f (x + x ′) ∈ Im(f ) и y · y ′ = f (x) · f (x ′) ∈ Im(f ).

• −y = −f (x) = f (−x) ∈ Im(f ).

1. Типы гомоморфизмов. Мономорфизм и ядро.

Типы гомоморфизмов

• Пусть f : K → L — гомоморфизм колец.

• Если f — инъекция, то f — **мономорфизм**.

• Если f — сюръекция (то есть, Im(f ) = L), то f —**эпиморфизм**.

• Если f — биекция, то f — **изоморфизм**.

• Изоморфизм = мономорфизм + эпиморфизм.

Лемма 4

Пусть f : K → L — гомоморфизм колец. Тогда f — мономорфизм, если и только если Ker(f ) = {0}. *Доказательство.*

⇒

• Если f — мономорфизм, то f — инъекция.

• Пусть a ∈ Ker(f ). Из f (a) = 0 = f (0) следует, что a = 0 (так как f — инъекция).

⇐

• Пусть f (a) = f (b). Тогда f (a − b) = f (a) − f (b) = 0.

• Значит, a − b ∈ Ker(f ) = {0}, откуда a = b. Таким образом, f — инъекция, а значит, мономорфизм.

1. Отображение, обратное к изоморфизму — изоморфизм.

Лемма 5

Пусть f : K → L — изоморфизм колец. Тогда и f−1: L → K — изоморфизм колец.

*Доказательство.*

• Достаточно доказать, что f−1 — гомоморфизм (так как отображение, обратное к биекции — биекция).

• Рассмотрим любые a, b ∈ L.

• Пусть w = f−1(a + b) − f−1(a) − f−1(b). Так как f — гомоморфизм, имеем f (w) = f (f−1(a+b)) − f (f −1(a)) − f (f−1(b)) = a + b - a - b = 0.

• Из (f (w) = 0 = f (0) и того, что f — биекция, следует w = 0.

• Следовательно, f−1(a + b) = f−1(a) + f−1(b).

• Пусть z = f−1(ab) − f−1(a)f−1(b). Так как f — гомоморфизм, имеем f (z) = f (f−1(ab)) − f (f−1(a)) · f (f−1(b)) = ab − ab = 0.

• Из f (z) = 0 = f (0) и того, что f — биекция, следует z = 0. Следовательно, f−1(ab) = f−1(a) · f−1(b).

1. Изоморфные кольца.

Определение

Если существует изоморфизм f : K → L, то говорят, что эти кольца **изоморфны**. Обозначение: K ≃ L.

Теорема 0

≃ — отношение эквивалентности(то есть, рефлексивно, симметрично и транзитивно) на множестве всех колец.

*Доказательство.*

• Рефлексивность очевидна: тождественное отображение id : K → K (заданное формулой id(x) = x для всех x ∈ K) очевидно, является изоморфизмом.

• Симметричность доказана в Лемме 5.

• Докажем транзитивность. Пусть K, L, M — кольца, K ≃ L и L ≃ M.

• Тогда существуют изморфизмы f : K → L и g : L → M. Докажем, что их композиция g · f : K → M (заданная правилом gf (a) := g(f (a))) также является изоморфизмом.

• Композиция биекций g и f , очевидно, является биекцией.

• Проверим, что gf — гомоморфизм колец: gf(a + b) = g(f (a + b)) = g(f (a) + f (b)) = g(f (a)) + g(f (b)) = gf (a) + gf (b); gf (ab) = g(f (ab)) = g(f (a) · f (b)) = g(f (a)) · g(f (b)) = gf (a) · gf (b).

1. Идеал. Ядро гомоморфизма является идеалом.

Определение

Пусть K — коммутативное кольцо. Множество I ⊂ K — **идеал** в K, если I — подкольцо K и выполнено следующее условие: ∀x ∈ K и ∀a ∈ I ax ∈ I.

• В любом кольце K есть два “неинетересных” идеала: это {0} и K.

Лемма 6

Пусть K — коммутативное кольцо, I ⊂ K. Пусть выполнены следующие условия:

1 ◦ Замкнутость по + ∀ a, b ∈ I a + b ∈ I.

2 ◦ ∃ обратного элемента по + ∀ a ∈ I ∃(−a) ∈ I.

3 ◦ Замкнутость по · на элементы K ∀x ∈ K и ∀a ∈ I ax ∈ I

Тогда I — идеал в K.

*Доказательство.*

• По Лемме 1, I — подкольцо K.

• Теперь по условию 3◦ несложно понять, что I — идеал.

Лемма 7

Пусть K — коммутативное кольцо, φ : K → L — гомоморфизм колец. Тогда ker(φ) — идеал в K. Доказательство.

• По Лемме 3, ker(φ) — подкольцо K.

• Пусть a ∈ ker(φ) и x ∈ K. Тогда φ(ax) = φ(a) · φ(x) = 0 · φ(x) = 0, а значит, ax ∈ ker(φ)

• По Лемме 6, ker(φ) — идеал в K.

1. Идеал и обратимые элементы. Идеалы в поле. Гомоморфизм из поля — инъекция.

Лемма 8

Пусть K — коммутативное кольцо с 1, I — идеал в K, а x ∈ I — обратимый элемент кольца K. Тогда I = K.

*Доказательство.*

• Так как x−1 ∈ K и x ∈ I, мы имеем 1 = x · x−1 ∈ I.

• ∀y ∈ K имеем y = y · 1 ∈ I. Значит, I = K.

Следствие 1

Пусть K — поле, а I — идеал в K. Тогда I = K или I = {0}.

*Доказательство.*

• Предположим, что I ≠ {0}. Тогда ∃a ∈ I, a ≠ 0. Так как a — обратимый элемент (как все ненулевые элементы поля), I = K по Лемме 8.

Следствие 2

Пусть K — поле, L — кольцо, а f : K → L — гомоморфизм колец. Тогда либо Im(f ) = {0}, либо f — мономорфизм.

*Доказательство.*

• По Лемме 7 ker(f ) — идеал в поле K.

• Тогда по Следствию 1 либо ker(f ) = K, либо ker(f ) = {0}.

• Если ker(f ) = K, то Im(f ) = {0}.

• Если ker(f ) = {0}, то f — мономорфизм.(по лемме 4)

1. Идеал, порожденный множеством элементов. Главный идеал.

Определение

Пусть K — коммутативное кольцо, M ⊂ K. Тогда ⟨M⟩ := {m1x1 + · · · + msxs : m1, . . . , ms ∈ M, x1, . . . , xs ∈ K} − **идеал, порожденный множеством M** (здесь количество элементов s не фиксировано и может быть любым натуральным числом).

• Идеал, порожденный M — множество всех линейных комбинаций элементов из M.

Определение.

Пусть K — коммутативное кольцо.

1) Пусть m ∈ K. Тогда mK = {mx : x ∈ K} — **главный идеал**.

2) Если все идеалы в кольце K — главные, то K — **кольцо главных идеалов**.

Лемма 9

Пусть K — коммутативное кольцо, M ⊂ K. Тогда ⟨M⟩ — идеал в K.

*Доказательство.*

• Нужно проверить условия из Леммы 6.

• Пусть a, b ∈ ⟨M⟩. Тогда существуют такие m1, . . . , ms ∈ M, a1, . . . , as , b1, . . . , bs ∈ K, что a = a1m1 + · · · + asms и b = b1m1 + · · · + bsms (можно считать, что a и b — линейные комбинации одних и тех же элементов M, при необходимости добавив слагаемые с нулевыми коэффициентами).

• −a = (−a1)m1 + · · · + (−as )ms ∈ ⟨M⟩. • Тогда a + b = (a1 + b1)m1 + · · · + (as + bs )ms ∈ ⟨M⟩.

• Для любого x ∈ K, ax = (a1x)m1 + · · · + (asx)ms ∈ ⟨M⟩.

• Условия Леммы 6 проверены, а значит, ⟨M⟩ — идеал в K.

1. Сравнения по модулю идеала. Вычеты.

Сравнение по модулю идеала

• Пусть K — коммутативное кольцо, I — идеал в K.

Определение

Пусть a, b ∈ K. Тогда a **≡I** b (или, что то же самое, a ≡ b (mod I)), если и только если a − b ∈ I.

Лемма 10

≡I — отношение эквивалентности (то есть, рефлексивно, симметрично и транзитивно). Доказательство.

• a ≡I a, так как a − a = 0 ∈ I.

• Если a ≡I b, то a − b ∈ I. Значит, b − a ∈ I, откуда b ≡I a.

• Если a ≡I b и b ≡I c, то a − b, b − c ∈ I. Значит, a − c = (a − b) + (b − c) ∈ I, откуда a ≡I c. □ Определение

**Вычет по модулю идеала I** — это класс эквивалентности по ≡I .

• Различные вычеты не пересекаются. Кольцо K разбито на вычеты.

1. Факторкольцо

Факторкольцо

• Для a ∈ K вычет, состоящий из элементов кольца, сравнимых с a, как правило, будем обозначать через .

• Из определения следует, что = a + I = {a + x : x ∈ I }.

Определение

• Пусть K — коммутативное кольцо, I — идеал в K. **Факторкольцо** K/I := { : a ∈ K}.

• a + b := a + b; a · b := ab.

Лемма 11

+ и · в K/I определены корректно.

*Доказательство.*

• Пусть a ≡I a′ , то есть, = ′ . Это означает, что a − a ′ ∈ I. Докажем, что от замены a на a′ результат + и · не изменится:

+ = ′+ ⇐⇒ a+b ≡I a′+b ⇐⇒ a+b−(a′+b) = a−a′ ∈ I;

· = ′ · ⇐⇒ ab ≡I a′b ⇐⇒ ab − (a′b) = (a − a′)b ∈ I ⇐ a − a ′ ∈ I.

Теорема 1

• K/I с определенными выше + и · — коммутативное кольцо.

• Если K — кольцо с 1, то K/I — тоже. Если при этом a ∈ K — обратимый элемент в K, то — обратимый в K/I.

*Доказательство.*

• Так как + = , из ассоциативности и коммутативности + в K следует ассоциативность и коммутативность + в K/I.

• Так как · = , из ассоциативности и коммутативности умножения в K следует ассоциативность и коммутативность умножения в K/I.

• Дистрибутивность: ( + ) = = = · + · .

• Ноль — это 0.

• Обратный по сложению: − := .

• Единица: если 1 ∈ K, то 1 — единица в K/I.

• Если a ∈ K — обратимый, то ()−1 := — обратный в K/I.

1. Теорема о гомоморфизме колец.

Теорема о гомоморфизме колец (Теорема 2)

Пусть K, L — коммутативные кольца, f : K → L — гомоморфизм. Тогда K/Ker(f ) ≃ Im(f ). Более того, отображение : K/Ker(f ) → Im(f ), заданное формулой () := f (x), является изоморфизмом колец.

*Доказательство.*

• Докажем корректность определения . Пусть = . Тогда x − y ∈ Ker(f ), а значит, f (x) = f (y) + f (x − y) = f (y) + 0 = f (y).

• Теперь ясно, что — гомоморфизм:

( + ) = f () = f (x + y) = f (x) + f (y) = () + ();

( · ) = () = f (xy) = f (x)f (y) = () · ();

• Очевидно, — сюръекция: ∀y ∈ Im(f ) ∃x ∈ K такой, что y = f(x). Тогда и y = ().

• Пусть ∈ Ker(). Тогда 0 = () = f (a), а значит, a ∈ Ker(f ), откуда следует = . Следовательно, Ker() = {}.

• Таким образом, — изоморфизм, а значит, K/Ker(f ) ≃ Im(f ).

1. Дроби: эквивалентность, простейшие свойства. Сложение и умножение дробей.

Поле частных

• Пусть K — коммутативное кольцо без делителей ноля (то есть, если a, b ∈ K и ab = 0, то a = 0 или b = 0).

• Обозначим через M множество всех дробей  , где a, b ∈ K, b ̸= 0.

• Пусть ∼ ⇐⇒ ad = bc.

Свойство 1

∼ ⇐⇒ c = 0.

*Доказательство.*

⇐. Если c = 0, то 0 · d = 0 = b · 0.

⇒. ∼ ⇒ 0 = 0 · d = bc. Так как по определению b ≠ 0, а делителей 0 в K нет, c = 0. □

Свойство 2

∼ ⇐⇒ c = d.

*Доказательство.*

Очевидно, a ≠ 0. Следовательно, ∼ ⇐⇒ ad = ac ⇐⇒ a(d − c) = 0 ⇐⇒ d − c = 0 ⇐⇒ c = d. □ Свойство 3

Сокращение дроби. ∼ при c ̸= 0.

*Доказательство.*

abc − bac = 0.

Лемма 12

∼ — отношение эквиваленности.

*Доказательство.*

• Рефлексивность очевидна.

• Симметричность. ∼ ⇐⇒ ad = bc ⇐⇒ cb = da ⇐⇒ ∼ .

• Транзитивность. Если ∼ и ∼ , то ad = bc и cf = de.

• Если хотя бы одно из a, c, e равно 0, то по Свойству 1 равны и два других. Тогда ∼ .

• Пусть 0 ∉ {a, c, e}. Тогда перемножим полученные равенства и сократим на cd ≠ 0: adcf = bcde ⇒ af = be ⇒ ∼ .

1. Поле частных.

Определение

**Поле частных** F коммутативного кольца K без делителей ноля состоит из классов эквивалентности дробей. Мы будем обозначать класс эквивалентности дроби в точности так же, как саму эту дробь.

Сложение: + := .

Умножение: · := .

Свойство 4

+ = .

*Доказательство.*

+ = = по Свойству 3.

Лемма 13

Сложение и умножение в поле частных определены корректно, то есть, результат не зависит от замены дроби на эквивалентную.

Доказательство.

• Достаточно доказать, что при замене первой дроби на эквивалентную дробь результат сложения и умножения не изменится. Отметим, что ab′ = a′b.

• Сложение (мы можем сократить на d2 , так как d ≠ 0):

+ = ∼ + = ⇐⇒ (ad+bc)b′d = (a′d+b′c)bd ⇐⇒ adb′d+**bcb′d** = a′dbd+**b′cbd** ⇐⇒ ab′d2 = a′bd2 ⇐⇒ ab′ = a′b.

• Умножение. Если c = 0, утверждение следует из Свойства 1. Иначе можно сокращать на cd:

· = ∼ · = ⇐⇒ acb′ d = a′cbd ⇐⇒ ab′ = a′b.

Теорема 3

Поле частных F коммутативного кольца K без делителей ноля — поле.

*Доказательство.*

**Коммутативность** **сложения и умножения** очевидно следуют из аналогичных свойств в K. **Ассоциативность сложения**. ( + ) + = + = . В каждом из слагаемых три сомножителя, один числитель и два знаменателя других дробей. Легко понять, что при другом порядке сложения будет то же самое.

**Ноль**. Дроби вида (b ∈ K, b ≠ 0) образуют класс эквивалентности по Свойству 1. Несложно проверить, что это класс и будет 0 в поле частных: + = = .

**Обратный элемент по +**. Положим −() := . Проверка: + = = 0.

**Ассоциативность умножения**. ( · ) · = · = . Легко понять, что при другом порядке умножения будет то же самое.

**Дистрибутивность.** ( + ) · = · =  = + = = + (последний переход верен по Свойству 3).

**Единица.** В качестве 1 подойдет класс эквивалентности дробей вида , где a ≠ 0.

**Обратный элемент по умножению.** Для дроби , где a ̸= 0 положим ()−1 := . Проверка: · = = 1 по определению. □

1. Вложение кольца в поле частных.

Лемма 14

Пусть K — коммутативное кольцо с 1 без делителей 0, а F — его поле частных. Тогда отображение φ : K → F, заданное формулой φ(a) = — мономорфизм колец.

*Доказательство.*

• Проверим, что φ — гомоморфизм колец. Пусть a, b ∈ K.

• φ(a) + φ(b) = + = = = φ(a + b).

• φ(a)φ(b) = = = φ(ab).

• Пусть a ∈ Ker(φ). Тогда 0 = φ(a) = ⇐⇒ a = 0. □

• Далее мы будем отождествлять число a ∈ K с дробью ∈ F и считать, что K ⊂ F.

1. Характеристика поля.

Определение

Пусть K — поле.

• Положим := 1 + 1 + · · · + 1(k раз) = k для k ∈ N и := −(1 + 1 + · · · + 1 ) = -k для отрицательных k ∈ Z, а также = 0.

• Если существует такие k ∈ N, что = 0, то характеристика поля char(K) равна наименьшему из таких чисел.

• Если же таких натуральных чисел нет, то считается, что char(K) = 0.

• Несложно проверить, что + = .

• Раскрыв скобки по дистрибутивности, можно убедиться в том, что · = .

Лемма 15

Пусть K — поле и char(K) = p ̸= 0. Тогда p ∈ P.

*Доказательство.*

• Пусть p = ab, где 1 < a < p и 1 < b < p.

• Тогда · = = = 0.

• Так как K — поле, отсюда следует, что хотя бы одно из чисел и равно 0, что противоречит определению характеристики поля.

1. Теорема о подполе.

Теорема 4

Пусть K — поле.

1) Если char(K) = p ∈ P, то отображение φ : Z/pZ → K, заданное формулой φ() = (для m ∈ Z) — мономорфизм полей. В частности, K имеет подполе, изоморфное Z/pZ.

2) Если char(K) = 0, то отображение φ : Q → K, заданное формулой φ() = (для a, b ∈ Z, b ̸= 0)— мономорфизм полей. В частности, K имеет подполе, изоморфное Q.

*Доказательство.*

1. Отображение ψ : Z → K, заданное формулой ψ(m) := , очевидно, является гомоморфизмом колец.

• ker(ψ) = {m ∈ Z : = 0} — идеал в Z. НУО, ker(ψ) = qZ.

• Тогда = 0 ⇐⇒ m q, то есть, char(K) = q. Значит, q = p и ker(ψ) = pZ.

• По Теореме 2 (о гомоморфизме колец), отображение ψ : Z/pZ → K, заданное формулой ψ(m) = m — изоморфизм между Z/pZ и Im(ψ) — подполем K.

1. • В этом случае ∀m ∈ N ≠ 0, то есть, char(K) = 0.

• Определим отображение φ : Q → K формулой () = (при b ̸= 0).

• Проверим корректность. Пусть = ⇐⇒ ad = bc (здесь b, d ̸= 0).

• Тогда по дистрибутивности в поле K имеем · = · ⇐⇒ · .

• Проверим, что φ — гомоморфизм:

• φ() · φ() = · = = φ) = φ( · ).

• φ() + φ() = + = = φ( ) = φ( + ).

• Так как Q — поле и φ принимает не только нулевые значения, ker(φ) = {0}.

• Значит, Im(φ) — подполе K, изоморфное Q. □

Следствие 3

Все поля из p ∈ P элементов изоморфны Z/pZ.

• Будем применять при p ∈ P обозначение Fp для поля из p элементов (изоморфного Z/pZ).

# Комплексные числа

1. Вещественная и мнимая часть, умножение, сложение, норма, модуль.

Определение

• Множество комплексных чисел состоит из упорядоченных пар вещественных чисел: C = {(a, b) : a, b ∈ R}.

• **Сложение**: (a, b) + (a′, b′ ) := (a + a ′ , b + b ′ ).

• **Умножение**: (a, b) · (a′, b′) := (aa′ − bb′ , ab′ + ba′ ).

Определение

• Пусть z = (a, b) ∈ C.

• **Вещественная часть** z — это Re(z) := a.

• **Мнимая часть** z — это Im(z) := b.

• **Комплексное сопряжение**: -z := (a, −b).

• **Норма** z — это N(z) := a2 + b2 .

• **Модуль** z — это |z| := sqrt(N(z)) = √( a2 + b2).

• Очевидно, --z = z.

1. Поле комплексных чисел.

Теорема 1

C — поле.

*Доказательство*.

• 1) и 2) Так как сложение в C — покомпонентное, ассоциативность и коммутативность наследуются из R.

• 3) Ноль в C — это 0 := (0, 0).

• 4) Обратный элемент по +. Для z = (a, b) положим -z := (−a, −b).

• 7) Коммутативность умножения: (a, b) · (a′, b′ ) = (aa′ − bb′ , ab′ + ba′ ) = (a′a − b′b, a′b + b′a) = (a′, b′ ) · (a, b).

• 5) Достаточно проверить одну дистрибутивность (так как умножение коммутативно): (a, b) · ((c1, d1) + (c2, d2)) = (a, b) · (c1 + c2, d1 + d2) = (ac1 + ac2 − bd1 − bd2, ad1 + ad2 + bc1 + bc2) = (ac1−bd1, ad1+bc1)+(ac2−bd2, ad2+bc2) = (a, b)·(c1, d1)+(a, b)·(c2, d2).

• 6) ассоциативность умножения: (a1, b1)·(a2, b2) ·(a3, b3) = (a1a2−b1b2, a1b2+b1a2)·(a3, b3) = (a1a2a3−b1b2a3−a1b2b3−b1a2b3, a1b2a3+b1a2a3+a1a2b3−b1b2b3). Нетрудно проверить, что при другом порядке получится то же самое (в вещественную часть попадают сомножители с четным числом b, в мнимую — с нечетным, знак − получается там, где более одной b).

• 8) Единица: это 1 := (1, 0).

• 9) Обратный элемент по ·. Для z = (a, b) положим z−1 := ( a/N(z) , −b/N(z) ). Проверяем: zz−1 = (a, b)·( a/N(z) , −b/N(z) ) = ( (a2 + b2)/N(z) , (−ab + ba)/N(z) ) = (1, 0).

1. Тригонометрическая форма записи комплексного числа. Изменение модуля и аргумента при перемножении комплексных чисел. Формула Муавра.

Геометрическая интерпретация C и тригонометрическая запись

• Рассмотрим декартову систему координат в R2, по оси абсцисс будем откладывать вещественную часть, а по оси ординат — мнимую. Тогда комплексное сопряжение — симметрия относительно оси абсцисс.

• Для числа z = (a, b) ∈ C **r** = |z| = √(a2 + b2) — расстояние от начала координат до z.

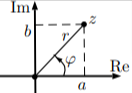
• Аргумент z — это направленный угол arg(z) = **φ** от оси абсцисс до луча Oz против часовой стрелки. Вычисляется с точностью до прибавления 2πk, где k ∈ Z.

• Пара (r, φ) однозначно задает точку z.

• **a** = r cos(φ), **b** = r sin(φ).

• **Тригонометрическая форма записи комплексного числа**: z = (r cos(φ),r sin(φ)).

• Если z = (r cos(φ),r sin(φ)), то |z| = r, arg(z) = φ.



Теорема 2

Пусть x, y ∈ C. Тогда |xy| = |x||y| и arg(xy) = arg(x) + arg(y).

*Доказательство.*

• Пусть x = (r cos(φ),r sin(φ)), а y = (p cos(ψ), p sin(ψ)). Тогда xy = (rp(cos(φ) cos(ψ)−sin(φ) sin(ψ)),rp(cos(φ) sin(ψ)+sin(φ) cos(ψ))) = (rp cos(φ + ψ),rp sin(φ + ψ)) .

• Следовательно, |xy| = rp и arg(xy) = φ + ψ.

Теорема 3 Формула Муавра.

Пусть z ∈ C, n ∈ N. Тогда |zn| = |z |n и arg(zn) = n · arg(z).

*Доказательство.*

Индукция по n.

База n = 1 очевидна.

Переход n → n + 1.

• Пусть |z| = r, arg(z) = φ и утверждение доказано для n, то есть, |zn| = rn и arg(zn) = n · φ.

• По Теореме 2 |z(n+1)| = |z| · |zn| = r · rn = r(n+1) и arg(z(n+1)) = arg(z) + arg(zn) = φ + nφ = (n + 1) · φ

1. Вложение вещественных чисел в комплексные.

Лемма 1

Отображение f : R → C, заданное формулой f (a) = (a, 0) — мономорфизм.

Доказательство.

• Очевидно, f — инъекция.

• Нужно проверить, что это гомоморфизм. Пусть a, b ∈ R.

• f (a + b) = (a + b, 0) = (a, 0) + (b, 0) = f (a) + f (b).

• f (ab) = (ab, 0) = (a, 0) · (b, 0) = f (a)f (b). □

• Очевидно, Im(f ) ≃ R. Таким образом, C имеет подполе Im(f ), изоморфное R. В дальнейшем мы будем отождествлять каждое вещественное число a с комплексным (a, 0).

• Теперь можно сказать, что для любого z = (a, b) ∈ C выполнено:

z · -z = N(z) = N(-z) (все это равно по a2 + b2 )

и

z + -z = 2Re(z) = 2Re(-z) (все это равно по 2a).

• Сопряженные комплексные числа z, -z ∈ C \ R — корни квадратного уравнения с вещественными коэффициентами t2 − 2Re(z) · t + N(z) = 0.

1. Извлечение корня из комплексного числа. Корни из 1.

Извлечение корня из комплексного числа

• Пусть a ∈ C и n ∈ N фиксированы, a ≠ 0. Решим уравнение zn = a.

• Будем использовать представление комплексных чисел через модуль и аргумент. Тогда a = (r, φ) (параметры даны) и z = (p, ψ) (эти параметры мы ищем).

• По формуле Муавра, p = n√r.

• С аргументом сложнее. По формуле Муавра, nψ = φ + 2πk, где k ∈ Z (напомним, что аргумент вычисляется с точностью до 2πk). Поделив на n, получаем

ψ = + . (1)

• При k ∈ {0, 1, . . . , n − 1} в (1) получается n разных аргументов.

• Каждое число k ∈ Z можно представить в виде k = qn + t, где 0 ≤ t < n (это теорема о делении с остатком). Тогда = + 2πq, а это тот же аргумент, что и .

• Таким образом, корень n степени извлекается из a ≠ 0 извлекается ровно n способами.

Корни из 1

• Отдельно рассмотрим корни n степени из 1 — решения уравнения zn = 1.

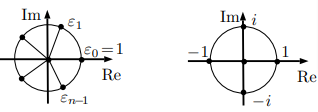
• Из сказанного выше следует, что модуль всех корней из 1 равен 1. Так как arg(1) = 0, все различные аргументы считаются по формуле

ψk = , где k ∈ {0, . . . , n − 1}. (1)

• Обозначим их ε0, . . . , εn−1 (корень εk имеет аргумент ψk ).

• Корни из 1 степени n лежат на окружности радиуса 1 в вершинах правильного n-угольника, одна из которых — в 1.

• По формуле Муавра εk = εk1 . Значит, все корни из 1 — это степени ε1.



• Еще одно часто встречающееся обозначение — комплексное число z с |z| = 1 и arg(z) = α часто записывают в виде z = eαi . • Таким образом, eαi = (cos(α),sin(α)).

# Целые числа

1. Делимость. Свойства. Теорема о делении с остатком

Определение

Пусть a, b ∈ Z, b ≠ 0. Тогда a **делится** на b (обозначение: a b) или, что то же самое, b **делит** a (обозначение: b | a), если a = bc, где c ∈ Z. Если a b, то b — **делитель** a.

Свойство 1

Если a b и b c, то a c.

*Доказательство.*

Тогда a = kb и b = nc, где k, n ∈ Z, откуда следует a = knc. □

Свойство 2

Пусть a, b d, а x, y ∈ Z. Тогда ax + by d.

*Доказательство.*

Тогда a = kd и b = nd, где k, n ∈ Z, откуда следует ax + by = (kx + ny)d. □

Свойство 3

Пусть a, d ∈ N, a d. Тогда a ≥ d.

*Доказательство.*

Тогда a = kd, где k ∈ N, откуда следует a = kd ≥ d.

Теорема о делении с остатком (Теорема 1)

Пусть a ∈ Z, b ∈ N. Тогда существуют единственные такие q,r ∈ Z, что 0 ≤ r < b и a = bq + r.

• Число r называется **остатком** от деления a на b.

*Доказательство.*

∃. Пусть q — такое целое число, что bq ≤ a < b(q + 1), а r = a − bq. Тогда 0 ≤ r < b (вычтем из всех трех частей первого неравенства bq).

!. Пусть a = bq1 + r1 = bq2 + r2, причем 0 ≤ r1 < b и 0 ≤ r2 < b.

• НУО r1 > r2. Тогда 0 < r1 − r2 < b.

• С другой стороны, r1 − r2 = b(q2 − q1) ≥ b. Противоречие.

1. НОД. Свойства.

Определение

Пусть a1, . . . , an ∈ Z. Обозначим через OD(a1, . . . , an) множество всех общих делителей этих чисел, а через (a1, . . . , an) — их **НОД** (наибольший из общих делителей).

Свойство 1

Если b ∈ N. a b, то OD(a, b) — это все делители b и (a, b) = b.

*Доказательство.*

• Если d — общий делитель a и b, то d — делитель b.

• Если d — делитель b, то a d по свойству 1 делимости. Значит, d — общий делитель a и b. □ Свойство 2

Пусть a, b, c, k ∈ Z, c = a + kb. Тогда OD(a, b) = OD(c, b), а следовательно, и (a, b) = (c, b). *Доказательство.*

• Пусть d ∈ OD(a, b). Тогда c d, а значит, d ∈ OD(c, b).

• Наоборот, если d ∈ OD(c, b), то a = c − kb d, а значит, d ∈ OD(a, b).

1. Алгоритм Евклида. Следствия из алгоритма Евклида.

Алгоритм Евклида

• Пусть a, b ∈ N, a > b. Каждая строка алгоритма — деление с остатком.

1) a = bq1 + r1, 0 ≤ r1 < b;

2) b = r1q2 + r2, 0 ≤ r2 < r1;

3) r1 = r2q3 + r3, 0 ≤ r3 < r2;

. . .

n) rn−2 = rn−1qn + rn, 0 ≤ rn < rn−1;

n + 1) rn−1 = rnqn+1.

• Так как b > r1 > r2 > . . . и все эти числа неотрицательны, алгоритм обязательно закончит работу. Теорема 2

(a, b) = rn, а OD(a, b) — это все делители (a, b).

*Доказательство.*

• По свойству 2 НОД OD(a, b) = OD(b,r1) = OD(r1,r2) = · · · = OD(rn−1,rn), а это по свойству 1 НОДа — все делители rn.

• Тогда (a, b) — наибольший из делителей rn, а это rn.

Теорема 3

Пусть a, b, m, d ∈ N. Тогда:

1) (am, bm) = m(a, b).

2) Если d ∈ OD(a, b), то ( , ) = .

*Доказательство.*

• НУО a > b.

1. • Рассмотрим первую строку алгоритма Евклида для am и bm: am = bm · q1 + r1m, 0 ≤ r1m < bm.

• Неполное частное не меняется, а остаток умножается на m.

• Так будет и со следующими строчками, в результате получится столько же строк, сколько в алгоритме Евклида для a и b, а НОД — последний ненулевой остаток — умножится на m.

1. • Рассмотрим первую строку алгоритма Евклида для и : = · q1 + , 0 ≤ < .

• Неполное частное не меняется, а остаток мы делим на d (в результате он остается целым).

• Так будет и со следующими строчками, в результате получится столько же строк, сколько в алгоритме Евклида для a и b, а НОД — последний ненулевой остаток — разделится на d.

1. Линейное представление НОД.

Теорема 4

Пусть a, b ∈ Z. Тогда существуют такие x, y ∈ Z, что (a, b) = ax + by.

• Это называется **линейным представлением НОДа**.

*Доказательство.*

• Так как делители у чисел a и −a одни и те же, (a, b) = (a, −b). Поэтому, можно считать, что a, b ∈ N.

• НУО a ≥ b. Воспользуемся алгоритмом Евклида и соответствующими обозначениями, дополним их: пусть r0 = b и r−1 = a.

• Докажем, что существует представление (a, b) = xkrk + ykrk−1 для всех k = {n, . . . , 0} (где (a, b) = rn) индукцией с обратным ходом. При k = 0 получим утверждение теоремы.

• База k = n очевидна: (a, b) = 1 · rn + 0 · rn−1.

• Переход k → k − 1. Из алгоритма Евклида мы знаем, что rk = rk−2 − rk−1qk . Подставим:

(a, b) = xkrk + ykrk−1 = xk(rk−2 − rk−1qk) + ykrk−1 = (−xkqk + yk)rk−1 + xkrk−2. □

1. НОД нескольких чисел через НОД двух чисел. Линейное представление НОД нескольких чисел.

Теорема 5

Пусть n ≥ 2, a1, . . . , an ∈ Z. Положим m2 = (a1, a2), m3 = (m2, a3), . . . , mn = (mn−1, an). Тогда mn = (a1, . . . , an), а OD(a1, . . . , an) — это все делители mn.

*Доказательство.*

• Индукцией по k докажем, что OD(a1, . . . , ak) — все делители mk .

• База k = 2 доказана в Теореме 2.

• Переход k → k + 1. OD(a1, . . . , ak , ak+1) — это все числа из OD(a1, . . . , ak), являющиеся делителями ak+1.

• Так как OD(a1, . . . , ak) — это все делители mk , получаем, что OD(a1, . . . , ak , ak+1) = OD(mk, ak+1), а это все делители mk+1 = (mk, ak+1) по Теореме 2.

• Итак, утверждение доказано и OD(a1, . . . , an) — это все делители mn. Теперь понятно, что mn = (a1, . . . , an). □

Следствие 1

Для a1, . . . , an ∈ Z существует линейное представление НОД, то есть, такие x1, . . . , xn ∈ Z, что (a1, . . . , an) = x1a1 + . . . xnan.

*Доказательство.*

• Докажем индукцией по k, что существует линейное представление mk = (a1, . . . , ak).

База k = 2 доказана в Теореме 4.

• Переход k → k + 1. По Теореме 5 и индукционному предположению,

mk+1 = (a1, . . . , ak, ak+1) = (mk, ak+1) = ymk+xk+1ak+1 = y(x′1a1 + · · · + x′kak) + xk+1ak+1 = (yx′1)a1 + . . .(yx′k)ak + xk+1ak+1. Все коэффициенты yx′1, . . . , yx′ k , очевидно, целые. □

1. Взаимно простые числа. Свойства.

Определение

• Числа a1, . . . , an ∈ Z называются **взаимно простыми**, если (a1, . . . , an) = 1.

• Если любые два из a1, . . . , an взаимно просты, эти числа называются **попарно взаимно простыми**. Свойство 1

Если a1, . . . ,an ∈ Z попарно взаимно просты, то они взаимно просты.

*Доказательство.*

Если (a1, . . . ,an) = d > 1, то (a1, a2) d, а значит, (a1, a2) > 1. □

Свойство 2

Если a, b, c ∈ Z и (a, b) = 1, то (ac, b) = (c, b).

*Доказательство.*

• Пусть d = (c, b) и f = (ac, b).

• Из c d следует, что ac d. Значит, d ∈ OD(ac, b) и по Теореме 2 f d.

• Из b f следует, что bc f . Значит, f ∈ OD(ac, bc).

• По Теоремам 3 и 2, c = c(a, b) = (ac, bc) f .

• Следовательно, f ∈ OD(c, b) и по Теореме 2 d f .

• Из d, f ∈ N, d f и f  d следует, что d = f . □

Свойство 3

Если a, b, c ∈ Z, (a, b) = 1 и ac b, то c b.

*Доказательство.*

По Свойству 2 (c, b) = (ac, b) = b (последнее верно так как ac b). Следовательно, c b. □

Свойство 4

Пусть a1, . . . , an, b1, . . . , bm ∈ Z, причем (ai , bj) = 1 для всех i ∈ {1, . . . , n} и j ∈ {1, . . . , m}. Тогда (a1 . . . an, b1 . . . bm) = 1.

*Доказательство.*

• Докажем, что (a1 . . . ak, bj) = 1 для всех j ∈ {1, . . . , m} и k ∈ {1, . . . , n} индукцией по k.

База k = 1: дано в условии.

Переход k → k + 1: (a1 . . . akak+1, bj) = (a1 . . . ak, bj) = 1 по свойству 2 (так как (ak+1, bj) = 1).

• Пусть A = a1 . . . an. Докажем, что (A, b1 . . . bk) = 1 для всех k ∈ {1, . . . , m} индукцией по k.

База k = 1: доказано выше.

Переход k → k + 1: (A, b1 . . . bkbk+1) = (A, b1 . . . bk) = 1 по свойству 2 (так как (A, bk+1) = 1). □

1. Простые числа, свойства. Бесконечность количества простых.

Определение

• Натуральное число, имеющее ровно два натуральных делителя, называется **простым**.

• Натуральное число, имеющее более двух натуральных делителей, называется **составным**.

• Множество всех простых чисел обозначается **P**.

• Если p ∈ P, то натуральные делители числа p — это 1 и p.

• 1 ∉ P. Любое натуральное число, большее 1 — простое или составное.

Определение

Пусть a ∈ N. **Собственный делитель** числа a — это любой его делитель, отличный от 1.

Свойство 1

Если a ∈ N — составное, то существует разложение a = bc, где b, c ∈ N, a > b, c > 1.

*Доказательство.*

• Составное число a имеет собственный делитель b < a. Тогда a = bc, где c ∈ N. Очевидно, 1 < c < a. □

Свойство 2

Пусть a ∈ N, a ≠ 1, а d — минимальный собственный делитель a. Тогда d ∈ P.

*Доказательство.*

• По определению, d > 1.

• Предположим, что d — составное. По свойству 1 тогда d = bc, где d > b > 1.

• Из a d и d b следует, что a b. Значит, b < d — собственный делитель a, противоречие с выбором d.

Теорема 6

Простых чисел бесконечно много.   
*Доказательство.*

• Предположим противное, пусть P = {p1, . . . , pn}.

• Пусть m = p1 . . . pn + 1, а q — наименьший собственный делитель m.

• По свойству 2 тогда q ∈ P. Значит, q = pi для некоторого i ∈ {1, . . . , n}

• Так как m − 1 pi, (m, pi) = (1, pi) = 1 (по свойству 2 НОДа). Значит, m / pi , противоречие.

Свойство 3

Пусть a ∈ Z, p ∈ P. Тогда либо a p, либо (a, p) = 1.

*Доказательство.*

• Так как d = (a, p) ∈ N и p d, то d = 1 или d = p.

• Во втором случае (a, p) = p, следовательно, a p. □

Свойство 4

Пусть a1, . . . ,an ∈ Z и p ∈ P таковы, что a1. . .an p. Тогда существует такое i ∈ {1, . . . , n}, что ai p.

*Доказательство*.

• Предположим противное, пусть ai / p для всех i ∈ {1, . . . , n}. По Свойству 3 тогда (ai, p) = 1.

• По Свойству 4 взаимно простых чисел, тогда и (a1. . .an, p) = 1. Значит, a1. . .an / p. Противоречие. □

1. Основная теорема арифметики в Z.

Теорема 7

Любое натуральное число a > 1 раскладывается в произведение простых чисел. Такое разложение единственно с точностью до порядка сомножителей.

*Доказательство.*

∃.

Индукция.

База a ∈ P очевидна: подходит разложение a = a.

Переход.

• Пусть a — составное, а для всех меньших чисел теорема доказана.

• Тогда a = bc, где 1 < b, c < a. Следовательно, b = p1 . . . pn и c = q1 . . . qm.

• Тогда a = p1 . . . pnq1 . . . qm — искомое разложение.

!

Предположим противное, пусть a = p1 . . . pn = q1 . . . qm — два разложения a в произведение простых, причем a — наименьшее натуральное число, для которого разложение в произведение простых не единственно.

• Из a = p1 . . . pn q1 следует, что pi q1 для некоторого i ∈ {1, . . . , n}. НУО i = 1.

• Из p1, q1 ∈ P и p1 q1 следует, что p1 = q1 (единственным делителем простого p1, большим 1, является само p1).

• Тогда a′ = ap1 = p2 . . . pn = q2 . . . qm. Но разложение a′ в произведение простых единственно с точностью до порядка сомножителей, откуда следует, что разложение a — тоже единственно с точностью до порядка сомножителей. □

1. Каноническое разложение. Количество натуральных делителей числа.

Определение

**Каноническое разложение** — это преставление натурального числа в виде n = p1k1. . .psks , где p1, . . . ,ps ∈ P различны.

Определение

Для n ∈ N обозначим через **d(n)** количество натуральных делителей n.

Теорема 8

Пусть n = p1k1. . .psks — каноническое разложение. Тогда выполнены следующие утверждения.

1) n d, если и только если d = p1l1. . .psls , где 0 ≤ ℓi ≤ ki для всех i ∈ {1, . . . ,s}.

2) d(n) = (k1 + 1). . .(ks + 1).

*Доказательство.*

1)

⇐ . Очевидно.

⇒ .

• Если n d, то d не может иметь простых делителей, кроме p1, . . . , ps . Следовательно, d = p1l1. . .psls.

• Если ℓi > ki для какого-то i ∈ {1, . . . ,s}, то очевидно, что n / d.

2)

• Показатель степени простого числа pi в каноническом разложении делителя d | n можно выбрать ki + 1 способами (0, 1, . . . , ki).

• Перемножаем количества вариантов для p1, . . . , ps и получаем доказываемую формулу. □

1. Представление НОД чисел через их канонические разложения.

Теорема 9

Пусть a1, . . . ,am ∈ N, p1, . . . , ps ∈ P причем ai = p1ki,1. . . pski,s для всех i ∈ {1, . . . , m} (некоторые из показателей могут быть равны 0). Тогда (a1, . . . ,am) = p1min(k1,1,...,k1,m). . . psmin(ks,1 ,...,ks,m).

*Доказательство.*

• По теореме 8, d | at, если и только если d = p1ℓ1. . . psℓs, где ℓj ≤ kt,j для всех j ∈ {1, . . . ,s}.

• Следовательно, d ∈ OD(a1, . . . , am), если и только если d = p1ℓ1. . . psℓs, где ℓi ≤ min(k1,i , . . . , km,i) для всех i ∈ {1, . . . ,s}.

• Теперь понятно, что наибольший элемент в OD(a1, . . . , am) вычисляется в точности по формуле из условия. □

1. Линейные диофантовы уравнения с двумя неизвестными.

Линейные диофантовы уравнения с двумя неизвестными

• ax + by = c, (∗) где a, b, c ∈ Z — константы, x, y ∈ Z — неизвестные.

• Пусть d = (a, b). Если c / d, то (∗) не имеет решений.

• Далее c d. Пусть a = da′, b = db′, c = dc′ . Тогда уравнение (∗) эквивалентно a′x + b′y = c′ , где (a′ , b′ ) = 1. (∗∗)

• Существует линейное представление НОД: a′x0 + b′y0 = 1. Умножив на c′ , получим a′(x0c′) + b′(y0c ′) = c′.

Теорема 10

Решения уравнения (∗) представляются в виде x = x0c′ + tb′ , y = y0c′ − ta′ , где t ∈ Z.

Доказательство.

• Будем работать с эквивалентным уравнением (∗∗). Проверим, что это действительно его решения:

a′(x0c′+tb′)+b′(y0c′−ta′) = a′(x0c′)+b′(y0c′)+a′tb′−b′ta′ = c

• Пусть (x, y) — решение (∗). Тогда a′x+b′y = c′ = a′(x0c′)+b′(y0c′) ⇒ a′(x−x0c′) = b′(y0c′−y).

• Тогда a′(x − x0c′) b ′ . Так как (a′ ,b′) = 1, откуда x − x0c′ b ′ . Пусть x − x0c ′ = tb′ .

• Аналогично, y0c′ − y a′. Пусть y0c′ − y = sa′ .

• Тогда a′tb′ = b′sa′ , откуда s = t. □

1. Идеалы в Z

Идеалы в Z

• Пусть m ∈ N, тогда нетрудно проверить, что mZ = {mx : x ∈ Z} — идеал в Z.

Теорема 11

Пусть I — идеал в Z. Тогда I = mZ, где m ∈ N0.

*Доказательство.*

• Если I = {0}, то подходит m = 0. Далее I ≠ {0}.

• Пусть a ∈ I, a ≠ 0. Тогда и −a ∈ I. Одно из чисел a и -a — натуральное. Таким образом, I′ = I ∩ N ≠ ∅.

• Тогда существует минимальный элемент в I′, обозначим его m. Докажем, что I = mZ.

• Предположим противное, пусть b ∈ I, b / m. Тогда b = mq + r, где 0 < r < m (теорема о делении с остатком).

• Так как b, m ∈ I, имеем r = b − mq ∈ I. Тогда r ∈ I′ . Противоречие с минимальностью m.

1. Линейное представление НОД: доказательство существования с помощью идеала.

Теорема 12

Пусть a1, . . . ,an ∈ Z \ {0}. Тогда существует линейное представление (a1, . . . ,an), а OD(a1, . . . ,an) состоит из всех делителей (a1, . . . ,an).

*Доказательство.*

• Пусть I = ⟨{a1, . . . ,an}⟩. Этот идеал состоит из линейных комбинаций чисел a1, . . . , an. • Очевидно, I ̸= {0}. Тогда по Теореме 11 существует такое d ∈ N, что I = dZ — состоит из кратных d.

• Так как a1, . . . , an ∈ I, все они делятся на d, значит, d ∈ OD(a1, . . . , an).

• С другой стороны, d ∈ I, а значит, d = x1a1 + · · · + xnan, где x1, . . . , xn ∈ Z.

• Значит, для любого f ∈ OD(a1, . . . , an) мы имеем d f .

• Так как d > 0, d — наибольший элемент в OD(a1, . . . , an), то есть, d = (a1, . . . , an). □

1. Сравнения по модулю натурального числа, свойства. Вычеты.

Определение

Пусть m ∈ N; a, b ∈ Z. Будем говорить, что **a сравнимо с b по модулю m**, если a − b m.

Обозначения: a ≡m b или a ≡ b (mod m).

Лемма 1

Пусть m ∈ N; a, b ∈ Z. Следующие утверждения равносильны.

1 ◦ a ≡ b (mod m).

2 ◦ a − b m.

3 ◦ a и b имеют одинаковые остатки от деления на m.

4 ◦ a ≡ b (mod mZ).

*Доказательство.*

1 ◦ ⇐⇒ 2 ◦ по определению сравнения.

2 ◦ ⇐⇒ 3 ◦ очевидно.

2 ◦ ⇐⇒ 4 ◦ по определению главного идеала mZ. □

Свойство 1

Если a ≡m a′ и b ≡m b′, а x, y ∈ Z, то ax + by ≡m a′x + b′y.

*Доказательство.*

ax + by − (a′x + b′y) = x(a − a′) + y(b − b′) m. □

Свойство 2

Если a ≡m a′ и b ≡m b′, то ab ≡m a′b′.

*Доказательство.*

ab − a′b′ = (ab − a′b) + (a′b − a′b′) = (a − a′ )b + a′(b − b′) m. □

Свойство 3

Если a ≡m b и n ∈ N, то an ≡m bn.

*Доказательство.*

• Индукция по n. База n = 1 очевидна.

• Переход n → n + 1. Так как an ≡m bn (по индукционному предположению) и a ≡m b, по свойству 2 имеем an+1 = an · a ≡m bn · b = bn+1. □

Свойство 4

Если (a, m) = 1 и ab ≡m ac, то b ≡m c.

*Доказательство.*

ab ≡m ac ⇒ a(b − c) m ⇒ b − c m ⇒ b ≡m c (по Свойству 3 взаимно простых чисел можно сократить на a). □

Вычеты

• ≡m — отношение эквивалентности, так как это частный случай сравнения по модулю идеала (впрочем, можно несложно проверить напрямую).

Определение

**Вычет по модулю m** — это класс эквивалентности по ≡m.

• Перечислим тривиальные следствия Леммы 1.

• Каждый вычет по модулю m имеет вид a + mZ для некоторого a ∈ Z.

• В каждом вычете все числа имеют одинаковый остаток от деления на m, а числа из разных вычетов имеют разные остатки.

• Существует ровно m вычетов по модулю m.

1. Полная система вычетов, свойства.

Определение

Числа a1, . . . , am ∈ Z — образуют **полную систему вычетов по модулю m** (сокращенно: ПСВ (mod m)), если каждый вычет по модулю m содержит ровно одно из них.

Лемма 2

a1, . . . , am ∈ Z — ПСВ (mod m), если и только если никакие два из них не сравнимы по модулю m. Доказательство.

⇒ очевидно следует из определения.

⇐. Если есть m чисел, и никакие два из них не сравнимы по модулю m, то в каждом вычете по модулю m ровно одно из них. □

Теорема 13

Пусть a1, . . . ,am — ПСВ (mod m), k, b ∈ Z, причем (k, m) = 1. Тогда ka1 + b, . . . , kam + b — ПСВ (mod m).

Доказательство.

• Достаточно проверить критерий из Леммы 2.

• Пусть kai + b ≡m kaj + b ⇐⇒ k(ai − aj) m.

• Так как (k, m) = 1, это означает, что ai − aj m ⇐⇒ ai ≡m aj, что не так. □

1. Приведенная система вычетов, свойства.

НОД вычета и модуля. Приведенная система вычетов

• Если a ≡m b, то a − b m и по свойству 2 НОД мы имеем (a, m) = (b, m).

• Таким образом, для каждого вычета = a + mZ корректно определен НОД (, m) := (a, m). Определение

1) Вычет a по модулю m называется взаимно простым с модулем m, если (, m) = 1.

2) Для m ∈ N **функция Эйлера** φ(m) — количество чисел от 1 до m, взаимно простых с m.

• !!! φ(1) = 1.

• Существует ровно φ(m) вычетов по модулю m, взаимно простых с m.

Определение

Числа a1, . . . , aφ(m) образуют **приведенную систему вычетов по модулю m**, (сокращенно: ПрСВ (mod m)), если каждый вычет по модулю m, взаимно простой с m, содержит ровно одно из них.

Лемма 3

a1, . . . , aφ(m) ∈ Z — ПpСВ (mod m), если и только если все эти числа взаимно просты с m и никакие два из них не сравнимы по модулю m.

*Доказательство.*

⇒ очевидно следует из определения.

⇐. Есть φ(m) чисел, и никакие два из них не сравнимы по модулю m, а также есть ровно φ(m) вычетов в ПрСВ (взаимно простых с m). Значит, в каждом вычете из ПрСВ ровно одно из этих чисел. □ Теорема 14

Пусть a1, . . . , aφ(m) — ПрСВ (mod m), k ∈ Z, причем (k, m) = 1. Тогда ka1, . . . , kaφ(m) — ПрСВ (mod m). *Доказательство.*

• Достаточно проверить критерий из Леммы 3.

• Так как (k, m) = 1 и (ai , m) = 1, то (kai , m) = 1 (для всех i ∈ {1, . . . , φ(m)}).

• Если kai ≡m kaj , то ai ≡m aj по Свойству 4 сравнений, что не так. □

1. Теорема Эйлера.

Теорема Эйлера (Теорема 15)

Пусть m ∈ N, a ∈ Z, (a, m) = 1. Тогда aφ(m) ≡ 1 (mod m).

*Доказательство.*

• Пусть r1, . . . ,rφ(m) — ПрСВ (mod m).

• По Теореме 14 тогда и ar1, . . . , arφ(m) — ПрСВ (mod m).

• Введем обозначения i1, . . . , iφ(m) так, что r1 ≡m ari1 , . . . , rφ(m) ≡m ariφ(m) и {1, . . . , φ(m)} = {i1, . . . , iφ(m)}.

• Пусть R = r1 · · · · · rφ(m) . Тогда (R, m) = 1.

• Перемножая записанные выше сравнения, получаем R ≡ r1·· · ··rφ(m) ≡ ar1·· · ··arφ(m) ≡ aφ(m)·R (mod m). Сокращая на R, получаем 1 ≡ aφ(m) (mod m). □

1. Мультипликативность функции Эйлера.
2. Функция Эйлера: значение на степени простого числа, явный вид.
3. Сумма функции Эйлера по делителям числа.
4. Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю.
5. Алгоритм поиска обратного вычета. Решение сравнения с одним неизвестным.
6. Делимость на попарно взаимно простые числа.
7. Китайская теорема об остатках.
8. Алгоритмы поиска решения для КТО.
9. Функция Мёбиуса. Сумма функции Мёбиуса по промежуточным делителям.
10. Формула обращения Мёбиуса, аддитивный вариант.
11. Вывод формулы для функции Эйлера из формулы обращения Мёбиуса.
12. Формула обращения Мёбиуса, мультипликативнй вариант.
13. Сумма мультипликативной функции по делителям числа мультипликкативна.
14. Сумма натуральных делителей числа.
15. Первообразные корни из 1 в C.

# Многочлены над полем

1. Сложение и умножение многочленов. Степень многочлена. Свойства.
2. Кольцо многочленов.
3. Вложение *K* в *K*[*t*]. Константы. Ассоциированные многочлены.
4. Теорема о делении с остатком в кольце многочленов над полем.
5. Делимость многочленов. Свойства.
6. Идеалы в кольце многочленов над полем.
7. НОД в кольце многочленов над полем: теорема о линейном представлении.
8. Свойства НОДа в кольце многочленов над полем.
9. Вычисление НОДа нескольких многочленов через НОДы двух.
10. Взаимно простые многочлены. Свойства.
11. Неприводимые многочлены. Свойства.
12. Основная теорема арифметики в кольце многочленов над полем. Каноническое разложение.
13. Значение многочлена в точке. Корень многочлена. Теорема Безу.
14. Кратность корня. Теорема о сумме кратностей корней.
15. Производная многочлена. Производная суммы и произведения.
16. Производная многочлена, раскладываемого на линейные множители.
17. Определение кратности корня многочлена с помощью производной.
18. Основная теорема алгебры (формулировка). Неприводимые многочлены в C[*t*], разложение на линейные множители многочлена в C[*t*].
19. Сопряженные корни. Теорема о корнях многочлена с вещественными коэффициентами.
20. Неприводимые многочлены в R[*t*], разложение на неприводимые множители многочлена в R[*t*].
21. Теорема Виета.
22. Интерполяция: формула Лагранжа.
23. Метод интерполяции по Ньютону.
24. Рациональные функции над полем. Правильные дроби и их свойства.
25. Разложение правильной дроби в сумму правильных дробей, знаменатели которых — степени неприводимых многочленов.
26. Разложение правильной дроби в сумму простейших.
27. Связь задачи разложения правильной дроби в сумму простейших с интерполяцией. Критерий отсутствия кратных корней.
28. Поле C, как факторкольцо R[*x*].
29. Многочлен деления круга. Представление *tn −* 1 в виде произведение многочленов деления круга.
30. Многочлен деления круга: формула, целые коэфиициенты.

# Многочлены и теория чисел

1. Показатель, к которому принадлежит вычет. Свойства.

Определение

Пусть p ∈ P, a ∈ Zp, a ≠ 0, d ∈ N. Вычет a принадлежит к показателю d, если ad = 1, но as ≠ 1 при s ∈ N, s < d. Обозначение: a ∈p d.

Лемма 1

Пусть p ∈ P, a ∈ Zp. Тогда выполнены следующие утверждения.

1) Если ad = 1 и a ∈p s, то s | d.

2) Если a ∈p d, то d | p − 1.

*Доказательство.*

1. • Предположим противное и поделим d на s с остатком: d = sq + r, 0 < r < s.

• Тогда 1 = ad = asq+r = (as)q · ar = ar , что противоречит минимальности s.

1. По теореме Эйлера ap−1 = 1. Тогда по пункту 1 имеем d | p − 1. □
2. Количество корней многочлена td − 1 в Zp, где p − 1 d.

Лемма 2

Если p ∈ P и d | p − 1, то многочлен td − 1 ∈ Zp[t] имеет ровно d корней, все они не 0.

Доказательство.

• Многочлен tp−1 − 1 имеет в Zp[t] ровно p − 1 корень (по теореме Эйлера, все ненулевые вычеты его корни).

• Пусть p − 1 = qd. Тогда tp−1 − 1 = (td − 1)(t(q−1)d + · · · + td + 1) =: (td − 1)f (t).

• Так как deg(f ) = (q − 1)d, этот многочлен по Теореме 3.7 имеет не более (q − 1)d корней.

• Если td − 1 имеет менее d корней, то tp−1 − 1 = (td − 1)f (t) имеет менее d + (q − 1)d = p − 1 корней, противоречие. □

1. Количество вычетов, принадлежащих к показателю *d*.

Теорема 1

Если p ∈ P и d | p − 1, то к показателю d принадлежит ровно φ(d) вычетов.

*Доказательство.*

• Индукция по d. База d = 1 очевидна: a ∈p 1 ⇐⇒ a = 1.

• Все вычеты, принадлежащие к показателю d, являются корнями многочлена td − 1.

• Если s | d (скажем, d = qs) и b ∈p s, то bd = (bs q = 1, то есть, b — корень td − 1.

• Так как каждый ненулевой вычет принадлежит в точности одному показателю, вычеты, принадлежащие собственным делителям d дают нам = ( − φ(d) = d − φ(d) различных корней многочлена td − 1 (последнее равенство верно по Теореме 2.17).

• Оставшиеся d − (d − φ(d)) = φ(d) корней многочлена td − 1 принадлежат к d (по Лемме 1 они должны принадлежать к делителю d, а этим делителем может быть только само d). □

1. Первообразный корень по простому модулю и их количество. Структура приведенной системы вычетов.

Определение

Пусть p ∈ P. Вычет a ∈ Zp — **первообразный корень по модулю p**, если a ∈p p − 1.

• По Теореме 1 существует в точности φ(p − 1) первообразных корней по модулю p.

Теорема 2

Пусть p ∈ P, a — первообразный корень по модулю p. Тогда a, a2, . . . , ap−1 = 1 — ПрСВ (mod p), то есть, в точности все ненулевые вычеты из Zp.

*Доказательство.*

• Достаточно доказать, что ai ̸= aj при 1 ≤ j < i ≤ p − 1.

• Предположим противное, пусть ai = aj ⇐⇒ aj(ai−j − 1) = 0.

• Однако, aj  ≠ 0 и ai−j ≠ 1, так как 0 < i − j < p − 1. Противоречие. □

• Если a — первообразный корень по модулю p, то любой ненулевой вычет b ∈ Zp представляется в виде b = ak , где 1 ≤ k ≤ p − 1.

1. Квадратичные вычеты и невычеты в Z*p*, их количества.

Определение

Пусть p ∈ P, a ∈ Zp, a ≠ 0.

• Тогда a — **квадратичный вычет**, если существует такой b ∈ Zp, что b2 = a.

• Если такого b не существует, то a — **квадратичный невычет**.

• Далее в этом разделе p — нечетное простое число.

Лемма 3

Пусть p ∈ P нечетно, p1:= (p-1)/2. Тогда:

1) квадратичные вычеты в Zp — корни многочлена tp1 − 1;

2) если x2 = y2, то x = y или x = −y;

3) существует в точности (p−1) / 2 квадратичных вычетов в Zp.

*Доказательство.*

1. • Если a — квадратичный вычет, то a = b2 в Zp.

• По Теореме Эйлера ap1 − 1 = b2p1 − 1 = bp−1 − 1 = 0.

1. x2 = y2 ⇐⇒ (x +y)(x −y) = 0 ⇐⇒ x = y или x = −y.
2. Из пункта 2 следует, что ненулевые вычеты из Zp разбиваются на (p−1)/2 пар вида {x, −x}, дающих одинаковый квадрат. Значит, существует ровно (p−1)/2 квадратичных вычетов по модулю p. □

Лемма 4

Пусть p ∈ P нечетно, p1 := (p−1)/2 . Тогда выполнены следующие утверждения.

1) Квадратичные невычеты в Zp — корни многочлена tp1 + 1.

2) Существует в точности (p−1)/2 квадратичных невычетов в Zp.

*Доказательство.*

• По Теореме Эйлера многочлен tp−1 − 1 = (tp1 − 1)(tp1 + 1) имеет в Zp ровно p − 1 корень — все ненулевые вычеты.

• Многочлен tp1 − 1 имеет ровно p1 корней, как мы знаем из Леммы 2. По Лемме 3 все эти корни — квадратичные вычеты.

• Все p1 ненулевых вычетов, не являющиеся корнями tp1 − 1, являются корнями многочлена tp1 + 1.

• Значит, и многочлен tp1 + 1 имеет ровно p1 корней — в точности все квадратичные невычеты. □

1. Умножение квадратичных вычетов и невычетов на квадратичные вычеты и невычеты.

Лемма 5

Пусть p ∈ P нечетно, a, b ∈ Zp, a ≠ 0, b ≠ 0. Тогда:

1) Если a, b — квадратичные вычеты, то ab — квадратичный вычет.

2) Если a — квадратичный вычет, а b — квадратичный невычет, то ab — квадратичный невычет.

3) Если a, b — квадратичные невычеты, то ab — квадратичный вычет.

*Доказательство*.

1. • Существуют такие x, y ∈ Zp, что a = x2 и b = y2. Тогда ab = (xy)2.
2. • Вычеты a, 2a, . . . ,(p − 1)a — это в точности все ненулевые элементы Zp: среди них нет 0 и все они различны, так как ai = aj ⇒ i = j (равенство можно домножить на a−1 .)

• Значит, среди a, 2a, . . . ,(p − 1)a ровно по (p−1)/2 квадратичных вычетов и квадратичных невычетов.

• Так как при умножении a на квадратичные вычеты (на все (p−1)/2 штук) по пункту 1 получаются различные квадратичные вычеты (все (p−1)/2 штук), то при умножении a на квадратичные невычеты получаются квадратичные невычеты.

1. • И на этот раз a, 2a, . . . a(p − 1) — это в точности все ненулевые элементы Zp, среди них ровно по (p−1)/2 квадратичных вычетов и квадратичных невычетов.

• Так как при умножении a на квадратичные вычеты (на все (p−1)/2 штук) по пункту 2 получаются различные квадратичные невычеты (все (p−1)/2 штук), то при умножении a на квадратичные невычеты получаются квадратичные вычеты. □

1. Решение квадратных уравнений в Z*p*.

Решение квадратных уравнений в Zp

• Пусть p ∈ P, p ≠ 2, a, b, c ∈ Zp, a ≠ 0, D = b2 − 4ac.

ax2 + bx + c = 0⇐⇒x2 + b/a\*x + c/a = 0⇐⇒(x + b/2a)2 = b2/4a2 – c/a = (b2 − 4ac)/4a2⇐⇒(x + b/2a)2 = D /4a2. • Если D — квадратичный вычет, то D = d2 для некоторого d ∈ Zp и D/4a2 = (±d/2a)2. Тогда уравнение имеет два решения: x1 = (−b+d)/2a и x2 = (−b−d)/2a .

• Если D = 0, то уравнение имеет одно решение: x1 = −b/2a .

• Если D — квадратичный невычет, то D/4a2 — также квадратичный невычет, а значит, решений нет (так как квадратичный невычет не может быть равен квадрату).

1. Символ Лежандра. Свойства. (() = () (). Вычисление ().)

Определение

Пусть p ∈ P, a ∈ Z, a / p.

• Тогда a — **квадратичный вычет по модулю p**, если вычет a в Zp — квадратичный вычет.

• Аналогично, a — **квадратичный невычет по модулю p**, если вычет a в Zp — квадратичный невычет.

Определение

Пусть p ∈ P, a ∈ Z. Тогда символ Лежандра

( =

Свойство 1

( ≡ (mod p).

*Доказательство.*

• a — квадратичный вычет по модулю p ⇐⇒ a — квадратичный вычет в Zp ⇐⇒ = 1.

• a — квадратичный невычет по модулю p ⇐⇒ a — квадратичный невычет в Zp ⇐⇒ = −1.

• a = 0 ⇐⇒ = 0. □

Свойство 2 (Первое дополнение к закону взаимности Гаусса.)

( ≡ (mod p).

Свойство 3

( = ( · (.

*Доказательство.*

• Следует из Леммы 5 и определения символа Лежандра

1. Формула () =

Лемма 6

Пусть p ∈ P, p1 = , a ∈ Z, a / p. Тогда () = .

*Доказательство.*

• Пусть M = {1, 2, . . . , p1}.

Утверждение 1

Для каждого j ∈ M существует sj ∈ {0, 1} и rj ∈ M такие, что ja ≡ (−1)sjrj (mod p).

*Доказательство.*

• Пусть r′j — остаток от деления ja на p.

• Если r′j ∈ M, то положим rj := r′j, sj = 0.

• Если r′j ∉ M, то r′j ∈ {p1 + 1, . . . , p − 1}, тогда p − r′j ∈ {1, . . . , p − 1 − p1 = p1} = M.

• В этом случае положим rj = p − r′j , sj = 1.

Утверждение 2

Если i, j ∈ M, i ≠j, то ri ≠ rj .

*Доказательство.*

• Предположим противное, пусть ri = rj .

• Если si = sj , то r′i = r′j.

• Следовательно, ia ≡pja ⇐⇒ a(i − j) p ⇒ i − j p, что не так (последний переход верен,так как(a, p)=1).

• Если si ̸= sj , то r′i = p − r′j .

• Следовательно, ia ≡p −ja ⇐⇒ a(i + j) p ⇒ i + j p, что не так: 2 ≤ i + j ≤ 2p1 = p − 1. □

Утверждение 3

sj = 1 ⇐⇒ [2aj/p] / 2.

*Доказательство.*

• Напомним, что aj = pq + r′j ⇐⇒ 2aj = 2pq + 2r′j , где r′j ∈ {1, . . . , p − 1}.

sj = 1 ⇐⇒ = p1 + 1 ≤ r′j ≤ p − 1 ⇐⇒ p+1 ≤ 2r′j ≤ 2p−2 ⇐⇒ p+1+2pq ≤ 2aj ≤ 2p−2+2pq

⇐⇒ p + 2pq < 2aj < 2p + 2pq ⇐⇒ 2q + 1 < < 2q + 2 ⇐⇒ = 2q + 1 / 2.

• Пояснение 1. Так как разность целых чисел не менее 1, p + 1 + 2pq ≤ 2aj ⇐⇒ p + 2pq < 2aj.

• Пояснение 2. Так как разность четных чисел не менее 2, 2aj ≤ 2p − 2 + 2pq ⇐⇒ 2aj < 2p + 2pq. □

• **Вернемся** к доказательству Леммы 6. По Утверждению 2, {r1, . . . ,rp1 } = M (так как все эти числа из M и различны, а |M| = p1).

• Пусть R = 1 · 2 · · · · · p1. Тогда r1r2 · · · · · rp1 = R.

• Напишем цепочку сравнений:

R ≡ · ≡ ≡ (mod p) ≡ R (mod p) (1).

• Сокращая (1) на R (можно, так как (R, p) = 1), получаем ≡ ≡ (mod p) (последний переход верен по Утверждению 3). □

1. Формула () = при нечетном a и вычислении ().

Лемма 7

Пусть p ∈ P, p1 = ,.

1) (Второе дополнение к закону взаимности Гаусса.) () = .

2) Пусть a ∈ Z, a / p и a / 2. Тогда () =

*Доказательство*

1. закон взаимности Гаусса.

Теорема 3 (Закон взаимности Гаусса.)

Пусть p, q ∈ P нечетны. Тогда () · () = .

*Доказательство.*

1. Лемма Гаусса и следствие о содержании произведения многочленов.

Определение

Пусть f (t) = antn + · · · + a0 ∈ Z[t]. Тогда его **содержание** c(f ) = (a0, . . . , an) (НОД коэффициентов). Лемма 8 (Лемма Гаусса.)

Пусть f , g ∈ Z[x], c(f ) = c(g) = 1. Тогда c(fg) = 1.

*Доказательство*.

Следствие 1

Для f , g ∈ Z[x] выполнено c(fg) = c(f )c(g).

*Доказательство.*

1. Лемма о связи разложений многочлена с целыми коэффициентами на множители в Q[*x*] и в Z[*x*]. Эквивалентность неприводимости в Z[*x*] и в Q[*x*].

Лемма 9

Пусть f ∈ Z[x], q1, . . . , qn ∈ Q[x], f = q1 . . . qn, deg(qi) ≥ 1 для всех i ∈ {1, . . . , n}. Тогда существуют такие p1, . . . , pn ∈ Z[x] и c1, . . . , cn ∈ Q, что f = p1 . . . pn и pi = ciqi для всех i ∈ {1, . . . , n}. *Доказательство.*

Следствие 2

Многочлен f ∈ Z[x] неприводим в Q[x], если и только если он неприводим в Z[x].

*Доказательство.*

1. ОТА в Z[*x*].

Определение

Многочлен f ∈ Z[t] — тривиальный, если c(f ) = 1.

Теорема 4

Любой многочлен f ∈ Z[x] с положительным старшим коэффициентом раскладывается в произведение f = r1 . . .rk · p1 . . . , pn, где r1, . . . ,rk ∈ P, а p1, . . . , pn ∈ Z[x] — тривиальные неприводимые многочлены с положительными старшими коэффициентами. Разложение единственно с точностью до перестановки сомножителей.

• Разумеется, многочлен f ∈ Z[x] с отрицательным старшим коэффициентом раскладывается в аналогичное произведение f = −r1 . . .rk · p1 . . . , pn.

*Доказательство.*

1. Критерий Эйзенштейна.

Критерий Эйзенштейна Теорема 5

Пусть f (t) = antn + · · · + a1t + a0 ∈ Z[t] и p ∈ P таковы, что an / p, an−1, . . . , a0 p и a0 / p2. Тогда f — неприводим в Z[t].

*Доказательство.*

Следствие 3

Пусть f (t) = antn + · · · + a1t + a0 ∈ Z[t] и p ∈ P таковы, что a0 / p, a1, . . . , an p и an / p2 . Тогда f — неприводим в Z[t].

• Доказательство аналогично Теореме 5.

1. Свойства рациональных корней и значений в целых точках многочленов с целыми коэффициентами.

Лемма 10

Пусть f (t) = antn + · · · + a0 ∈ Z[t], x, y ∈ Z, x ≠ y. Тогда f (x) − f (y) x − y.

Доказательство.

• НУО x − y > 0. Так как x ≡x−y y, для всех k ∈ {0, . . . , n} выполняется xk ≡x−y yk .

• Тогда f (x) = ≡x−y = f (y). □

Лемма 11

Пусть f (t) = antn + · · · + a0 ∈ Z[t], f ( ) = 0, где p, q ∈ Z, (p, q) = 1. Тогда an q и a0 p.

*Доказательство.*

0 = qn f() = anpn + an−1pn−1q + · · · + a1pqn−1 + a0qn . (1)

• Все слагаемые в правой части (1), кроме anpn, делятся на q, значит, и anpn q. Так как (p, q) = 1, получаем an q.

• Все слагаемые в правой части (1), кроме a0qn, делятся на p, значит, и a0qn p. Так как (p, q) = 1, получаем a0 p. □

Следствие 4

Пусть f (t) = tn + · · · + a0 ∈ Z[t], α ∈ Q, f(α) = 0. Тогда α ∈ Z.

*Доказательство.*

• Пусть α = , где p, q ∈ Z, (p, q) = 1.

• По Лемме 11, 1 q, то есть α ∈ Z. □

Лемма 12

Пусть f (t) = antn +· · ·+ a0 ∈ Z[t], f () = 0, где p, q ∈ Z, (p, q) = 1. Тогда f (k) kq − p для любого k ∈ Z.

*Доказательство.*

• qnf (k) = qn(f (k) – f()) = () –() = ,

так для всех i ∈ {1, . . . , n} (kq)i − pi kq − p ⇐⇒ (kq)i ≡kq-p pi ⇐ kq ≡kq−p p.

• Так как (qn, kq − p) = (q, p) = 1, из qnf (k) kq − p следует, что f (k) kq − p.

1. Разностный многочлен.

Определение

Пусть f ∈ K[x], где K — коммутативное кольцо с 1, причем K ⊃ Z.

• **Разностный многочлен** задается формулой ∆f(x) := f (x + 1) − f (x).

• Примеры подходящих колец K: Z, Q, R, C.

Лемма 13

Пусть f ∈ K[x],где K—коммутативное кольцо с 1,причем K⊃Z. Тогда ∆f ∈ K[x], deg(∆f ) = deg(f ) − 1. *Доказательство.*

• Пусть f (x) = anxn + · · · + a0, где n = deg(f ).

• По биному Ньютона, ak((x + 1)k − xk) =.

• Поэтому ∆f ∈ K[x].

• Одночлены с xn в ∆f сокращаются, а единственный одночлен с xn−1 — это anxn−1 с коэффициентом an ≠ 0. Следовательно, deg(∆f ) = n − 1.

# Линейные пространства

1. Линейное пространство. Свойства.

Определение

Пусть K — поле, V — множество, и определены операции + : V × V → V и · : K × V → V, удовлетворяющие следующим условиям.

1) Ассоциативность сложения. ∀a, b, c ∈ V (a + b) + c = a + (b + c).

2) Коммутативность сложения. ∀a, b ∈ V a + b = b + a.

3) Ноль. ∃0 ∈ V такой, что ∀a ∈ V a + 0 = a.

4) Обратный элемент. ∀a ∈ V ∃ −a ∈ V такой, что a + (−a) = 0.

5) Дистрибутивность. ∀α, β ∈ K и ∀a ∈ V выполнено (α + β)a = αa + βa.

6) Дистрибутивность. ∀α ∈ K и ∀a, b ∈ V выполнено α(a + b) = αa + αb.

7) Ассоциативность умножения. ∀α, β ∈ K и ∀a ∈ V выполнено α(βa) = (α · β)a.

8) Умножение на 1. ∀a ∈ V выполнено 1 · a = a. Тогда мы будем говорить, что V — **линейное пространство над полем K**, а элементы V называть **векторами**.

• Как правило, мы будем обозначать векторы строчными латинскими буквами, а числа из поля — греческими.

• 0-вектор (0 ∈ V) и 0 ∈ K — разные нули, хоть мы и обозначаем их одинаково.

Свойство 1

Ноль-вектор единственен

*Доказательство.*

Пусть есть два ноль-вектора: 01 и 02. Тогда 01 = 01 + 02 = 02. □

Свойство 2

Обратный вектор −a всегда единственен.

*Доказательство.*

Пусть a1 и a2 — два обратных вектора к a ∈ V. Тогда a1 + a = a + a2 = 0, откуда a1 = a1 + (a + a2) = (a1 + a) + a2 = a2. □

Определение

Для a, b ∈ V определим a − b := a + (−b).

Свойство 3

Для любого a ∈ V выполнено 0 · a = 0 (слева 0-число, справа 0-вектор).

*Доказательство.*

0 · a = (0 + 0) · a = 0 · a + 0 · a. Вычтем из левой и правой части 0 · a и получим то, что нужно. □ Свойство 4

Для любого a ∈ V выполнено −a = (−1) · a.

*Доказательство.*

• a + (−1) · a = 1 · a + (−1) · a = (1 − 1) · a = 0 · a = 0.

• По Свойству 2, обратный вектор единственен. Значит, −a = (−1) · a. □

1. Линейное подпространство.

Определение

Если U, V — линейные пространства над полем K, U ⊂ V, причем операции сложения и умножения в U и V одинаковы. Тогда U — линейное **подпространство** V, а V — линейное **надпространство** U.

Лемма 1

Пусть V — линейное пространство над полем K, U ⊂ V, причем U замкнуто по сложению векторов и умножению на число (то есть, ∀α ∈ K, ∀a, b ∈ U выполнено a + b ∈ U и αa ∈ U). Тогда U — линейное подпространство V (со сложением и умножением из V).

*Доказательство.*

• При выполнении этих условий, + : U × U → U и · : K × U → U.

• Отметим, что для любого a ∈ U выполнено −a ∈ U и 0 = a − a ∈ U.

• Теперь несложно понять, U — линейное пространство над K со сложением и умножением из V (6 свойств из определения наследуются из V, существование 0-вектора и обратного элемента обосновано выше). □

1. Линейная комбинация, линейная оболочка. Порождающая система векторов.

Определение

Пусть V — линейное пространство над полем K.

1) Пусть x1, . . . , xn ∈ V, α1, . . . , αn ∈ K. Тогда α1x1 + · · · + αnxn —**линейная комбинация** векторов x1, . . . , xn. Линейная комбинация называется **нетривиальной**, если не все α1, . . . ,αn нули.

2) Пусть M ⊂ V. **Линейная оболочка** множества M — это множество Lin(M) всех линейных комбинаций векторов из M (с любым количеством векторов).

Свойство 1

Если M ⊂ V, то и Lin(M) ⊂ V.

*Доказательство.*

Несложно проверить, что линейная комбинация векторов линейного пространства V всегда лежит в V.

Свойство 2

Для любого M ⊂ V, Lin(M) — линейное подпространство V.

Доказательство.

• Достаточно проверить замкнутость по сложению и умножению.

• Пусть x1, . . . , xn ∈ M, α1, . . . , αn ∈ K. Тогда β(α1x1 + · · · + αnxn) = (βα1)x1 + · · · + (βαn)xn ∈ Lin(M).

• Пусть, кроме того, β1, . . . , βn ∈ K. Тогда α1x1 + · · · + αnxn + β1x1 + · · · + βnxn = (α1 + β1)x1 + · · · + (αn + βn)xn ∈ Lin(M). (Здесь достаточно проверить сложение линейных комбинаций одних и тех же векторов, так как в линейную комбинацию можно добавить отсутствующие в ней вектора с нулевыми коэффициентами.) □

Определение

1) Пусть V — линейное пространство над полем K и M ⊂ V. Если Lin(M) = V, то M — **порождающая система векторов пространства V**.

2) Пространство V называется **конечно порожденным**, если оно имеет конечную порождающую систему векторов.

• В основном, мы будем изучать конечно порожденные линейные пространства.

1. Линейно зависимые и линейно независимые системы векторов и их свойства.

Определение

Пусть V — линейное пространство над полем K.

• Вектора x1, . . . , xn ∈ V называются **линейно зависимыми** (коротко: ЛЗ), если существует их нетривиальная линейная комбинация, равная 0. (То есть, α1, . . . , αn ∈ K не все равны 0, а α1x1 + · · · + αnxn = 0.) Если такой комбинации нет, то вектора x1, . . . , xn ∈ V называются **линейно независимыми** (коротко: ЛНЗ).

• Бесконечное множество векторов называется линейно зависимым, если из них можно составить нетривиальную линейную комбинацию, равную 0 и линейно независимым, если нельзя.

Свойство 0

Пусть V — линейное пространство над полем K, 0 ∈ M ⊂ V. Тогда множество векторов M ЛЗ. *Доказательство.*

Есть нетривиальная линейная комбинация 1 · 0 = 0. □

Свойство 1

Если множество векторов ЛЗ, то любое его надмножество тоже ЛЗ.

*Доказательство.*

Можно не использовать добавленные вектора в линейных комбинациях. □

Свойство 2

Если множество векторов ЛНЗ, то любое его подмножество тоже ЛНЗ.   
*Доказательство.*

Убрав некоторые вектора из множества, мы не добавим новых линейных комбинаций. □

Свойство 3

Если x1, . . . ,xn ∈ V ЛЗ, то среди них есть вектор, который является линейной комбинацией остальных.

Доказательство.

• Пусть α1x1 + · · · + αnxn = 0, НУО αn  ̸= 0.

• Тогда xn = −α1/αn \* x1 + · · · + −αn−1/αn \* xn−1 ∈ Lin(x1, . . . , xn−1). □

Свойство 4

Если x1, . . . , xn ∈ V ЛНЗ и y ∉ Lin(x1, . . . , xn), то x1, . . . , xn, y — ЛНЗ.

Доказательство.

• Пусть x1, . . . , xn, y — ЛЗ. Тогда существует нетривиальная линейная комбинация α1x1 + · · · + αnxn + βy = 0.

• Если β = 0, то не все α1, . . . , αn равны 0 и α1x1 + · · · + αnxn = 0, а значит, x1, . . . , xn ЛЗ, противоречие.

• Значит, β ̸= 0. Тогда y = −α1/β \* x1 + · · · + −αn/β \* xn ∈ Lin(x1, . . . , xn), противоречие. □

Свойство 5

Если x1, . . . , xn ∈ V ЛНЗ, а y ∈ V таков, что x1, . . . , xn, y — ЛЗ, то y ∈ Lin(x1, . . . , xn). *Доказательство.*

Прямое следствие Cвойства 4. □

1. Однородные системы линейных уравнений: приведение к ступенчатому виду, нетривиальное решение.

Определение

Пусть K — поле, ai,j ∈ K (где i ∈ {1, . . . , n}, j ∈ {1, . . . , m}), b1, . . . , bn ∈ K. Пусть x1, . . . , xm — неизвестные. Тогда **система линейных уравнений** (далее СЛУ) — это

,

СЛУ называется **однородной** (далее ОСЛУ), если b1 = · · · = bn = 0.

Элементарные преобразования СЛУ

1. Поменять местами два уравнения.
2. К одному уравнению прибавить другое, умноженное на λ ∈ K.
3. Умножить уравнение на λ ∈ K, отличное от 0.

• Везде умножение уравнения на число происходит вместе с правой частью.

Лемма 2

1) Элементарные преобразования всех трех типов обратимы, то есть имеют обратные элементарные преобразования.

2) Элементарные преобразования не меняют решений СЛУ.

*Доказательство.*

1. • Элементарное преобразование типа (I) само себе обратно.

• Рассмотрим элементарное преобразование типа (II), пусть мы к i-му уравнению прибавили j-е, умноженное на λ.

• Тогда обратное преобразование — прибавить к i-му уравнению j-е уравнение, умноженное на −λ.

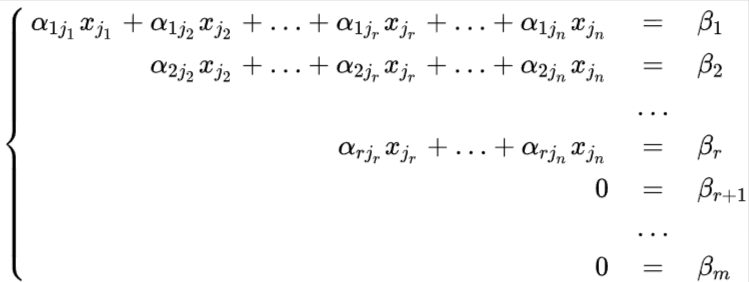
• Наконец, обратное преобразование к умножению уравнения на λ ̸= 0 — умножить его же на λ −1 .

1. • Очевидно, элементарное преобразование системы оставляет все ее решения (все уравнения останутся верными).

• Так как такое преобразование обратимо, добавиться новые решения не могут — иначе проведем обратное преобразование, и все новые решения сохранятся. □

Определение

ОСЛУ **приведена к ступенчатому виду**, если каждое уравнение, имеющее ненулевые коэффициенты, имеет вид xsi + ci,si +1xsi +1 + · · · + cm,skxm = 0, причем s1 < s2 < · · · < sk (где k — наибольший номер уравнения, имеющего ненулевые коэффициенты).



Лемма 3

ОСЛУ можно привести элементарными преобразованиями к ступенчатому виду.

Доказательство.

• Индукция по количеству неизвестных. База для одного неизвестного очевидна — наша система имеет вид ax1 = 0.

• Если a ̸= 0, то на a можно поделить и получить x1 = 0. Если же a = 0, система уже имеет ступенчатый вид

Переход.

• Если все коэффициенты при x1 равны 0, то достаточно привести к ступенчатому виду систему без x1, что можно сделать по индукционному предположению.

• Если не все коэффициенты ai,1 равны 0, то переставим уравнения (с помощью элементарных преобразований типа (I)) так, чтобы a1,1 ̸= 0, после чего поделим первое уравнение на a1,1 — оно примет нужный нам вид x1 + c1,2x2 + · · · + c1,mxm = 0.

• Теперь для всех k ∈ {2, . . . , n} вычтем из k уравнения новое первое уравнение, умноженное на ak,1 — во всех уравнениях, кроме первого, исчезнет переменная x1.

• Далее останется применить к системе из всех уравнений, кроме первого, индукционное предположение. □

Лемма 4

ОСЛУ, в которой неизвестных больше, чем уравнений, имеет нетривиальное решение (не все xi равны 0).

*Доказательство.*

• Приведем систему к ступенчатому виду.

• Будем считать, что обозначения как в определении. Пусть осталось k уравнений с ненулевыми коэффициентами. Тогда s1 < s2 < · · · < sk — не более чем n < m номеров переменных.

• Остались переменные с номерами не из {s1, . . . ,sk }. Положим все их равными 1.

• После чего последовательно вычислим: сначала xsk , потом xsk−1 , и так далее, xs1 .

• Переменную xsi мы вычисляем из i уравнения: xsi = −(ci,si+1xsi+1 + · · · + ci,mxm), все значения в правой части уже известны. □

1. Лемма о линейной зависимости линейных комбинаций.

Лемма 5

Пусть V — линейное пространство над полем K, n < m, a1, . . . , an ∈ V и y1, . . . , ym ∈ Lin(a1, . . . , an). Тогда y1, . . . ,ym ЛЗ.

Доказательство.

• Пусть y1 = β1,1a1 + · · · + βn,1an, . . . , ym = β1,ma1 + · · · + βn,man.

• Мы хотим найти такие λ1, . . . , λm ∈ K (не все равные 0), что λ1y1 + · · · + λmym = 0. Это означает, что 0 = λ1(β1,1a1 +· · ·+βn,1an)+· · ·+λm(β1,ma1 +· · ·+βn,man) = (β1,1λ1 + · · · + β1,mλm)a1 + · · · + (βn,1λ1 + · · · + βn,mλm)an.

• Для равенства нулю этого выражения достаточно, чтобы были равны 0 коэффициенты при a1, . . . , an. Это дает нам ОСЛУ (относительно неизвестных λ1, . . . , λm):

• В этой ОСЛУ неизвестных больше, чем уравнений. Значит, она имеет нетривиальное решение — соответствующие λ1, . . . , λm дают линейную зависимость y1, . . . , ym.

1. Базис, размерность. Корректность определения размерности. Разложение по базису.

Определение

1) **Базис** линейного пространства — это линейно независимая порождающая система векторов.

2) **Размерность** линейного пространства V (обозначение: dim(V)) — это количество элементов в базисе. Если пространство V имеет бесконечный базис, то dim(V) = ∞.)

Отдельно скажем о размерности пространства, состоящего из 0: dim({0}) = 0.

• Позже мы докажем существование базиса в конечно порожденном пространстве. А сейчас докажем корректность определения размерности.

Лемма 6

Размерность определена корректно, то есть, любые два базиса пространства V имеют одно и то же число элементов (любые два бесконечных базиса мы считаем равными по количеству элементов.) *Доказательство.*

• Пусть V имеет два базиса с разным числом векторов. Рассмотрим меньший из них - скажем, e1,..., en.

• Тогда все вектора большего базиса принадлежат V = Lin(e1, . . . , en), а значит, больший базис ЛЗ по Лемме 5, противоречие. □

Лемма 7

Пусть e1, . . . , en — базис линейного пространства V. Тогда для любого x ∈ V существует единственное представление в виде линейной комбинации x = α1e1 + · · · + αnen, где α1, . . . , αn ∈ K. *Доказательство.*

• Так как базис является порождающей системой векторов, такое представление существует.

• Пусть есть два представления: x = α1e1 + · · · + αnen = β1e1 + · · · + βnen.

• Тогда (α1 − β1)e1 + · · · + (αn − βn)en = 0.

• Так как базис ЛНЗ, отсюда следует, что α1 − β1 = · · · = αn − βn = 0, то есть два наших представления одинаковы. □

1. Существование базиса в конечно порожденном пространстве. Выделение базиса из конечной порождающей системы.

Теорема 1

Пусть V — конечно порожденное линейное пространство над полем K. Тогда V имеет базис. Более того, из любой конечной порождающей системы векторов V можно выделить базис.

Доказательство.

• Пусть a1, . . . , an — любая конечная порождающая система V (есть у конечно порожденного пространства).

• Если эти вектора ЛНЗ, то они — базис. Если же они ЛЗ, то по Свойству 3 ЛЗ векторов, один из них является линейной комбинацией остальных. Пусть, скажем, an = β1a1 + · · · + βn−1an−1.

• Докажем, что a1, . . . , an−1 — тоже порождающая система векторов V. Пусть x ∈ V, тогда существует преставление x = α1a1+· · ·+αnan = α1a1+· · ·+αn−1an−1+αn(β1a1+· · ·+βn−1an−1) = (α1 + αnβ1)a1 + · · · + (αn−1 + αnβn−1)an−1.

• Таким образом, мы уменьшили порождающую систему на один вектор. Такие шаги не могут продолжаться бесконечно. Значит, в некоторый момент мы получим ЛНЗ порождающую систему векторов — то есть, базис. □

1. Дополнение до базиса линейно независимой системы. в конечномерном пространстве.

Теорема 2

Пусть V — конечно порожденное линейное пространство над полем K, а векторы a1, . . . , an ЛНЗ. Тогда эти векторы можно дополнить до базиса.

*Доказательство.*

• Если a1, . . . , an — порождающая система V, то это — базис.

• Иначе есть вектор an+1 ∈ V\Lin(a1, . . . , an).

• По свойству 4 ЛНЗ векторов, a1, . . . , an, an+1 ЛНЗ.

• Будем так действовать, пока это возможно.

• Пространство V имеет конечную порождающую систему — скажем, из m векторов. Тогда по Лемме 5 не существует множества более чем из m ЛНЗ векторов.

• Значит, наш процесс должен закончиться и в некоторый момент мы получим линейно независимую порождающую систему векторов — то есть, базис. □

1. Три эквивалентных определения базиса.

Теорема 3

Пусть V — конечно порожденное линейное пространство над полем K, a e1, . . . , en ∈ V. Тогда следующие три утверждения равносильны.

1 ◦ e1, . . . , en — базис V.

2 ◦ e1, . . . , en — минимальная порождающая система векторов в V.

3 ◦ e1, . . . , en — максимальная ЛНЗ система векторов в V.

Доказательство.

1 ◦ ⇒ 2 ◦ . Если есть порождающая система f1, . . . , fm из m < n векторов, то e1, . . . , en ∈ Lin(f1, . . . , fm) и по Лемме 5 вектора e1, . . . , en ЛЗ, что не так.

2 ◦ ⇒ 1 ◦ . Пусть e1, . . . , en — минимальная порождающая система векторов в V. По Теореме 1 из этих векторов можно выбрать базис, который также является порождающей системой векторов. Значит, в нем не может быть менее n векторов, то есть, e1, . . . , en — базис.

1 ◦ ⇒ 3 ◦ . Если есть ЛНЗ система f1, . . . , fm из m > n векторов, то дополним ее до базиса (это можно сделать по Теореме 2). Тогда у V существуют два базиса с разным числом векторов (n и не менее чем m), что невозможно.

3 ◦ ⇒ 1 ◦ . Пусть e1, . . . , en — максимальная ЛНЗ система векторов в V. Ее можно дополнить до базиса, который тоже является ЛНЗ системой векторов, а значит, не может иметь более n векторов. Следовательно, e1, . . . , en — базис. □

1. Сумма и пересечение линейных пространств.

Пересечение линейных пространств. (Лемма 8)

Пусть {Ui}i∈I — множество линейных подпространств линейного пространства V над полем K. Тогда U = ∩i∈I Ui — тоже линейное подпространство V.

*Доказательство.*

• Достаточно проверить замкнутость по сложению и умножению на число.

• Пусть a, b ∈ U. Тогда для всех i ∈ I мы имеем a, b ∈ Ui .

• Следовательно, для всех i ∈ I мы имеем a + b ∈ Ui , откуда следует, что a + b ∈ U.

• Пусть λ ∈ K. Тогда для всех i ∈ I мы имеем λa ∈ Ui , откуда следует, что λa ∈ U. □

Определение

Пусть {Ui}i∈I — множество линейных подпространств линейного пространства V над полем K. Тогда — это множество всех сумм вида xi1 + · · · + xin , где ij ∈ I, xij ∈ Uij для всех j ∈ {1, . . . , n} (число n не фиксировано).

• Другими словами, **сумма линейных подпространств V** — это множество всех конечных сумм элементов, взятых по одному из пространств, что мы складываем.

Лемма 9

Пусть {Ui}i∈I — множество линейных подпространств линейного пространства V над полем K. Тогда U = — тоже линейное подпространство V.

*Доказательство.*

• Достаточно проверить замкнутость по сложению и умножению на число.

• Пусть a, b ∈ U. Тогда существуют представления a = ai1 + · · · + ain , b = bi1 + · · · + bin , где i1, . . . ,in ∈ I, aij , bij ∈ Uij для всех j ∈ {1, . . . , n} (индексы в суммах для a и b можно считать одинаковыми: при необходимости можно дополнить суммы нулевыми слагаемыми).

• Тогда aij + bij ∈ Uijдля всех j ∈ {1, . . . , n}, откуда следует, что a + b = (ai1 + bi1 )+· · ·+(ain + bin) ∈ U.

• Пусть λ ∈ K. Тогда λaij ∈ Uij для всех j ∈ {1, . . . , n}, откуда следует, что λa = λai1 + · · · + λain ∈ U. □

1. Размерность суммы двух линейных пространств.

Размерность суммы двух линейных пространств (Теорема 4)

Пусть U, W — конечномерные линейные подпространства линейного пространства V над полем K. Тогда dim(U + W) = dim(U) + dim(W ) − dim(U ∩ W ).

*Доказательство.*

• Пусть v1, . . . , vk — базис U ∩ W . Дополним его до базиса U: v1, . . . , vk , u1, . . . , un.

• Также дополним базис U ∩ W до базиса W : v1, . . . , vk , w1, . . . ,wm.

• Тогда dim(U) = k + n, dim(W ) = k + m, dim(U ∩ W ) = k.

• Нам нужно доказать, что dim(U + W ) = k + m + n, для чего достаточно доказать, что v1, . . . , vk , u1, . . . , un, w1, . . . ,wm — базис U + W .

• Из Утверждений 1 и 2 немедленно следует, что v1, . . . , vk , u1, . . . , un, w1, . . . ,wm — базис U + W .

• Теорема доказана. □

Утверждение 1

v1, . . . , vk , u1, . . . , un, w1, . . . ,wm — порождающая система векторов U + W .

*Доказательство.*

• Пусть v ∈ U + W , тогда v = u + w, где u ∈ U, w ∈ W . Тогда существуют представления

u = α1v1 + · · · + αkvk + β1u1 + · · · + βnun,

w = α′1v1 + · · · + α′kvk + γ1w1 + · · · + γmwm, где α1, α′1, . . . , αk,α′k , β1, . . . , βn, γ1, . . . , γm ∈ K.

• Тогда v = u + w = (α1 + α′1 )v1 + · · · + (αk + α′k)vk + β1u1 + · · · + βnun + γ1w1 + · · · + γmwm — искомое представление. □

Утверждение 2

v1, . . . , vk , u1, . . . , un, w1, . . . ,wm ЛНЗ.

*Доказательство.*

• Предположим, что α1v1+· · ·+αkvk +β1u1+· · ·+βnun+γ1w1+· · ·+γmwm = 0.

• Нам нужно доказать, что все коэффициенты в этом представлении равны 0. Перепишем его в виде α1v1 + · · · + αkvk + β1u1 + · · · + βnun = x = − γ1w1 − · · · − γmwm. (1)

• Тогда x ∈ U (так как это линейная комбинация базисных векторов U) и x ∈ W (так как это линейная комбинация базисных векторов W ). Следовательно, x ∈ U ∩ W .

• Значит, можно разложить x по базису U ∩ W : x = λ1v1 + · · · + λkvk (2)

• Но (1) и (2) — два разложения x по базису U, а такое разложение единственно. Значит, β1 = · · · = βn = 0.

• Теперь можно переписать (1) в виде α1v1 + · · · + αkvk = x = −γ1w1 − · · · − γmwm. (3)

• Это два разложения x по базису W , но такое разложение также единственно. Следовательно, α1 = · · · = αk = γ1 = · · · = γm = 0, что и требовалось доказать. □

1. Прямая сумма. Свойство прямой суммы.

Определение

Пусть {Ui}i ∈ I — множество линейных подпространств линейного пространства V над полем K, U = .

• Тогда U — **прямая сумма**, если из xi1 + · · · + xin = 0 (где i1, . . . , in ∈ I — различные индексы, xij ∈ Uij для всех j ∈ {1, . . . , n}) следует, что xi1 = · · · = xin = 0.

• Обозначение: U = ⊕i∈I Ui

Свойство

Пусть U = ⊕i∈I Ui, x ∈ U, x ≠ 0. Тогда существует единственное представление вида x = xi1+· · ·+xin, где i1, . . . , in ∈ I — различные индексы, xij ∈ Uij и xij ≠ 0 для всех j ∈ {1, . . . , n}.

*Доказательство.*

• Существование такого представления следует из определения суммы линейных пространств.

• Предположим, что есть два таких представления. Дополним их нулями так, чтобы суммировались элементы одних и тех же подпространств: x = xi1 + · · · + xin = x′i1 + · · · + x′in.

• Тогда 0 = (xi1 − x′i1) + · · · + (xin − x′in).

• По определению прямой суммы, все слагаемые равны 0. Значит, xi1 = x′i1 , . . . , xin = x′in, то есть, наши представления совпадают. □

1. Критерий прямой суммы.

Критерий прямой суммы (Теорема 5)

Пусть {Ui}i∈I — множество линейных подпространств линейного пространства V над полем K, U = . Для каждого i ∈ I пусть U′i = .(сумма всех подпространств, кроме Ui). Тогда U = ⊕ i∈I Ui, если и только если Ui ∩ U′i = {0} для каждого i ∈ I.

*Доказательство.*

⇒. • Предположим, что Ui ∩ U′i ∋ x, x ̸= 0 для некоторого i ∈ I.

• Из x ∈ U′i следует, что существует представление x = xj1 + · · · + xjn , где xjs ∈ Ujs , js ̸= i для всех s ∈ {1, . . . , n}.

• Тогда −x ∈ Ui и 0 = (−x) + xj1 + · · · + xjn — представление, которого не может быть по определению прямой суммы, противоречие.

⇐. • Предположим, что U — не прямая сумма.

• Тогда существует представление 0 = xj1 + · · · + xjn, где xjs ∈ Ujs , xjs ̸= 0 для всех s ∈ {1, . . . , n}.

• Тогда −xj1 = xj2 + · · · + xjn ∈ U′j1 , но при этом, очевидно, −xj1 ∈ Uj1 . Таким образом, Uj1 ∩ U′j1 ̸= {0}, противоречие. □

1. Размерность и базис прямой суммы конечного числа пространств.

Теорема 6

Пусть U1, . . . ,Un — линейные подпространства конечномерного линейного пространства V над полем K, а U = Ui . Тогда dim(U) = dim(U1) + · · · + dim(Un).

Доказательство.

• Индукция по n.

База n = 2. В этом случае U = U1 ⊕ U2 и U′1 = U2. По критерию прямой суммы, U1 ∩ U2 = {0}, следовательно, dim(U1 ∩ U2) = 0 и dim(U1 ⊕ U2) = dim(U1) + dim(U2).

Переход n − 1 → n.

• Пусть W = U′n = U1 + · · · + Un−1. Докажем, что сумма из определения W прямая.

• Для всех i ∈ {1, . . . , n − 1} определим W′i = . Тогда W′i ⊂ U′i .

• По Теореме 5, из W′i ∩ Ui ⊂ U′i ∩ Ui = {0} следует, что W — прямая сумма.

• Следовательно, dim(W ) = dim(U1) + · · · + dim(Un−1).

• Так как W ∩ Un = U′n ∩ Un = {0}, сумма U = W + Un также прямая. Следовательно, dim(U) = dim(W) + dim(Un) = dim(U1) + · · · + dim(Un−1) + dim(Un), что нам и нужно. □

Следствие 1

Пусть U1, . . . ,Un — линейные подпространства конечномерного линейного пространства V над полем K, а U = Ui . Для каждого i ∈ {1, . . . , k} пусть , . . . , — базис Ui . Тогда , . . . , , . . . , , . . . , — базис U.

*Доказательство.*

• Докажем, что , . . . , , . . . , , . . . , — порождающая система векторов U.

• Любой вектор x ∈ U представим в виде x = x1 + · · · + xk , где xi ∈ Ui для любого i ∈ {1, . . . , k}.

• Вектор xi ∈ Ui можно разложить по базису Ui : xi = .

• Тогда x = — искомое представление.

• Из любой порождающей системы векторов по Теореме 1 можно извлечь базис. Но количество векторов в базисе равно dim(U) = dim(U1) + · · · + dim(Uk ) — а именно столько векторов у нас и есть. Значит, наша система векторов и есть базис U.

1. Аффинные подпространства. Свойства.

Определение

Пусть U — линейное подпространство линейного пространства V над полем K, a ∈ V. Тогда U + a = {x + a : x ∈ U} — аффинное подпространство V. Положим dim(U + a) := dim(U).

• Таким образом, аффинное подпространство — это сдвиг линейного подпространства на вектор.

• Простейший пример, показывающий что это такое. Пусть V = R2 — стандартная евклидова плоскость. Тогда линейные подпространства V размерности 1 — это прямые, проходящие через 0, а аффинные подпространства — это все прямые.

• Здесь и далее U — линейное **подпространство** линейного пространства V над полем K, a, b ∈ V.

Свойство 1

U + a = U + b, если и только если a − b ∈ U.

*Доказательство.*

⇒. Если U + a = U + b, то a ∈ U + b. Так как a = b + (a − b), то a − b ∈ U.

⇐.

• Пусть a − b ∈ U, а x ∈ U + a. Тогда существует такое u ∈ U, что x = a + u.

• Но (a − b) + u ∈ U (линейное подпространство замкнуто по сложению), значит, x = a + u = b + (a − b + u) ∈ U + b. Таким образом, U + a ⊂ U + b.

• Так как b − a ∈ U, аналогично получается, что U + b ⊂ U + a. □

Свойство 2

Пусть λ1, . . . , λn ∈ K, λ1 + · · · + λn = 1, x1, . . . , xn ∈ U + a. Тогда λ1x1 + · · · + λnxn ∈ U + a. *Доказательство.*

• Пусть xi = ui + a, где ui ∈ U для всех i ∈ {1, . . . , n}.

• Тогда u = λ1u1 + · · · + λnun ∈ U и λ1x1 + · · · + λnxn = λ1(u1 + a) + · · · + λn(un + a) = (λ1u1 + · · · + λnun) + (λ1 + · · · +λn)a = u + a ∈ U + a. □

Свойство 3

Пусть W ⊂ V таково, что для любых w1,w2,w3 ∈ W и таких λ1, λ2, λ3 ∈ K, что λ1 + λ2 + λ3 = 1, выполнено λ1w1 + λ2w2 + λ3w3 ∈ W . Тогда W — аффинное подпространство V.

*Доказательство.*

1. Факторпространство и его размерность.

Определение

Пусть U — линейное подпространство линейного пространства V над полем K.

• **Факторпространство** V/U = {U + a : a ∈ V}.

• Будем использовать обозначение  := U + a.

• Сложение и умножение в V/U определим так: + := ; λ := .

• Введем отношение a ∼ b на V, означающее что a + U = b + U.

• По доказанному ранее, a ∼ b ⇐⇒ a − b ∈ U.

• Несложно проверить, что ∼ — отношение эквивалентности, а классы эквивалентности — как раз аффинные подпространства вида a + U

Лемма 10

1) Сложение и умножение в V/U определены корректно.

2) V/U с этими операциями является линейным пространством над полем K.

*Доказательство.*

Теорема 7

Пусть U — линейное подпространство конечномерного линейного пространства V над полем K. Тогда dim(V/U) = dim(V) − dim(U).

*Доказательство.*