Конспекты к коллоквиуму по линейной алгебре
Лектор: Карпов Дмитрий Валерьевич

Егор Федоров, P3115
Университет ИТМО

2022 — 2023

Оглавление

1 Основные понятия **3**

1.1 Кольцо, поле, типы колец . . . 3
1.2 Свойства 0, 1 и обратных элементов. Вычитание и деление . . . 3
1.3 Подкольцо и подполе . . . 5
1.4 Гомоморфизмы колец. Ядро и образ гомоморфизма . . . 5
1.5 Типы гомоморфизмов. Мономорфизм и ядро . . . 6
1.6 Отображение, обратное к изоморфизму — изоморфизм . . . 6
1.7 Изоморфные кольца . . . 7
1.8 Идеал. Ядро гомоморфизма является идеалом . . . 7
1.9 Идеал и обратимые элементы. Идеалы в поле. Гомоморфизм из поля — инъекция . . . 8
1.10 Идеал, порожденный множеством элементов. Главный идеал . . . 8
1.11 Сравнения по модулю идеала. Вычеты . . . 8
1.12 Факторкольцо . . . 9
1.13 Теорема о гомоморфизме колец . . . 9
1.14 Дроби: эквивалентность, простейшие свойства. Сложение и умножение дробей . . . 9
1.15 Поле частных . . . 10
1.16 Вложение кольца в поле частных . . . 11
1.17 Характеристика поля . . . 11
1.18 Теорема о подполе . . . 12

2 Комплексные числ **13**

2.1 Вещественная и мнимая часть, умножение, сложением, норма, модуль . . . 13
2.2 Поле комплексных чисел . . . 13
2.3 Тригонометрическая форма записи комплексного числа. Изменение модуля и аргумента при перемножении комплексных чисел. Формула Муавра . . . 14
2.4 Вложение вещественных чисел в комплексные . . . 14
2.5 Извлечение корня из комплексного числа. Корни из 1 . . . 14

3 Целые числа **15**

3.1 Делимость. Свойства. Теорема о делении с остатком . . . 15
3.2 НОД. Свойства . . . 16
3.3 Алгоритм Евклида. Следствия из алгоритма Евклида . . . 16
3.4 Линейное представление НОД . . . 17
3.5 НОД нескольких чисел через НОД двух чисел. Линейное представление НОД нескольких чисел . . . 17
3.6 Взаимно простые числа. Свойства . . . 17
3.7 Простые числа, свойства. Бесконечность количества простых . . . 18
3.8 Основная теорема арифметики в Z . . . 19
3.9 Каноническое разложение. Количество натуральных делителей числа . . . 19
3.10 Представление НОД чисел через их канонические разложения . . . 19
3.11 Линейные диофантовы уравнения с двумя неизвестными . . . 19
3.12 Идеалы в . . . 20
3.13 Линейное представление НОД: доказательство существования с помощью идеала . . . 20
3.14 Сравнения по модулю натурального числа, свойства. Вычеты . . . 20
3.15 Полная система вычетов, свойства . . . 21
3.16 Приведенная система вычетов, свойства . . . 21
3.17 Теорема Эйлера . . . 21
3.18 Мультипликативность функции Эйлера . . . 22
3.19 Функция Эйлера: значение на степени простого числа, явный вид . . . 22
3.20 Сумма функции Эйлера по делителям числа . . . 22
3.21 Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю . . . 23
3.22 Алгоритм поиска обратного вычета. Решение сравнения с одним неизвестным . . . 23
3.23 Делимость на попарно взаимно простые числа . . . 23
3.24 Китайская теорема об остатках . . . 24
3.25 Алгоритмы поиска решения для КТО . . . 24

3.26 Функция Мёбиуса. Сумма функции Мёбиуса по промежуточным делителям . . . 24
3.27 Формула обращения Мёбиуса, аддитивный вариант . . . 25
3.28 Вывод формулы для функции Эйлера из формулы обращения Мёбиуса . . . 25
3.29 Формула обращения Мёбиуса, мультипликативнй вариант . . . 25
3.30 Сумма мультипликативной функции по делителям числа мультипликкативна . . . 25
3.31 Сумма натуральных делителей числа . . . 25
3.32 Первообразные корни из 1 в C . . . 25

4 Многочлены над полем **26**
4.1 Сложение и умножение многочленов. Степень многочлена. Свойства . . . 26
4.2 Кольцо многочленов . . . 27
4.3 Вложение K в $K[t]$. Константы. Ассоциированные многочлены . . . 27
4.4 Теорема о делении с остатком в кольце многочленов над полем . . . 27
4.5 Делимость многочленов. Свойства . . . 28
4.6 Идеалы в кольце многочленов над полем . . . 28
4.7 НОД в кольце многочленов над полем: теорема о линейном представлении . . . 28
4.8 Свойства НОДа в кольце многочленов над полем . . . 29
4.9 Вычисление НОДа нескольких многочленов через НОДы двух . . . 30
4.10 Взаимно простые многочлены. Свойства . . . 30
4.11 Неприводимые простые многочлены. Свойства . . . 31
4.12 Основная теорема арифметики в кольце многочленов над полем. Каноническое разложение . . . 31
4.13 Значение многочлена в точке. Корень многочлена. Теорема Безу . . . 31
4.14 Кратность корня. Теорема о сумме кратностей корней . . . 32
4.15 Производная многочлена. Производная суммы и произведения . . . 32
4.16 Производная многочлена, раскладываемого на линейные множители . . . 33
4.17 Определение кратности корня многочлена с помощью производной . . . 33
4.18 Основная теорема алгебры (формулировка). Неприводимые многочлены в $\mathbb{C}[t]$, разложение на линейные множители многочлена в $\mathbb{C}[t]$. . . . 33
4.19 Сопряженные корни. Теорема о корнях многочлена с вещественными коэффициентами . . . 34
4.20 Неприводимые многочлены в $\mathbb{R}[t]$, разложение на линейные множители многочлена в $\mathbb{R}$[t]. . . . 34
4.21 Теорема Виета . . . 34
4.22 Интерполяция: формула Лагранжа . . . 35
4.23 Метод интерполяции по Ньютону . . . 35
4.24 Рациональные функции над полем. Правильные дроби и их свойства . . . 35
4.25 Разложение правильной дроби в сумму правильных дробей, знаменатели которых — степени неприводимых многочленов . . . 35
4.26 Разложение правильной дроби в сумму простейших . . . 35
4.27 Связь задачи разложения правильной дроби в сумму простейших с интерполяцией. Критерий отсутствия кратных корней . . . 35
4.28 Поле $\mathbb{C}$, как факторкольцо $[x]$. . . . 35
4.29 Многочлен деления круга. Представление t^{n-1} в виде поризведение многочленов деления круга. . . . 35
4.30 Многочлен деления круга: формула, целые коэфиициенты . . . 35

5 Многочлены и теория чисел **36**
5.1 Показатель, к которому принадлежит вычет. Свойства. . . . 36
5.2 Количество корней многочлена $t^d - 1$ в $\mathbb{Z}_p$ . . . 36
5.3 Количество вычетов, принадлежащих к показателю d. . . . 36
5.4 Первообразный корень по простому модулю и их количество. Структура приведенной системы вычетов. 36
5.5 Квадратичные вычеты и невычеты в Zp, их количества. . . . 37
5.6 Умножение квадратичных вычетов и невычетов на квадратичные вычеты и невычеты. . . . 37
5.7 Решение квадратных уравнений в Zp. . . . 37
5.8 Символ Лежандра . . . 37
5.9 Формула при любом n . . . 37
5.10 Формула при нечетном n. . . . 37
5.11 Квадратичный закон взаимности Гаусса. . . . 37
5.12 Лемма Гаусса и следствие о содержании произведения многочленов. . . . 37
5.13 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]. . . . 37
5.14 ОТА в Z[x]. . . . 37
5.15 Критерий Эйзенштейна. . . . 37
5.16 Свойства рациональных корней и значений в целых точках многочленов с целыми коэффициентами. . . . 37
5.17 Разностный многочлен. . . . 37

Глава 1

Основные понятия

1.1 Кольцо, поле, типы колец

Пусть K — множество, элементы которого мы будем называться числами. На множестве K определены две операции:

- $+\colon K + K \to K$
- $\cdot\colon K \cdot K \to K$

1. Ассоциативность сложения: $\forall a, b, c \in K\colon (a + b) + c = a + (b + c)$
2. Коммутативность сложения: $\forall a, b \in K\colon a + b = b + a$
3. Существования нуля (нейтрального элемента по сложению): $\forall a \in K\colon \exists 0 \in K + a = a$.
4. Существование обратного элемента по $+$: $\forall a \in K\colon \exists(-a) \in K\colon a + (-a) = 0$.
5. Дистрибутивность: $\forall a, b, c \in K\colon (a + b)c = ac + bc$ и $a(b + c) = ab + ac$.
6. Ассоциативность умножения: $\forall a, b, c \in K\colon (ab)c = a(bc)$.
7. Коммутативность умножения: $\forall a, b \in K\colon ab = ba$.
8. Существование единицы (нейтрального элемента по умножения) $\forall a \in K\colon \exists 1 \in K\colon a \cdot 1 = a$.
9. Существование обратного элемента по умножению: $\forall a \neq 0 \in K\colon \exists(a^{-1}) \in K\colon a \cdot (a^{-1}) = 1$

- 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

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

Свойство 1.0.1. *Ноль в кольце K единственен.*

Доказательство. Пусть в кольце K существует для нуля: 0_1, 0_2. Тогда:

$$0_1 = 0_1 + 0_2 = 0_2 + 0_1 = 0_2$$

□

Свойство 1.0.2. *Для любого $a \in K$ обратный элемент по $+$ единственен.*

Доказательство. Пусть есть два обратных элемента для $a \in K$: b_1 и b_2.

$$b_1 = b_1 + 0 = b_1 + (a + b_2) = (b_1 + a) + b_2 = 0 + b_2 = b_2$$

□

Свойство 1.0.3. $\forall a \in K\colon -(-a) = a$.

Доказательство.

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

□

Свойство 1.0.4. *В кольце не более одной единицы*

Доказательство. Пусть есть две единицы: $1_1, 1_2$.

$$1_1 = 1_1 \cdot 1_2 = 1_2$$

□

Определение 1.1. *Пусть K — кольцо с 1. Элемент $a \in K$ называется обратимым, если существует $a^{-1} \in K : a \cdot a^{-1} = 1$.*

Свойство 1.1.1. *Пусть K — кольцо с 1. Тогда для любого $a \in K$ существует не более одного обратного элемента по $\cdot$.*

Доказательство. Пусть есть два обратных элемента по $\cdot$: b_1 и b_2.

$$b_1 = b_1 \cdot 1 = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = 1 \cdot b_2 = b_2$$

□

Свойство 1.1.2. *Пусть K — кольцо с 1. Тогда $\forall a \in K : (a^{-1})^{-1} = a$*

Доказательство.

$$a = a \cdot 1 = a \cdot (a^{-1} \cdot (a^{-1})^{-1}) = (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = 1 \cdot (a^{-1})^{-1} = (a^{-1})^{-1}$$

□

Свойство 1.1.3.

$$-0 = 0$$

Доказательство. Очевидно следует из того, что $0 + 0 = 0$. □

Свойство 1.1.4. *Если K — кольцо с 1, то $1^{-1} = 1$.*

Доказательство. Следует из того, что $1 \cdot 1^{-1} = 1$. □

Определение 1.2. *Вычитание — прибавление обратного элемента по сложению:*

$$a - b \coloneqq a + (-b)$$

Деление (на обратимый элемент) — умножение на обратный элемент по сложению:

$$\frac{a}{b} \coloneqq a \cdot (b^{-1})$$

1.3 Подкольцо и подполе

Определение 1.3. *Пусть $K \subset L$, причем оба они — кольца с одними и теми же операциями $+$ и $\cdot$. Тогда K – подкольцо L, а L — надкольцо K.*

Пусть $K \subset L$, причем оба они — поля с одними и теми же операциями $+$ и $\cdot$. Тогда K – подполе L, а L — надполе K.

Лемма 1.1. *Пусть $K \subset L$, а L — кольцо, при этом выполнены следующие условия:*

- *Замкнутость K по умножению и сложению:*

$$\forall a, b \in K \colon a + b \in K$$

$$\forall a, b \in K \colon a \cdot b \in K$$

- *Существование обратного элемента по $+$*

$$\forall a \in K \colon \exists (-a) \in K \colon a + (-a) = 0$$

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

Доказательство. Условие 1 означает, что $+$ и $\cdot$ корректно определены в K. Ассоциативность и коммутативность $+$ и ассоциативность и коммутативность (если есть) $\cdot$ наследуются из L.

Рассмотрим $\forall a \in K$. Тогда $(-a) \in K$, и, по замкнутости операции $+$: $a + (-a) = 0 \in K$. Таким образом, в K существует 0. □

Лемма 1.2. *Пусть L — поле, $K \subset L$ и выполнены следующие условия:*

- *Замкнутость L по $+$ и $\cdot$.*
- *Существование обратного элемента по $+$*
- *Существование обратного элемента по $\cdot$.*

Тогда K — поле, а значит подполе L.

Доказательство. По Лемме 1.2, K — коммутативное подкольцо L.

Рассмотрим $\forall a \in K, a \neq 0$. Тогда $a^{-1} \in K$, причем K замкнуто по умножению, значит $a \cdot a^{-1} = 1 \in K$ □

1.4 Гомоморфизмы колец. Ядро и образ гомоморфизма

Определение 1.4. *Пусть K, L — кольца. Отображение $f \colon K \to L$ называется гомоморфизмом, если $\forall a, b \in K \colon f(a + b) = f(a) + f(b)$ и $f(ab) = f(a) \cdot f(b)$.*

Ядро гомоморфизма — это $\mathrm{Ker}(f) = \{x \in K \colon f(x) = 0\}$

Образ гомоморфизма — это $\mathrm{Im}(f) = \{y \in L : \exists x \in K \colon f(x) = y\}$

Свойство 1.4.1. *Если $f \colon K \to L$ — гомоморфизм, то $f(0_K) = 0_L$.*

Доказательство.

$$f(0_K) = f(0_K + 0_K) = f(0_K) + f(0_K)$$

$$f(0_K) = f(0_K) + f(0_K)$$

Вычтем из обеих частей $f(0_K)$ и получим:

$$f(0_K) - f(0_K) = f(0_K)$$

$$0_L = f(0_K)$$

□

Свойство 1.4.2. *Если $f \colon K \to L$ — гомоморфизм, то $f(-a) = -f(a)$.*

Доказательство.

$$0_L = f(0_K) = f(a + (-a)) = f(a) + f(-a)$$

$$0_L = f(a) + f(-a)$$

Вычтем из обеих частей $f(a)$ и получим:

$$0_L - f(a) = f(-a)$$

$$-f(a) = f(-a)$$

□

Лемма 1.3. *Пусть K, L — кольца, $f\colon K \to L$ — гомоморфизм колец. Тогда* $\mathrm{Ker}(f)$ *— подкольцо K,* $\mathrm{Im}(f)$ *— подкольцо L.*

Доказательство. Проверим условия из Леммы 1.2 Очевидно, что $\mathrm{Ker}(f) \subset K$. Пусть $a, b \in \mathrm{Ker}(f)$. Тогда $f(a) = f(b) = 0_L$. Значит $f(a+b) = f(a) + f(b) = 0_L + 0_L = 0_L$, следовательно, $f(a+b) \in \mathrm{Ker}(f)$, то есть $\mathrm{Ker}(f)$ замкнуто по $+$.

$f(ab) = f(a) \cdot f(b) = 0_L \cdot 0_L = 0_L$, значит $f(ab) \in \mathrm{Ker}(f)$, то есть $\mathrm{Ker}(f)$ замкнут опо $\cdot$.

$f(-a) = -f(a) = -0_L = 0_L$, значит $\forall a \in \mathrm{Ker}(f)\colon \exists(-a) \in \mathrm{Ker}(f)$.

Докажем для $\mathrm{Im}(f)$. Очевидно, что $\mathrm{Im}(f) \subset L$. Пусть $y, y' \in \mathrm{Im}(f)$, а x, x' таковы, что $f(x) = x$, $f(x') = y'$. Тогда $y + y' = f(x) + f(x') = f(x + x') \in \mathrm{Im}(f)$, то есть $\mathrm{Im}(f)$ замкнут по сложению.

$yy' = f(x)f(x') = f(xx') \in \mathrm{Im}(f)$, то есть $\mathrm{Im}(f)$ замкнут по умножению.

$-y = -f(x) = f(-x) \in Im(f)$ — существование обратного элемента по сложению □

1.5 Типы гомоморфизмов. Мономорфизм и ядро

Определение 1.5. *Пусть $f\colon K \to L$ — гомоморфизм колец. Если f — инъекция, то f — мономорфизм. Если f — сюръекция (т.е.* $\mathrm{Im}(f) = L$*), то f — эпиморфизм. Если f — биекция, то f — изоморфизм.*

Лемма 1.4. *Пусть $f\colon K \to L$ — гомоморфизм колец. Тогда f — мономорфизм, если и только если* $\mathrm{Ker}(f) = \{0\}$.

Доказательство. $\Rightarrow$: если f — мономорфизм, то f — инъекция. Пусть $a \in \mathrm{Ker}(f)$. Тогда, по свойству 1.4.1 $f(a) = 0 = f(0_K)$, откуда $a = 0$, так как f — инъекция.

$\Leftarrow$. Пусть $f(a) = f(b)$. Тогда $0 = f(a) - f(b) = f(a - b)$, откуда $a - b \in \mathrm{Ker}(f)$. Значит $a = b$, таким образом f — инъекция.

□

1.6 Отображение, обратное к изоморфизму — изоморфизм

Лемма 1.5. *Пусть $f\colon K \to L$ — изоморфизм колец. Тогда и $f^{-1}\colon L \to K$ — изоморфизм колец.*

Доказательство. Докажем, что f^{-1} — гомоморфизм.

Рассмотрим $\forall a, b \in L$. Пусть $w = f^{-1}(a+b) - f^{-1}(a) - f^{-1}(b)$. Так как f — гомоморфизм, то $f(w) = f(f^{-1}(a + b)) - f^{-1}(f(a) - f^{-1}(f(b))) = a + b - a - b = 0$ Так как $f(w) = 0_L = f(0_K)$ и того, что f — биекция следует, что $w = 0$. Значит $f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$.

Пусть $z = f^{-1}(ab) - f^{-1}(a)f^{-1}(b)$. Так как f — гомоморфизм, то $f(z) = f(f^{-1}(ab)) - f(f^{-1}(a))f(f^{-1}(b)) = ab - ab = 0$. Так как $f(z) = 0_L = f(0_K)$ и того, что f — биекция следует, что $z = 0$. Значит $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$. □

1.7 Изоморфные кольца

Определение 1.6. *Если существует изоморфизм $f\colon K \to L$, то говорят что кольца K и L изоморфны. Обозначение: $K \simeq L$.*

Теорема 1.1. *$\simeq$ — отношение эквивалентности на множестве всех колец.*

Доказательство. Необходимо доказать три свойства:

- Рефлексивность: $K \simeq K$
- Симметричность: $K \simeq L \Rightarrow L \simeq K$.
- Транзитивность: $K \simeq L \wedge L \simeq M \Rightarrow K \simeq M$.

Рефлексивность очевидна: тождественное отображение $id\colon K \to K$ заданное формулой $id(x) = x$ для всех $x \in K$ очевидно является изоморфизмом.

Симметричность следует из леммы 1.5: если $K \simeq L$, то существует отображение $f\colon K \to L$, а значит и $f^{-1}\colon L \to K$ — изоморфизм, то есть $L \simeq K$.

Докажем транзитивность. Пусть K, L, M — кольца, $K \simeq L$ и $L \simeq M$. Тогда существуют изоморфизмы $f\colon K \to L$ и $g\colon L \to M$. Докажем, что их композиция $g \circ f\colon K \to M$ (заданная формулой $g \circ f = g(f(a))$) также является изоморфизмом.

Композиция биекций, очевидно, является биекцией. Проверим, что $g \circ f$ — гомоморфизм колец.

$$g \circ f(a+b) = g(f(a+b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = g \circ f(a) + g \circ f(b)$$

$$g \circ f(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = g \circ f(a) \cdot g \circ f(b)$$

□

1.8 Идеал. Ядро гомоморфизма является идеалом

Определение 1.7. *Пусть K — коммутативное кольцо. Множество $I \subset K$ — идеал в K если I — подкольцо K и выполнено следующее условие:*

$$\forall x \in K \quad \forall a \in I \qquad ax \in I$$

В любом кольце K есть два «неинтересных» идеала: $\{0\}$ и K.

Лемма 1.6. *Пусть K — коммутативное кольцо, $I \subset K$. Пусть выполнены следующие условия:*

- *Замкнутость по $+$:* $\forall a, b \in I \quad a + b \in I$
- *Существование обратного элемента по $+$:* $\forall a \in I \qquad \exists(-a) \in I$
- *Замкнутость по $\cdot$ на элементы K:* $\forall x \in K \quad \forall a \in I \qquad ax \in I$.

Тогда I — идеал в K.

Доказательство. По Лемме 1.2 I — подкольцо K.

Тогда по условию 3 очевидно, что I — идеал в K. □

Лемма 1.7 (Лемма о ядре гомоморфизма)**.** *Пусть K — коммутативное кольцо, $\varphi\colon K \to L$ — гомоморфизм колец. Тогда* $\mathrm{Ker}(\varphi)$ *— идеал в K.*

Доказательство. По Лемме 1.3 $\mathrm{Ker}(\varphi)$ — подкольцо K. Проверим замкнутость по умножению на элементы K. Пусть $a \in \mathrm{Ker}(\varphi)$ и $x \in K$.

Тогда $f(ax) = f(a)f(x) = f(x) \cdot 0 = 0$. Значит $ax \in \mathrm{Ker}(\varphi)$. Таким образом $\mathrm{Ker}(\varphi)$ — идеал в K. □

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

Лемма 1.8. *Пусть K — коммутативное кольцо с 1. I — идеал в K, при этом $\exists x \in I$ — обратимый элемент кольца K. Тогда $I = K$.*

Доказательство. Так как $x^{-1} \in K$ и $x \in I$, мы имеем $1 = x \cdot x^{-1} \in I$ (по определению идеала).
$\forall y \in K\ y = y \cdot 1 \in I$, значит $I = K$. □

Следствие 1.1.1. *Пусть K — поле, а I — идеал в K. Тогда $I = K$ или $I = \{0\}$*

Доказательство. Предположим, что $I \neq \{0\}$. Тогда $\exists x \in I, x \neq 0$. Так как все ненулевые элементы поля обратимы, то x тоже. Значит, по Лемме 1.8 $I = K$ □

Следствие 1.1.2. *Пусть K — поле, L — кольцо, а $f\colon K \to L$ — гомоморфизм колец. Тогда либо $\mathrm{Im}(f) = \{0\}$, либо f — мономорфизм.*

Доказательство. По Лемме 1.7 $\mathrm{Ker}(f)$ — идеал в K. Значит по следствию 1.1.1 либо $\mathrm{Ker}(f) = K$ и тогда $\mathrm{Im}(f) = \{0\}$, либо $\mathrm{Ker}(f) = \{0\}$ и тогда f — гомоморфизм по Лемме 1.4. □

1.10 Идеал, порожденный множеством элементов. Главный идеал

Определение 1.8 (Идеал, порожденный множеством)**.** *Пусть K — коммутативное кольцо, $M \subset K$. Тогда*

$$\langle M \rangle \coloneqq \{m_1 x_1 + \cdots + m_s x_s \colon m_1, \ldots, m_s \in M, x_1, \ldots, x_s \in K\}$$

— идеал, порожденный множеством K. Идеал, порожденный множеством M — множество всех линейных комбинаций элементов M.

В Лемме 1.9 доказано, что $\langle M \rangle$ — действительно идеал.

Определение 1.9. *Пусть K — коммутативное кольцо, $m \in K$.*
Тогда $mK = \{mx \colon x \in K\}$ — главный идеал.
Если все идеалы в кольце K — главные, то K — кольцо главных идеалов.

Лемма 1.9. *Пусть K — кольцо, $M \subset K$. Тогда $\langle M \rangle$ — идеал в K.*

Доказательство. Проверим условия из Леммы 1.6.
Пусть $a, b \in \langle M \rangle$. Тогда $a = a_1 m_1 + \cdots + a_s m_s$ и $b = b_1 m_1 + \cdots b_s m_s$, где $m_1, \ldots, m_s \in M$, $a_1, \ldots, a_s, b_1, \ldots, b_s \in K$. (можно считать, что a и b — линейные комбинации одних и тех же элементов, при необходимости добавить слагаемые с нулевыми коэффициентами)
Обратный элемент: $-a = (-a_1)m_1 + \cdots + (-a_s)m_s \in \langle M \rangle$, так как $(-a_1), \ldots - (a_s) \in K$.
Замкнутость по сложению: $a + b = (a_1 + b_1)m_1 \cdots + (a_s + b_s)m_s \in \langle M \rangle$, так как K замкнут по сумме.
Замкнутость по умножению на элементы из K: $\forall x \in K, ax = (a_1 x)m_1 + \cdots + (a_s x)m_s \in \langle M \rangle$, так как $a_i x \in K$.
Все условия из Леммы 1.6 проверены, значит $\langle M \rangle$ — идеал в K. □

1.11 Сравнения по модулю идеала. Вычеты

Определение 1.10. *Пусть K — коммутативное кольцо, I — идеал в K, $a, b \in K$.*
Тогда $a \equiv_I b \Leftrightarrow a - b \in I$

Лемма 1.10. *$\equiv_I$ — отношение эквивалентности.*

Доказательство. Рефлексивность: $a \equiv_I a$ так как $a - a = 0 \in I$.
Симметричность: $a \equiv_I b \Rightarrow a - b \in I \Rightarrow -(a - b) = b - a \in I \Rightarrow b \equiv_I a$
Транзитивность: если $a \equiv_I b$ и $b \equiv_I c$, то $a - b \in I$ и $b - c \in I$. Тогда $a - c = (a - b) + (b - c) \in I \Leftrightarrow a \equiv_I c$.
□

Определение 1.11. *Вычет по модулю идеала I — класс эквивалентности по отношению эквивалентности $\equiv_I$.*
Различные вычеты не пересекаются. Кольцо K разбито на классы эквивалентности (вычеты).

1.12 Факторкольцо

Для $a \in K$ вычет, состоящий из всех элементов, сравнимых с a будем обозначать как $\overline{a} = a + I = \{a + x \colon x \in I\}$.

Определение 1.12. *Пусть K — коммутативное кольцо, I — идеал в K. Факторкольцо* ${}^{K}\!/_{I} \coloneqq \{\overline{a} \colon a \in K\}$
$\overline{a} + \overline{b} = \overline{a + b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Лемма 1.11. *$+$ и $\cdot$ в ${}^{K}\!/_{I}$ определены корректно.*

Доказательство. Пусть $a \equiv_I a'$, а значит и $\overline{a} = \overline{a'}$ (так как вычет у них общий). Это означает, что $a - a' \in I$. Проверим, что мы можем заменить a на a' если $a = a'$. То есть $\overline{a} + \overline{b} = \overline{a'} + \overline{b}$ и $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b}$

$$\overline{a} + \overline{b} = \overline{a'} + \overline{b} \Leftrightarrow a + b \equiv_I a' + b \Leftrightarrow a + b - (a' + b) = a + b - a' - b = a - a' \in I$$

$$\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b} \Leftrightarrow ab \equiv_I a'b \Leftrightarrow ab - a'b = b(a - a') \in I \Leftarrow a - a' \in I$$

□

Теорема 1.2. *${}^{K}\!/_{I}$ с определенными выше операциями $+$ и $\cdot$ — коммутативное кольцо.*
Если K — кольцо с 1, то ${}^{K}\!/_{I}$ — тоже. Если при этом $a \in K$ — обратимый элемент, то $\overline{a}$ — обратимый в ${}^{K}\!/_{I}$.

Доказательство. Так как $\overline{a} + \overline{b} = \overline{a + b}$ и $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, из ассоциативности и коммутативности $+$ и $\cdot$ в K следует ассоциативность и коммутативность $+$ и $\cdot$ в ${}^{K}\!/_{I}$.
Дистрибутивность: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$
Ноль — это $\overline{0}$.
Обратный по сложению: $-\overline{a} \coloneqq \overline{-a}$.
Единица: если $1 \in K$, то $\overline{1}$ — единица в ${}^{K}\!/_{I}$.
Если $a \in K$ — обратимый, то $(\overline{a})^{-1} \coloneqq \overline{a^{-1}}$ — обратимый в ${}^{K}\!/_{I}$.

□

1.13 Теорема о гомоморфизме колец

Теорема 1.3 (Теорема о гомоморфизме колец)**.** *Пусть K, L — коммутативные кольца. $f \colon K \to L$ — гомоморфизм колец. Тогда ${}^{K}\!/_{\mathrm{Ker}(f)} \simeq \mathrm{Im}(f)$.*

Более того, отображение $\overline{f} \colon {}^{K}\!/_{\mathrm{Ker}(f)} \to \mathrm{Im}(f)$ заданное формулой $\overline{f}(\overline{x}) \coloneqq f(x)$ является изоморфизмом колец.

Доказательство. Докажем корректность определения $\overline{f}$. Пусть $\overline{x} = \overline{y}$, а значит и $x \equiv_{\mathrm{Ker}(f)} y$, то есть $x - y \in \mathrm{Ker}(f)$, а значит

$$f(x) = f(x) + f(y) - f(y) = f(y) + f(x - y) = f(y) + 0 = f(y)$$

$f(x - y) = 0$ так как $x - y \in \mathrm{Ker}(f)$.
Покажем, что $\overline{f}$ — гомоморфизм:

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y})$$

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(x \cdot y) = f(x) \cdot f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$$

Покажем, что $\overline{f}$ — сюръекция: $\forall y \in \mathrm{Im}\, f \colon \exists y \in K \colon y = f(x)$. Тогда и $y = \overline{f}(\overline{x})$.
Пусть $\overline{a} \in \mathrm{Ker}(\overline{f})$. Тогда $0 = \overline{f}(\overline{a}) = f(a)$ (избавляемся от черты по определению $\overline{f}$). Значит $a \in \mathrm{Ker}(f)$, откуда следует, что $\overline{a} = \overline{0}$, то есть $\mathrm{Ker}(\overline{f}) = \{\overline{0}\}$, а отсюда по Лемме 1.4 следует, что f — инъекция.
Таким образом, f — изоморфизм, а значит ${}^{K}\!/_{\mathrm{Ker}\, f} \simeq \mathrm{Im}(f)$

□

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

Определение 1.13. *Пусть K — коммутативное кольцо без делителей нуля (то есть если $ab \in K, ab = 0$, то $(a = 0) \vee (b = 0)$).*
Обозначим через M множество всех дробей $\frac{a}{b}$, где $a, b \in K$, $b \neq 0$.
Пусть $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$

Свойство 1.13.1.

$$\frac{0}{b} \sim \frac{c}{d} \Leftrightarrow c = 0$$

Доказательство. $\Leftarrow$: Если $c = 0$, то $0 \cdot d = 0 = b \cdot 0$.
$\Rightarrow$: $\frac{0}{b} \sim \frac{c}{d} \Rightarrow 0 = 0 \cdot d = bc$. Так как в K нет делителей нуля, а $b \neq 0$ по определнию, то $c = 0$. □

Свойство 1.13.2.

$$\frac{a}{a} \sim \frac{c}{d} \Leftrightarrow c = d$$

Доказательство. $ad = ac \Leftrightarrow ad - ac = 0 \Leftrightarrow a(d-c) = 0$, где $a \neq 0$ по определению, значит $d - c = 0 \Leftrightarrow c = d$ □

Свойство 1.13.3 (Сокращение дроби)**.**

$$\frac{a}{b} \sim \frac{ac}{bc}$$

Доказательство. $abc = acb$ □

Лемма 1.12. $\sim$ *— отношение эквивалентности*

Доказательство. Рефлексивность очевидна: $\frac{a}{b} \sim \frac{a}{b} \Leftrightarrow ab = ab$

Симметричность: $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow \frac{c}{d} \sim \frac{a}{b}$

Транзитивность: $\frac{a}{b} \sim \frac{c}{d}$, $\frac{c}{d} \sim \frac{e}{f}$. Значит $ad = bc$, $cf = de$. Перемножим полученные равенства и разделим на cd:

$$adcf = bcde \Rightarrow af = be \Leftrightarrow \frac{a}{b} \sim \frac{e}{f}$$

□

1.15 Поле частных

Определение 1.14. *Поле частных F коммутативного кольца K без делителей нуля состоит из классов эквивалентности дробей.*

Обозначим за $\frac{a}{b}$ как класс эквивалентности этой дроби, так и саму дробь.

$$\frac{a}{b} + \frac{c}{d} \coloneqq \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} \coloneqq \frac{ac}{bd}$$

Лемма 1.13. *Сложение и умножение в поле частных определены корректно, то есть, результат не зависит от замены дроби на эквивалентную.*

Доказательство. Достаточно доказать, что при замене дроби $\frac{a}{b}$ на $\frac{a'}{b'} \sim \frac{a}{b}$ результат не изменится. Заметим, что $ab' = a'b$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \sim \frac{a'd + b'c}{b'd} = \frac{a'}{b'} + \frac{c}{d} \Leftrightarrow$$
$$(ad + bc)b'd = (a'd + b'c)bd \Leftrightarrow ab'd^2 + bb'cd = a'bd^2 + bb'cd \Leftrightarrow$$
$$ab'd^2 = a'bd^2 \Leftrightarrow ab' = a'b$$

Умножение: если $c = 0$, утверждение верно из Свойства 1.13.1. Иначе можно сокращать на cd, так как $d \neq 0$ по определению.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \sim \frac{a'c}{b'd} = \frac{a'}{b'} \cdot \frac{c}{d} \Leftrightarrow ab'cd = a'bcd \Leftrightarrow ab' = a'b$$

□

Теорема 1.4. *Поле частных F коммутативного кольца K — действительно поле.*

Доказательство. Коммутативность сложения и умножения следуют из аналогичных свойств в кольце K.

Ассоцитивность сложения:

$$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$

Очевидно, что при другом порядке дробей будет то же самое.

Ноль: дроби вида $\frac{0}{b}, b \in K, b \neq 0$ образуют класс эквивалентности по свойству 1.13.1. Легко проверить, что этот класс и будет нейтральным по сложению: $\frac{0}{b} + \frac{c}{d} = \frac{0 \cdot d + bc}{bd} = \frac{c}{d}$

Обратный элемент по $+$: положим $-(\frac{a}{b}) \coloneqq \frac{-a}{b}$

Ассоцитивность и дистрибутивность умножения легко доказываются.

Единица: дроби вида $\frac{a}{a}, a \in K, a \neq 0$

Обратный элемент по умножению: $(\frac{a}{b})^{-1} \coloneqq \frac{b}{a}$ □

1.16 Вложение кольца в поле частных

Лемма 1.14. *Пусть K — коммутативное кольцо с 1 без делителей 0, а F — его поле частных. Тогда отображение $\varphi\colon K \to F$, заданное формулой $\varphi(a) = \frac{a}{1}$ — мономорфизм колец. (т.е. инъекция)*

Доказательство. Проверим, что φ — гомоморфизм колец. Пусть $a, b \in K$.

$$\varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = \varphi(a+b)$$

$$\varphi(a) \cdot \varphi(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = \varphi(ab)$$

Пусть $a \in \mathrm{Ker}(f)$. Тогда $0 = \varphi(a) = \frac{a}{1} \Leftrightarrow a = 0$. Тогда $\mathrm{Ker}(f) = \{0\}$, и по Лемме 1.4 f — мономорфизм. □

Таким образом, $K \subset F$. Будем отождествлять $a \in K$ с дробью $\frac{a}{1} \in F$

1.17 Характеристика поля

Определение 1.15. *Пусть K — поле. Положим $\underline{k} \coloneqq \underbrace{1 + \cdots + 1}_{k}$ для $k \in \mathbb{N}$ и $\underline{k} \coloneqq \underbrace{1 + \cdots + 1}_{-k}$ для отрицательных $k \in \mathbb{Z}$, а также $\underline{0} = 0$.*

Если существуют такие $k \in \mathbb{N}$, что $\underline{k} = 0$, то характеристика поля $\mathrm{char}(K)$ равна наименьшему из таких чисел. Если таких чисел нет, то положим $\mathrm{char}(K) = 0$.

Несложно проверить, что $\underline{a+b} = \underline{a} + \underline{b}$ и, раскрыв по дистрибутивности, $\underline{a \dots b} = \underline{a} \dots \underline{b}$

Лемма 1.15. *Пусть K — поле, $\mathrm{char}(K) = p \neq 0$. Тогда $p \in \mathbb{P}$.*

Доказательство. Предположим обратное. Пускай $p \notin \mathbb{P}$, значит $p = ab$, где $1 < a, b < p$.

Тогда $\underline{a} \cdot \underline{b} = \underline{ab} = \underline{p} = 0$. Значит одно из чисел $\underline{a}$ и $\underline{b}$ равно нулю, что противоречит минимальности p в определении характеристики поля. □

1.18 Теорема о подполе

Теорема 1.5. *Пусть K — поле.*

1. *Если* $\mathrm{char}(K) = p \in \mathbb{P}$, *то отображение* $\varphi\colon {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, *заданное формулой* $\varphi(\overline{m}) = \underline{m}$ *(для* $m \in \mathbb{Z}$*) — мономорфизм полей. В частности,* K *имеет подполе* ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

2. *Если* $\mathrm{char}(K) = 0$, *то отображение* $\varphi\colon \mathbb{Q} \to K$, *заданное формулой* $\varphi(\frac{a}{b}) = \left(\frac{(a)}{(b)}\right)$ *(для* $a, b \in \mathbb{Z}, b \neq 0$*) — мономорфизм полей. В частности,* K *имеет подполе* $\mathbb{Q}$.

Доказательство. 1. Отображение $\psi\colon \mathbb{Z} \to K$ заданное формулой $\psi(m) := \underline{m}$ очевидно является гомоморфизмом колец.

$\mathrm{Ker}(\psi) = \{m \in \mathbb{Z}\colon \underline{m} = 0\}$ — идеал в $\mathbb{Z}$ по лемме 1.7. Так как $\mathbb{Z}$ — кольцо главных идеалов, то пусть $\mathrm{Ker}(\psi) = q\mathbb{Z}$. Тогда $\underline{m} = 0 \iff m \vdots q$, то есть $\mathrm{char}(K) = q$. Значит $q = p$ и $\mathrm{Ker}(\psi) = p\mathbb{Z}$.

По теореме 1.3 отображение $\bar{\psi}\colon {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \to \mathrm{Im}(\psi) \subset K$, заданное формулой $\bar{\psi}(\bar{m}) = \underline{m}$ — изоморфизм колец между ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ и $\mathrm{Im}(\psi)$.

2. В этом случае $\forall m \in \mathbb{N} \underline{m} \neq 0$, то есть $\mathrm{char}(K) = 0$. Определим отображение $\varphi\colon \mathbb{Q} \to K$ формулой $\varphi(\frac{a}{b}) = \frac{(a)}{(b)}$, $\underline{b} \neq 0$

Проверим корректность: пусть $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$ ($b, d \neq 0$ по определению поля частных). Тогда по дистрибутивности поля K имеем: $\underline{a} \cdot \underline{d} = \underline{b} \cdot \underline{c} \iff \frac{(a)}{(b)} \sim \frac{(c)}{(d)}$.

Проверим, что φ — гомоморфизм.

$$\varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right) = \frac{\underline{a}}{\underline{b}} + \frac{\underline{c}}{\underline{d}} = \frac{\underline{ad} + \underline{bc}}{\underline{cd}} = \varphi\left(\frac{ad + bc}{bd}\right) = \varphi\left(\frac{a}{b} + \frac{c}{d}\right)$$

$$\varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \frac{\underline{a}}{\underline{b}} \cdot \frac{\underline{c}}{\underline{d}} = \frac{\underline{ac}}{\underline{bd}} = \varphi\left(\frac{ac}{bd}\right) = \varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right)$$

Так как $\mathbb{Q}$ — поле и φ принимает не только нулевые значения (т.е. $\mathrm{Im}(\varphi) \neq \{0\}$), то по Следствию 1.1.2 $\mathrm{Ker}(\varphi) = \{0\}$, а из этого по Лемме 1.4 следует, что φ — мономорфизм, а $\mathrm{Im}(\varphi) \subset K$ — поле, изоморфное $\mathbb{Q}$. $\square$

Глава 2

Комплексные числ

2.1 Вещественная и мнимая часть, умножение, сложением, норма, модуль

Определение 2.1. *Множество комплексных чисел состоит из упорядоченных пар вещественных чисел*

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$$

Пусть $z = (a, b) \in \mathbb{C}$.

- *Сложение:* $(a, b) + (c, d) = (a + b, c + d)$
- *Умножение:* $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$
- *Вещественная часть:* $\mathrm{Re}(z) \coloneqq a$.
- *Мнимая часть:* $\mathrm{Im}(z) \coloneqq b$.
- *Комплексное сопряжение:* $\bar{z} \coloneqq (a, -b)$.
- *Норма* z*:* $N(z) \coloneqq a^2 + b^2$.
- *Модуль* z*:* $|z| \coloneqq \sqrt{N(z)} = \sqrt{a^2 + b^2}$

2.2 Поле комплексных чисел

Теорема 2.1 (Теорема 1)**.** $\mathbb{C}$ *— поле*

Доказательство. Ассоциативность и коммутативность сложения наследуется из $\mathbb{R}$.
Ноль в $\mathbb{C}$ это $0 \coloneqq (0, 0)$.
Обратный элемент по сложению: $z = (a, b)$, $-z \coloneqq (-a, -b)$.
Коммутативность умножения: $(a, b) \cdot (a', b') = (aa' - bb', ab' + ba') = (a'a - b'b, a'b + b'a) = (a'b') \cdot (a, b)$
Так как умножение коммутативно, достаточно проверить лишь одну дистрибутивность:

$$(a, b) \cdot ((c_1, d_1) + (c_2, d_2)) = (a, b) \cdot (c_1 + c_2, d_1 + d_2) = (ac_1 + ac_2 - bd_1 - bd_2, ad_1 + ad_2 + bc_1 + bc_2) =$$

$$(ac_1 - bd_1, ad_1 + bc_1) + (ac_2 - bd_2, ad_2 + bc_2) = (a, b) \cdot (c_1, d_1) + (a, b) \cdot (c_2, d_2)$$

Ассоциативность умножения:

$$((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2) \cdot (a_3, b_3) =$$

$$(a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - b_1a_2b_3, a_1b_2a_3 + b_1a_2a_3 + a_1a_2b_3 - b_1b_2b_3)$$

Нетрудно проверить, что при другом порядке получится то же самое.
Единица: $1 \coloneqq (1, 0)$.
Обратный элемент по умножению: для $z = (a, b)$ положим $z^{-1} = \left(\frac{a}{N(z)}, \frac{-b}{N(z)}\right)$ Проверяем:

$$zz^{-1} = (a, b) \cdot \left(\frac{a}{N(z)}, \frac{-b}{N(z)}\right) = \left(\frac{a^2 + b^2}{N(z)}, \frac{-ab + ba}{N(z)}\right) = (1, 0)$$

□

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

Определение 2.2. *Рассмотрим декартову систему координат в $\mathbb{R}^2$. По оси абсцисс будем откладывать вещественную часть, а по оси ординат — мнимую. Тогда комплексное сопряжение — симметрия относительно оси абсцисс.*

Для числа $z = (a, b) \in \mathbb{C}$ тогда $r = |z| = \sqrt{a^2 + b^2}$ — расстояние от начала координат до z.

Аргумент z — это направленный угол $\arg(z) = \varphi$ от оси абсцисс до луча Oz против часовой стрелки. Вычисляется с точностью до $2\pi k, k \in \mathbb{Z}$.

Пара (r, φ) однозначно задает точку z.

$a = r\cos(\varphi), b = r\sin(\varphi)$.

Тригонометрическая форма записи: $z = (r\cos(\varphi), r\sin(\varphi))$.

Теорема 2.2 (Теорема 2)**.** *Пусть $x, y \in \mathbb{C}$. Тогда $|xy| = |x||y|$ и $\arg(xy) = \arg(x) + \arg(y)$.*

Доказательство. Пусть $x = (r\cos(\varphi), r\sin(\varphi))$, $y = (p\cos(\psi), p\sin(\psi))$.

Тогда:

$$xy = (rp(\cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)), rp(\cos(\varphi)\sin(\psi) + \sin(\varphi)\cos(\psi))) = (rp\cos(\varphi + \psi), rp\sin(\varphi + \psi))$$

Переход совершен по формулам:

$$\cos(\alpha + \beta) = \cos(\alpha) \cdot \cos(\beta) - \sin(\alpha) \cdot \sin(\beta)$$

$$\sin(\alpha + \beta) = \sin(\alpha) \cdot \cos(\beta) + \cos(\alpha) \cdot \sin(\beta)$$

□

Теорема 2.3 (Формула Муавра, Теорема 3)**.** *Пусть $z \in \mathbb{C}, n \in \mathbb{N}$. Тогда $|z^n| = |z|^n$, $\arg(z^n) = n \cdot \arg(z)$.*

Доказательство. Индукция по n. База $n = 1$ очевидна.

Переход $n \to n + 1$.

Пусть $|z| = r$, $\arg(z) = \varphi$ и утверждение доказано для n, то есть $|z^n| = |z|^n = r^n$, $\arg(z^n) = n \cdot \arg(z) = n\varphi$. Необходимо доказать для $n + 1$.

По теореме 2.2 $|z^{n+1}| = |z^n \cdot z| = |z^n| \cdot |z| = r^{n+1}$ и $\arg(z^{n+1}) = \arg(z^n \cdot z) = \arg(z^n) + \arg(z) = n\varphi + \varphi = \varphi(n + 1)$. □

2.4 Вложение вещественных чисел в комплексные

Лемма 2.1 (Лемма 1)**.** *Отображение $f\colon \mathbb{R} \to \mathbb{C}$, заданное формулой $f(a) = (a, 0)$ — мономорфизм.*

Доказательство. Очевидно, f — инъекция.

Проверим, что f — гомоморфизм. Пусть $a, b \in \mathbb{R}$.

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

$$f(a) \cdot f(b) = (a, 0) \cdot (b, 0) = (ab, 0) = f(a \cdot b)$$

Таким образом $\mathbb{C}$ имеет подполе $\mathrm{Im}(f)$, изоморфное $\mathbb{R}$. □

2.5 Извлечение корня из комплексного числа. Корни из 1

Пусть $a \in \mathbb{C}$, $n \in \mathbb{N}$, $a \neq 0$. Решим уравнение $z^n = a$. Представим комплексные числа в тригонометрической форме. $a = (r, \varphi)$ — эти числа даны, $z = (p, \psi)$ — эти числа мы ищем.

По формуле Муавра, $p = \sqrt[n]{r}$, а $n\psi = \varphi + 2\pi k$. Разделим на n и получим: $\psi = \frac{\varphi}{n} + \frac{2\pi k}{n}$

Это уравнение дает k различных решений при $k \in \{0, \ldots, n - 1\}$. Каждое число $k \in \mathbb{Z}$ можно представить в виде $k = qn + r, 0 \leq r < n$ (теорема о делении с остатком). Тогда $\frac{2\pi k}{n} = 2\pi q + \frac{2\pi r}{n}$, а это тот же аргумент, что и $\frac{2\pi r}{n}$.

Таким образом, корень n степени извлекается ровно n способами.

Глава 3

Целые числа

3.1 Делимость. Свойства. Теорема о делении с остатком

Определение 3.1. *Пусть $a, b \in \mathbb{Z}, b \neq 0$. Тогда a делится на b ($a \vdots b$) или b делит a ($b \mid a$), если $\exists c \in \mathbb{Z}\colon a = bc$.*

Свойство 3.1.1 (Свойство 1)**.** *Если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.*

Доказательство. $a = kb, b = nc \Rightarrow a = knc, kn \in \mathbb{Z}$ □

Свойство 3.1.2 (Свойство 2)**.** *Пусть $a, b \vdots d$, $x, y \in \mathbb{Z}$. Тогда $ax + by \vdots c$.*

Доказательство. $a = kd, b = nd$, $ax + by = dkx + dny = d(kx + ny) \vdots d$. □

Свойство 3.1.3 (Свойство 3)**.** *Пусть $a, d \in \mathbb{N}, a \vdots d$. Тогда $a \geqslant d$.*

Доказательство. $a = kd, k \in \mathbb{N} \Rightarrow a = kd \geqslant d$. □

Теорема 3.1 (Теорема о делении с остатком)**.** *Пусть $a \in \mathbb{Z}, b \in \mathbb{N}$. Тогда существуют такие единственные числа $q, r \in \mathbb{Z}\colon 0 \leqslant r < b$ и $a = bq + r$.*

Доказательство. Докажем существование. Всегда существует такой q, что $bq \leqslant a < b(q+1)$. Возьмем $r = a - bq$. Вычтем из обеих частей неравенства bq.

$$bq \leqslant a < bq + b$$

$$0 \leqslant a - bq < b$$

$$0 \leqslant r < b$$

Докажем единственность. Пусть $a = bq_1 + r_1 = bq_2 + r_2$, причем $0 \leqslant r_1, r_2 < b$.

Не умоляя общности, пусть $r_1 > r_2$. Тогда $0 < r_1 - r_2 < b$. С другой стороны, $r_1 - r_2 = a - bq_1 - (a - bq_2) = a - bq_1 - a + bq_2 = b(q_2 - q_1)$, при этом $r_1 - r_2 > 0$, а значит и $q_2 - q_1 > 0 \Rightarrow q_2 - q_1 \in \mathbb{N}$. Тогда $b(q_2 - q_1) \geqslant b$, получаем противоречие.

□

3.2 НОД. Свойства

Определение 3.2. *Пусть* $a_1, \ldots, a_n \in \mathbb{Z}$. *Обозначим через* $\mathrm{OD}(a_1, \ldots, a_n)$ *множество всех общих делителей этих чисел, а через* $(a_1, \ldots, a_n)$ *— их НОД.*

Свойство 3.2.1. *Если* $b \in \mathbb{N}, a \vdots b$, *то* $\mathrm{OD}(a, b)$ *— это все делители* b *и* $(a, b) = b$.

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

Если d — любой делитель b, то $a \vdots d$ по Свойтсву 3.1.1, а значит d — общий делитель a и b.
Понятно, что наибольший делитель среди чисел (a, b) это и будет сам b. □

Свойство 3.2.2. *Пусть* $a, b, k \in \mathbb{Z}$. *Тогда* $\mathrm{OD}(a, b) = \mathrm{OD}(a + kb, b)$, *а значит и* $(a, b) = (a + kb, b)$

Доказательство. Пусть $d \in \mathrm{OD}(a, b)$. Тогда $a + kb \vdots d$ (по свойству 3.1.2). Значит $d \in \mathrm{OD}(a + kb, b)$.

Пусть $d \in \mathrm{OD}(a + kb, b)$. Тогда $a = (a + kb) - kb \vdots d$ (по свойству 3.1.2), значит $d \in \mathrm{OD}(a, b)$. □

3.3 Алгоритм Евклида. Следствия из алгоритма Евклида

Пусть $a, b \in \mathbb{N}, a > n$. Каждая строка алгоритма — деление с остатком.

1. $a = bq_1 + r_1 \quad 0 \leqslant r_1 < b$
2. $b = r_1 q_2 + r_2 \quad 0 \leqslant r_2 < r_1$
   $\vdots$
3. $r_{n-2} = r_{n-1} q_n + r_n \quad 0 \leqslant r_n < r_{n-1}$
4. $r_{n-1} = r_n q_{n+1}$

Так как $b > r_1 > r_2 > \ldots$ и все эти числа неотрицательны, алгоритм обязательно закончит работу.

Теорема 3.2. $(a, b) = r_n$, $\mathrm{OD}(a, b)$ *— это все делители* (a, b).

Доказательство. По свойству 3.2.2 $\mathrm{OD}(a, b) = \mathrm{OD}(a, b_1) = \mathrm{OD}(b_1, r_1) = \mathrm{OD}(r_1, r_2) = \cdots = \mathrm{OD}(r_{n-1}, r_n)$, а это по свойству 3.2.1 — все делители r_n. Тогда (a, b) — наибольший из делителей r_n, то есть сам r_n. □

Теорема 3.3. *Пусть* $a, b, m \in \mathbb{N}$. *Тогда:*

1. $(am, bm) = m(a, b)$
2. *Если* $d \in \mathrm{OD}(a, b)$, *то* $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$

Доказательство. НУО $a > b$.

1. Рассмотрим первую строку алгоритма Евклида для am и bm:

$$am = bm \cdot q_1 + r_1 m, \quad 0 \leqslant r_1 m < bm$$

Неполное частное не меняется, а остаток умножается на m. Очевидно, что с остальными строками будет также, и в итоге получится $r_n m = m(a, b)$

2. Рассмотрим первую строку алгоритма Евклида для $\frac{a}{d}$ и $\frac{b}{d}$.

$$\frac{a}{d} = \frac{b}{d} \cdot q_1 + \frac{r_1}{d}, \quad 0 \leqslant \frac{r_1}{d} < b$$

Неполное частное не меняется, а остаток делится на m. Очевидно, что с остальными строками будет также, и в итоге получится $\frac{r_n}{d} = \frac{(a,b)}{d}$

□

3.4 Линейное представление НОД

Теорема 3.4. *Пусть $a, b \in \mathbb{Z}$. Тогда существуют такие $x, y \in \mathbb{Z}$, что $(a, b) = ax + by$.*

Доказательство. Так как делители a, b одни и те же, то $(a, b) = (a, -b)$. Поэтому можно считать, что $a, b \in \mathbb{N}$.

Не умоляя общности, пусть $a \geqslant b$. Воспользуемся алгоритмом Евклида и соответствующими обозначениями. Дополним их: $r_0 = b, r{-}1 = a$.

По индукции обратным ходом докажем, что существует представление $(a, b) = x_k r_k + y_k y k - 1$. При $k = 0$ получим утверждение теоремы.

База $k = n$ очевидна: $(a, b) = 1 \cdot r_n + 0 \cdot r_{n-1}$.

Переход $k \to k - 1$. Из алгоритма Евклида мы знаем: $r_k = r_{k-2} - r_{k-1} q_k$. Подставим:

$$(a, b) = x_k(r_{k-2} - r_{k-1} q_k) + y_k r_{k-1} = (-x_k q_k + y_k) r_{k-1} + x_k r_{k-2}$$

□

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

Теорема 3.5. *Пусть $n \geqslant 2$, $a_1, \ldots, a_n \in \mathbb{Z}$. Положим $m_2 = (a_1, a_2), m_3 = (m_2, a_3), \ldots, m_n = (m_{n-1}, a_n)$.*

Тогда $m_n = (a_1, \ldots, a_n)$, а $\mathrm{OD}(a_1, \ldots, a_n)$ — все делители m_n.

Доказательство. Индукцией по k докажем, что $\mathrm{OD}(a_1, \ldots, a_k)$ — все делители m_k. База $k = 2$ доказана в Теореме 3.2.

Переход: $OD(a_1, \ldots, a_k, a_{k+1})$ — все числа из $\mathrm{OD}(a_1, \ldots, a_k)$, являющиеся делителями a_{k+1}.

Так как $\mathrm{OD}(a_1, \ldots, a_k)$ это все делители m_k, получаем, что $\mathrm{OD}(a_1, \ldots, a_k, a_{k+1}) = \mathrm{OD}(m_k, a_{k+1})$, а это все делители m_{k+1} по Теореме 3.2.

Таким образом $\mathrm{OD}(a_1, \ldots, a_n)$ — это все делители m_n. Теперь понятно, что $(a_1, \ldots, a_n) = m_n$. □

Следствие 3.5.1 (Линейное представление НОД нескольких чисел)**.** *Для $a_1, \ldots, a_n \in \mathbb{Z}$ существует линейное представление НОД, то есть такие числа $x_1, \ldots, x_n \in \mathbb{Z}$, что $(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n$.*

Доказательство. Докажем индукцией по k что существует линейное представление $m_k = (a_1, \ldots, a_k)$.

База $k = 2$ доказана в Теореме 3.4.

Переход: по Теореме 3.5 и индукционному предположению:

$$m_{k+1} = (a_1, \ldots, a_k, a_{k+1}) = (m_k, a_{k+1}) = y m_k + x_{k+1} a_{k+1} = y(x'_1 a_1 + \cdots + x'_k a_k) + x_{k+1} a_{k+1}$$

$$= (y x_1)' + \cdots + (y x'_k) + x_{k+1} a_{k+1}$$

□

3.6 Взаимно простые числа. Свойства

Определение 3.3. *Числа $a_1, \ldots, a_n \in \mathbb{Z}$ называются взаимно простыми если $(a_1, \ldots, a_n) = 1$.*

Если любые два из $a_1, \ldots, a_n$ взаимно просты, то эти числа называются попарно взаимно простыми.

Свойство 3.3.1. *Если $a_1, \ldots, a_n \in \mathbb{Z}$ попарно взаимно просты, то они взаимно просты.*

Доказательство. Предположим, что это не так. $(a_1, \ldots, a_n) = d > 1$. Тогда $(a_1, a_2) \vdots d \Rightarrow (a_1, a_2) > 1$ — противоречие. □

Свойство 3.3.2. *Если $a, b, c \in \mathbb{Z}$ и $(a, b) = 1$, то $(ac, b) = (c, b)$.*

Доказательство. Пусть $d = (c, b)$ и $f = (ac, b)$.

Из $c \vdots d$ следует, что $ac \vdots d$. Значит $d \in \mathrm{OD}(ac, b)$ и по Теореме 3.2 $f \vdots d$.

Из $b \vdots f$ следует, что $bc \vdots f$. Значит $d \in \mathrm{OD}(ac, bc)$.

По Теоремам 3.3 и 3.2 $c = c(a, b) = (ac, bc) \vdots f$.

Значит $f \in \mathrm{OD}(c, b)$ и по Теореме 3.2 $d \vdots f$.

Так как $d, f \in \mathbb{N}, d \vdots f, f \vdots d$, то $d = f$. □

Свойство 3.3.3. *Если $a, b, c \in \mathbb{Z}$, $(a, b) = 1, ac \vdots b$, то $c \vdots b$.*

Доказательство. По Свойству 3.3.2 $(c, b) = (ac, b) = b$. Следовательно, $c \vdots b$. □

Свойство 3.3.4. *Пусть $a_1, \ldots, a_n, b_1, \ldots, b_m \in \mathbb{Z}$, причем $(a_i, a_j) = 1$. Тогда $(a_1 \cdots a_n, b_1 \cdots b_m) = 1$.*

Доказательство. Докажем, что $(a_1 \cdots a_k, b_j) = 1$ индукцией по k. База $k = 1$ дана в условии. Переход: $(a_1 \cdots a_k a_{k+1}, b_j) = (a_1 \cdots a_k, b_j) = 1$ (по свойству 3.3.2, $(a_{k+1}, b_j) = 1$)

Пусть $A = a_1 \cdots a_n$. Докажем, что $(A, b_1 \cdots b_k) = 1$ индукцией по k. База $k = 1$ доказана ранее. Переход: $(A, a_1 \cdots a_k a_{k+1}) = (A, a_1 \cdots a_k) = 1$ (по свойству 3.3.2 и доказанному ранее) □

3.7 Простые числа, свойства. Бесконечность количества простых

Определение 3.4. *Натуральное число, имеющие ровно два делителя называется простым.*

Натуральное число, имеющие более двух делителей называется составным.

Множество всех простых чисел – $\mathbb{P}$.

Свойство 3.4.1. *Если $a \in \mathbb{N}$ — составное, то существует разложение $a = bc$, где $b, c \in \mathbb{N}$, $a > b, c > 1$.*

Доказательство. Составное число a имеет собственный делитель $b < a$. Тогда $a = bc$, где $c \in \mathbb{N}$. Очевидно, $1 < c < a$. □

Свойство 3.4.2. *Пусть $a \in \mathbb{N}, a \neq 1$. а d — минимальный собственный делитель a. Тогда $d \in \mathbb{P}$.*

Доказательство. По определению, $d > 1$. Предположим, что d — составное. Тогда $d = bc$, $d > b > 1$. Из $a \vdots d$ и $d \vdots b$ следует, что $a \vdots b$. Противоречие с выбором минимального делителя. □

Теорема 3.6. *Простых чисел бесконечно много.*

Доказательство. Предположим противное. Пусть $\mathbb{P} = \{p_1, \ldots, p_n\}$. Пусть $m = p_1 \cdots p_n + 1$, а q — наименьший собственный делитель m. По свойству 3.4.2 $q \in \mathbb{P}$.

Значит, $q = p_i$ для некоторого $i \in \{1, \ldots, p_i\}$. Так как $m - 1 \vdots p_i$, то по свойству 3.2.2 $(m, p_i) = (p_1 \cdots p_i \cdots p_n + 1, p_i) = (1, p_i) = 1$. Значит $m \not\vdots p_i$, противоречие. □

Свойство 3.4.3. *Пусть $a \in \mathbb{Z}, p \in \mathbb{P}$. Тогда либо $a \vdots p$, либо $(a, p) = 1$.*

Доказательство. Так как $d = (a, p) \in \mathbb{N}$ и $p \vdots d$, то $d = 1$ или $d = p$ (так как $p \in \mathbb{P}$). Во второму случае $(a, p) = p \Rightarrow a \vdots p$. □

Свойство 3.4.4. *Пусть $a_1, \ldots, a_n \in \mathbb{Z}$ и $p \in \mathbb{P}$ таковы, что $a_1 \cdots a_n \vdots p$.*

Тогда существует такое i, что $a_i \vdots p$.

Доказательство. Предположим противное. Пусть $\forall i\colon a_i \not\vdots p \Rightarrow (a_i, p) = 1$. По Свойству 3.3.4 тогда $(a_1 \cdots a_n, p) = 1 \Rightarrow a_1 \cdots a_n \not\vdots p$, противоречие. □

3.8 Основная теорема арифметики в Z

Теорема 3.7. *Любое натуральное число $a > 1$ раскладывается в произведение простых чисел. Разложение единственно с точностью до порядка сомножителей.*

Доказательство. Докажем существование по индукции. База — все простые числа, подходит разложение $a = a$.

Переход: пусть a — составное и для всех меньших чисел утверждение доказано. Тогда $a = bc, 0 < b, c < a$. Значит для b, c уже есть разложение, пусть $b = p_1 \cdots p_n, c = q_1 \cdots q_m$. Тогда $a = p_1 \cdots p_n q_1 \cdots q_m$ — искомое разложение.

Докажем единственность. Пусть $a = p_1 \cdots p_n = q_1 \cdots q_m$ — два разложения в произведение простых, причем a — наименьшее натуральное число, для которого существует два разложения.

Так как $p_1 \cdots p_n = a \vdots q_i$, то для некоторого i верно, что $p_i \vdots q_i$. (по свойству 3.4.4) НУО $i = 1$. Так как $p_1, q_1 \in \mathbb{P}$, то $p_1 = q_1$.

Тогда $a' = \frac{a}{p_1} = p_2 \cdots p_n = q_2 \cdots q_m < a$. Однако по предположению a — минимальное число с двумя разложениями. Противоречие.

□

3.9 Каноническое разложение. Количество натуральных делителей числа

Определение 3.5. *Каноническое разложение — представление натурального числа в виде $n = p_1^{k_1} \cdots p_s^{k_s}$, где $p_1, \ldots, p_s \in \mathbb{P}$ различны, а $k_1, \ldots, k_s \in \mathbb{Z}_+$.*

Для $n \in \mathbb{N}$ обозначим через $d(n)$ количество натуральных делителей n.

Теорема 3.8. *Пусть $n = p_1^{k_1} \cdots p_s^{k_s}$ — каноническое разложение. Тогда верны следующие утверждения:*

1. *$n \vdots d$ если и только если $d = p_1^{l_1} \cdots p_s^{l_s}$, где $0 \leqslant l_i \leqslant k_i$*
2. *$d(n) = (k_1 + 1) \cdots (k_s + 1)$*

Доказательство. 1. Достаточность очевидна. Докажем необходимость. Если $n \vdots d$, то d не может иметь простых делителей, кроме $p_1, \ldots p_s$. Значит $d = p_1^{l_1} \cdots p_s^{l_s}$.

Если $l_i > k_i$ для некоторого i, то очевидно, $n \not\vdots d$.

2. Показатель степени простого числа p_i можно выбрать $k_i + 1$ способом. Перемножим количество вариантов для всех p_i и получим искомую формулу. □

3.10 Представление НОД чисел через их канонические разложения

Теорема 3.9. *Пусть $a_1, \ldots, a_n \in \mathbb{N}$. $p_1, \ldots p_s \in \mathbb{P}$, причем $a_i = p_1^{k_{i,1}} \cdots p_s^{k_{i,s}}$ (некоторые показатели могут быть равны 0)*

Тогда

$$(a_1, \ldots, a_m) = p_1^{\min(k_{1,1}, \ldots, k_{m,1})} \cdots p_s^{\min(k_{1,s}, \ldots, k_{m,s})}$$

Доказательство. По теореме 3.8 $d \mid a_t \iff d = p_1^{l_1} \cdots p_s^{l_s}$, где $l_j \leqslant k_{t,j}$ для всех j.

Следовательно, $d \in \mathrm{OD}(a_1, \ldots, a_m) \iff l_i \leqslant \min(k_{1,i}, \ldots, k_{s,i})$

Теперь понятно, что наибольший элемент из $\mathrm{OD}(a_1, \ldots, a_m)$ вычисляется в точности по формуле из условия. □

3.11 Линейные диофантовы уравнения с двумя неизвестными

$$ax + by = c \tag{$*$}$$

где $a, b, c \in \mathbb{Z}$ — константы, $x, y \in \mathbb{Z}$ — неизвестные.

Пусть $d = (a, b)$. Если $c \not\vdots d$, то уравнение не имеет решений.

Далее пусть $c \vdots d, a = da', b = db', c = dc'$. Тогда уравнение $(*)$ эквивалентно

$$a'x + b'y = c \qquad \text{где } (a',\, b') = 1 \tag{$**$}$$

Существует линейное представление НОД $a'x_0 + b'y_0 = 1$. Умножим на c', получим $a'(x_0c') + b'(y_0c') = 1$

Теорема 3.10. *Решения уравнения $(*)$ представляются в виде $x = x_0c' + tb', y = y_0c' - ta', t \in \mathbb{Z}$.*

Доказательство. Будем работать с эквивалентным уравнением $(**)$. Проверим, что это действительно его решения.

$$a'(x_0c' + tb') + b'(y_0c' - ta') = a'(x_0c') + c'(y_0b') + a'tb' - b'ta' = a'(x_0c') + c'(y_0b') = c'$$

Пусть (x, y) - решение $(*)$. Тогда

$$a'x + b'y = c' = a'(x_0c') + b'(y_0c')$$

$$a'x + b'y = a'(x_0c') + b'(y_0c')$$
$$a'(x - x_0c') = b'(y_0c' - y)$$

Тогда $a'(x - x_0c') \vdots b'$. Но $(a', b') = 1$, значит $(x - x_0c') \vdots b'$. Пусть $x - x_0c' = tb'$.

С другой стороны, $b'(y_0c' - y) \vdots a'$. Но $(a', b') = 1$, значит $y_0c' - y \vdots a'$. Значит $y_0c' - y = sa'$. Тогда $a'tb' = b'sa' \Rightarrow s = t$. □

3.12 Идеалы в

Пусть $m \in \mathbb{N}$, тогда нетрудно проверить, что $m\mathbb{Z} = \{mx \colon x \in \mathbb{Z}\}$ — идеал в $\mathbb{Z}$.

Теорема 3.11. *Пусть I — идеал в $\mathbb{Z}$. Тогда $I = m\mathbb{Z}$, где $m \in \mathbb{N}_0$.*

Доказательство. Если $I = \{0\}$, подходит $m = 0$. Далее $I \neq \{0\}$.

Пусть $a \in I$. Тогда и $-a \in I$ (существование обратного элемента в кольце). Одно из чисел a и $-a$ — натуральное. Таким образом, $I' = I \cap \mathbb{N} \neq \emptyset$.

Тогда в I' существует минимальный элемент, обозначим его за m. Докажем, что $I = m\mathbb{Z}$.

Предположим противное, пусть $b \in I, b \not\vdots m$. Тогда $b = mq + r, 0 < r < m$.

Тогда $r = b - mq \in I$, значит $r \in I'$. Противоречие с выбором минимального элемента в I'. □

3.13 Линейное представление НОД: доказательство существования с помощью идеала

Теорема 3.12. *Пусть $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Тогда существует линейное представление $(a_1, \ldots a_n)$, а $\mathrm{OD}(a_1, \ldots, a_n)$ состоит из всех делителей $(a_1, \ldots, a_n)$.*

Доказательство. Пусть $I = \langle\{a_1, \ldots, a_n\}\rangle$ — идеал в $\mathbb{Z}$. Он состоит из линейных комбинаций чисел $a_1, \ldots, a_n$.

Очевидно, $I \neq \{0\}$. Тогда по Теореме 3.11 $\exists d \in \mathbb{N}$: $I = d\mathbb{Z}$. Тогда I состоит из чисел, кратных d.

Так как $a_1, \ldots, a_n \in I$, то все они делятся на d. Значит $d \in \mathrm{OD}(a_1, \ldots, a_n)$.

С другой стороны, $d \in I$, значит $d = a_1x_1 + \cdots + a_nx_n$, где $a_1, \ldots, a_n \in \mathbb{Z}$.

Значит, для любого $f \in \mathrm{OD}(a_1, \ldots, a_n)$ мы имеем $d \vdots f$ (по свойству 4.4.2).

Так как $d > 0$, d — наибольший элемент в $\mathrm{OD}(a_1, \ldots, a_n)$, то есть $d = (a_1, \ldots, a_n)$. □

3.14 Сравнения по модулю натурального числа, свойства. Вычеты

Определение 3.6. *Пусть $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Будем говорить, что a сравнимо по модулю с b, если $a - b \vdots m$. Обозначения: $a \equiv_m b$ или $a \equiv b \pmod m$*

Лемма 3.1. *Пусть $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Следующие утверждения равносильны:*

1. $a \equiv b \pmod m$
2. $a - b \vdots m$
3. *a и b имеют одинаковые остатки от деления на m.*
4. $a \equiv b \pmod{m\mathbb{Z}}$

Доказательство. $1 \iff 2$ по определению сравнения. $2 \iff 3$ очевидно. $2 \iff 4$ по определению главного идеала $m\mathbb{Z}$. □

Свойство 3.6.1. *Если $a \equiv_m a'$ и $b \equiv_m b'$, $x, y \in \mathbb{Z}$, то $ax + by \equiv_m ax' + by'$*

Доказательство.

$$ax + by - (a'x + b'y) = x(a - a') + y(b - b') \vdots m$$

□

Свойство 3.6.2. *Если $a \equiv_m a'$ и $b \equiv_m b'$, то $ab \equiv_m a'b'$.*

Доказательство.

$$ab - a'b' = (ab - a'b) + (a'b - a'b') = b(a - a') + a'(b - b') \vdots m$$

□

Свойство 3.6.3. *Если $a \equiv_m b$ и $n \in \mathbb{N}$, то $a^n \equiv_m b^n$.*

Доказательство. Индукция по n. База $n = 1$ дана в условии. Переход: так как $a^n \equiv_m b^n$ по индукционному предположению и $a \equiv_m b$, то по свойству 3.6.2 имеем $a^{n+1} = a^n \cdot a \equiv b^n \cdot b = b^{n+1}$ □

Свойство 3.6.4. *Если $(a, m) = 1$ и $ab \equiv_m ac$, то $b \equiv_m c$.*

Доказательство. $a(b-c) \vdots m \Rightarrow b - c \vdots m \Rightarrow b \equiv_m c$ (по свойству 3.3.3). □

3.15 Полная система вычетов, свойства

Определение 3.7. *Числа $a_1, \ldots, a_n \in \mathbb{Z}$ — образуют полную систему вычетов по модулю m если каждый вычет по модулю m содержит ровно одно из них.*

Лемма 3.2. *$a_1, \ldots, a_m \in \mathbb{Z}$ — ПСВ $\pmod m$, если и только если никакие два из них не сравнимы по модулю m.*

Доказательство. $\Rightarrow$ следует из определения, $\Leftarrow$ очевидно следует из того, что всего m чисел и никакие два из них не сравнимы по модулю m. □

Теорема 3.13. *Пусть $a_1, \ldots, a_m$ — ПСВ $\pmod m$, $k, b \in \mathbb{Z}, (k, m) = 1$. Тогда $ka_1 + b, \ldots, ka_m + b$ — ПСВ $\pmod m$.*

Доказательство. Проверим условие из леммы 3.2. Предположим, что существует два числа, сравнимых по модулю m. $ka_i + b \equiv_m ka_j + b \Leftrightarrow ka_i + b - ka_j - b \vdots m \Rightarrow k(a_i - a_j) \vdots m$ Так как $(k, m) = 1$, то это означает, что $a_i - a_j \vdots m \Leftrightarrow a_i \equiv_m a_j$, что не так. □

3.16 Приведенная система вычетов, свойства

Если $a \equiv_m b$, то $a - b \vdots m$. Тогда $(a, m) = (b, m)$. Таким образом можно для каждого вычета $\bar{a}$ определить НОД: $(\bar{a}, m) = (a, m)$.

Определение 3.8. *Вычет $\bar{a}$ по модулю m называется взаимно простым с m, если $(\bar{a}, m) = 1$.*

Для $m \in \mathbb{N}$ функция Эйлера $\varphi(m)$ — количество натуральных делителей от 1 до m, взаимно простых с m.

$$\varphi(1) = 1$$

Существует ровно $\varphi(m)$ вычетов по модулю m, взаимно простых с m.

Числа $a_1, \ldots, a_{\varphi(m)}$ образуют приведенную систему вычетов по модулю m (ПрСВ $\pmod m$), если каждый вычет, взаимно простой с m, содержит ровно одно из них.

Лемма 3.3. *$a_1, \ldots, a_{\varphi(m)}$ – ПрСВ $\pmod m$ если и только если все эти числа взаимно просты с m и никакие два из них не сравнимы по модулю с m.*

Доказательство. $\Rightarrow$ следует из определения, $\Leftarrow$ очевидно следует из того, что всего $\varphi(m)$ вычетов взаимно простых с m и никакие два из них не сравнимы по модулю m. □

Теорема 3.14. *Пусть $a_1, \ldots, a_{\varphi(m)}$ — ПрСВ $\pmod m$, $k \in \mathbb{Z}, (k, m) = 1$. Тогда $ka_1, \ldots, ka_{\varphi(m)}$ — ПрСВ $\pmod m$.*

Доказательство. Проверим критерий из леммы 3.3. Так как $(k, m) = 1$ и $(a_i, m) = 1$, то $(ka_i, m) = 1$. Если $ka_i \equiv_m ka_j$, то, так как $(k, m) = 1$, $(a_i \equiv_m a_j)$ по Свойству 3.6.4, что не так. □

3.17 Теорема Эйлера

Теорема 3.15. *Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}, (a, m) = 1$. Тогда $a^{\varphi(m)} \equiv_1 \pmod m$.*

Доказательство. Пусть $r_1, \ldots, r_{\varphi m}$ — ПрСВ $\pmod m$.

Тогда по Теореме 3.14 и $ar_1, \ldots, ar_{\varphi(m)}$ — ПрСВ $\pmod m$.

Введем обозначения $i_1, \ldots, i_{\varphi(m)}$ так, что $r_1 \equiv_m ar_{i_1}, \ldots, r_{\varphi(m)} \equiv_m ar_{i_{\varphi(m)}}$.

Пусть $R = r_1 \cdots r_{\varphi(m)}$. Тогда $(R, m) = 1$, по свойству 3.3.4.

Тогда $R = r_1 \cdots r_{\varphi(m)} \equiv ar_1 \cdots ar_{\varphi(m)} \equiv a^{\varphi(m)} \cdot R \pmod m$ Значит $R \equiv a^{\varphi(m)} R \pmod m$. Сократим на R

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

□

3.18 Мультипликативность функции Эйлера

Лемма 3.4. *Функция Эйлера мультипликативна. То есть, если $a, b \in \mathbb{N}, (a,b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.*

Доказательство. Запишем числа от 1 до ab в таблицу $a \times b$, так, что в первой строке числа от 1 до a, во второй — от $a+1$ до $2a$, и т.д., в b строке от $(b-1)a+1$ до ba.

Все числа в i-м столбце $(i, i+a, \ldots)$ принадлежат одному вычету $\overline{i} = i + a\mathbb{Z}$. Эти числа взаимно просты с a, если и только если $(i,a) = 1$.

Вычеркнем все столбцы с номерами, не взаимно простыми с a. Останется ровно $\varphi(a)$ столбцов. Все числа, взаимно простые с ab должны быть взаимно просты с a, значит они лежат в оставшихся $\varphi(a)$ столбцах.

Рассмотрим оставшийся столбец, пусть числа в нем имеют вид $j, a+j, \ldots, (b-1)a+j$. Эти числа образуют ПСВ (mod b) в силу Теоремы 3.13 (умножили на $a, (a,b) = 1$ и прибавили j к ПСВ $0, 1, \ldots, b-1$).

Значит среди чисел $j, a+j, \ldots, (b-1)a+j$ ровно $\varphi(b)$ чисел, взаимно простых с b. Остальные числа точно не взаимно просты с ab, вычеркнем их.

Таким образом, осталось ровно $\varphi(a)\varphi(b)$ ($\varphi(a)$ столбцов и $\varphi(b)$ чисел в столбце) чисел, взаимно простых с a и b, а значит взаимно простых с ab. □

3.19 Функция Эйлера: значение на степени простого числа, явный вид

Лемма 3.5. *Если $p \in \mathbb{P}, n \in \mathbb{N}$, то $\varphi(p^n) = p^n - p^{n-1}$.*

Доказательство. Посчитаем количество чисел 1 до p^n, не взаимно простых с p.

Пусть $(a, p^n) = d > 1$. Так как $p^n \vdots d$, то $d \vdots p$.

Следовательно, числа от 1 до p^n, не взаимно простые с p^n — это все числа от 1 до p^n, кратные p. Их количество равно $\frac{p^n}{p} = p^{n-1}$. □

Теорема 3.16. *Если $n \in \mathbb{N}$ имеет каноническое разложение $n = p_1^{k_1} \cdots p_m^{k_m}$, то*

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$$

Доказательство. Докажем индукцией по количеству простых делителей s, что $\varphi(p_1^{k_1} \cdots p_s^{k_s}) = \prod_{i=1}^{s} \varphi(p_i^{k_i})$

База $s = 1$ очевидна.

Переход. Так как $(p_1^{k_1} \cdots p_s^{k_s}, p_{s+1}^{k_{s+1}}) = 1$, по индукционному предположению и Лемме 3.4 (мультипликативность функции Эйлера) имеем:

$$\varphi(p_1^{k_1} \cdots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}}) = \varphi(p_1^{k_1} \cdots p_s^{k_s}) \cdot \varphi(p_{s+1}^{k_{s+1}}) =$$

$$= \prod_{i=1}^{s} \left(\varphi(p_i^{k_i})\right) \cdot \varphi(p_{i+1}^{k_{i+1}}) = \prod_{i=1}^{s+1} \left(\varphi(p_i^{k_i})\right)$$

Следовательно,

$$\varphi(n) = \prod_{i=1}^{m} \varphi\left(p_i^{k_i}\right) = \prod_{i=1}^{m} \left(p_i^{k_i} - p_i^{k_i - 1}\right) = \prod_{i=1}^{m} \left(p_i^{k_i}\left(1 - \frac{1}{p_i}\right)\right) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

□

3.20 Сумма функции Эйлера по делителям числа

Теорема 3.17. *Для любого $n \in \mathbb{N}$* $\sum\limits_{d \in \mathbb{N}, d \mid n} \varphi(d) = n$

Доказательство. Рассмотрим все $\mathbb{N}$ числа от 1 до n — всего их ровно n штук. Каждое из них имеет НОД с n — и этот НОД будет делителем n.

Для всех $d \mid n$ посчитаем количество чисел из $\{1, \ldots, n\}$, чей НОД с n равен d.

Такие числа кратны d, значит их надо искать среди $d, 2d, \ldots, n = \frac{n}{d} \cdot d$. Пусть k — множитель при этом числе $(((kd, n = d)))$, тогда $d = (kd, n) = (kd, d \cdot \frac{n}{d}) = d(k, \frac{n}{d}) \Leftrightarrow (k, \frac{n}{d}) = 1$ (можем вынести d по теореме 3.3).

Значит количество чисел из $\{1, \ldots, n\}$, чей НОД с n равен d — это в точности количество таких $k \in \left\{1, \ldots, \frac{n}{d}\right\}$, что $(k, \frac{n}{d}) = 1$, а это количество в точности равно $\varphi(\frac{n}{d})$.

Если суммой пройтись по всем натуральным делителям n и суммировать по $\frac{n}{d}$, то можно и просто пройтись по d.

Таким образом

$$n = \sum_{d \in \mathbb{N}, d \mid n} \varphi(\frac{n}{d}) = \sum_{d \in \mathbb{N}, d \mid n} \varphi(d)$$

□

3.21 Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю

Вычеты по модулю $m \in \mathbb{Z}$ — они же вычеты по модулю идеала $m\mathbb{Z}$ — образуют кольцо вычетов $Z_m := {}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$

Лемма 3.6. *Обратимые элементы в $\mathbb{Z}_m$ — это в точности вычеты из ПрСВ* $(\mathrm{mod}\ m)$.

Доказательство. Если $\bar{a} \in \mathbb{Z}_m$ обратим, то существует такой $\bar{b} \in \mathbb{Z}_m$, что $\bar{a}\bar{b} = \bar{1} \Leftrightarrow ab \equiv_m 1$. Тогда $\Rightarrow (ab, m) = 1 \Rightarrow (a, m) = 1$

Наоборот, если $(a, m) = 1$, то по Теореме 3.13 $0, a, 2a, \ldots, (m-1)a$ — ПСВ $(\mathrm{mod}\ m)$. Значит $\exists b\colon ab \equiv_m 1 \Rightarrow \bar{a}\bar{b} = 1$ □

Теорема 3.18. *Если $p \in \mathbb{P}$, то $\mathbb{Z}_p$ — поле.*

Доказательство. Так как все некратные p числа взаимно просты с p, ПрСВ $(\mathrm{mod}\ p)$ — это все ненулевые вычеты из $\mathbb{Z}_p$. Тогда по Лемме 6, все ненулевые вычеты из $\mathbb{Z}_p$ обратимы. □

3.22 Алгоритм поиска обратного вычета. Решение сравнения с одним неизвестным

Алгоритм поиска обратного вычета. Пусть $a \in \mathbb{Z}, m \in \mathbb{N}$. Как найти обратный вычет a^{-1} в $\mathbb{Z}_m$.

Пусть r — остаток от деления a на m, тогда $0 \leqslant r < m$. Если $r = 0$, то $(a, m) > 1$ и обратного вычета не существует (тогда a не принадлежит ПрСВ $(\mathrm{mod}\ m)$).

Если $r > 0$, то с помощью алгоритма Евклида ищем $d = (r, m) = (a, m)$.

Если $d > 1$ то a, m не взаимно просты, а значит вычета не существует.

Если $d = 1$, ищем линейное представление НОД $(a, m) = 1 = a \cdot x + m \cdot y$.

Значит если они равны, то и остаток от деления на m у них будет равен:

$$ax + my \equiv_m 1$$

Так как $my \equiv_m 0$, избавимся от него:

$$ax \equiv_m 1$$

Тогда $ax \equiv_m 1$, а значит $(\bar{a})^{-1} = \bar{x}$ в $\mathbb{Z}_m$.

Решение сравнения с одним неизвестным. Пусть $a, b \in \mathbb{Z}, m \in \mathbb{N}$. Нужно решить относительно x сравнение

$$ax \equiv b \pmod{m} \qquad (*)$$

Пусть $d = (a, m)$. Если $b \not\vdots d$, то $(*)$ решений не имеет.

Если $b \vdots d$, то пусть $a = a'd$, $b = b'd$, $m = m'd$. Тогда уравнение $(*)$ эквивалентно: $ax - b \vdots m \Leftrightarrow a'dx - b'd \vdots m'd \Leftrightarrow a'x - b' \vdots m' \Leftrightarrow a'x \equiv_{m'} b'$

$$a'x \equiv b' \pmod{m'} \qquad (**)$$

Тогда $(a, m) = (a'd, m'd) = d \Rightarrow (a', m') = 1$, а значит существует обратный вычет $(\overline{a'})^{-1}$ в $\mathbb{Z}_{m'}$.

Пусть $s \in (\overline{a'})^{-1}$. Тогда $x \equiv b's \pmod{m'}$ — решение сравнения $(**)$. Проверим это:

$$a'b's = (a's)b' = 1 \cdot b' = b'$$

3.23 Делимость на попарно взаимно простые числа

Лемма 3.7. *Пусть $m_1, \ldots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \cdots m_k$. Пусть $b \in \mathbb{Z}$ таково, что $b \vdots m_1, \ldots, b \vdots m_k$.*

Доказательство. Пусть $n_l = m_1 \cdots m_l$. Докажем индукцией по l, что $b \vdots n_l$. База $l = 1$ очевидна. Переход: по индукционному предположению $b = cn_l$, где $c \in \mathbb{Z}$.

Так $cn_l \vdots m_{l+1}$ и $(n_l, m_{l+1}) = 1$ (как взаимно простые), по Свойству 3.3.3 имеем $c \vdots m_{l+1}$.

Значит $c = dm_{l+1}$ и $b = dm_{l+1}n_l = dn_{l+1} \vdots n_{l+1}$. □

3.24 Китайская теорема об остатках

Теорема 3.19. *Пусть $m_1, \dots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \cdots m_k$, $a_1, \dots, a_k \in \mathbb{Z}$. Тогда существует единственное $a \in \{0, 1, \dots, m-1\}$, такое что $a \equiv_{m_1} a_1, \dots, a \equiv_{m_k} a_k$.*

Доказательство. Докажем существование. Пусть $n_l = m_1 \cdots m_l$. Докажем индукцией по l существование такого $b_l \in \mathbb{Z}$, что $b_l \equiv_{m_1} a_1, \dots b_l \equiv_{m_l} a_l$.

База $l = 1$ очевидна.

Переход: Так как $(m_{l+1}, n_l) = 1$, то по Теореме 3.13 числа $b_l, n_l + b_l, 2n_l + b_l, \dots, (m_{l+1}-1)n_l + b_l$ — ПСВ $\pmod{m_{l+1}}$ (они получены из ПСВ $0, 1, \dots, m_{l+1} - 1$ умножением на n_l и прибавлением b_l).

Значит, среди этих чисел есть числo $kn_l + b_l \equiv_{m_{l+1}} a_{l+1}$. Положим $b_{l+1} \coloneqq kn_l + b_l$

Тогда $b_{l+1} - a_{l+1} \vdots m_{l+1} \iff b_{l+1} \equiv_{m_{l+1}} a_{l+1}$.

По построению $b_{l+1} - b_l = kn_l + b_l - b_l = kn_l \vdots n_l$. Так как по индукционному предположению $b_l \equiv_{m_i} a_i$ для $i \leqslant l$, то $b_{l+1} - a_i = (b_l + 1 - b_l) + (b_l - a_i) \vdots m_i$.

Таким образом мы получили число b_k удовлетворяющее требованиям теоремы, кроме одного: число должно быть от 0 до $m - 1$.

Для получения такого числа поделим на m. Пусть $b_k = mq + a, 0 \leqslant a \leqslant m-1$ Так как $a - b_k \vdots m \vdots m_i \Rightarrow a - b_k \vdots m_i \Rightarrow a \equiv_{m_i} b_k$ и $b_k - a_i \vdots m_i$, то $a - a_i \vdots m_i$.

Докажем единственность. Предположим что a и a' — два различных числа, удовлетворяющих условию. Тогда $a \equiv_{m_i} a' \Rightarrow a - a' \vdots m_i$.

Так как $m_1, \dots, m_k$ попарно взаимно просты, то по Лемме 3.7 $a - a' \vdots m = m_1 \dots m_k$, но $|a - a'| < m$, так как $a, a' < m$. Противоречие. □

3.25 Алгоритмы поиска решения для КТО

Необходимо решить следующую систему:

$$\begin{cases} a \equiv a_1 \pmod{m_1} \\ \vdots \\ a \equiv a_k \pmod{m_k} \end{cases}$$

Первый алгоритм.
Пусть $m'_i = \frac{m_1 \cdots m_k}{m_i}$. Тогда $(m'_i, m_i) = 1$. Пусть $b_i \in \{0, 1, \cdots, m_i -\}$ — такое число, что $b_i \cdot m'_i \equiv 1 \pmod{m_i}$.
Тогда $a = a_1 b_1 m'_1 + a_2 b_2 m'_2 + \cdots + a_k b_k m'_k$ — решение КТО.

Так как $m'_j \vdots m_i$ при $i \neq j$, то

$$a = a_1 b_1 m'_1 + \cdots + a_i b_i m'_i + \cdots + a_k b_k m'_k \equiv_{m_i} a_i b_i m'_i \equiv a_i \cdot (b_i m'_i) \equiv a_i$$

Второй алгоритм. Индукцией по s найдем x_s, удовлетворяющий первым s сравненям: $x_s \equiv_{m_1} a_1, \dots, x_s \equiv_{m_s} a_s$.
База $s = 1$ очевидна: подойдет $x_1 = a_1$.
Переход. Пусть $n_s = m_1 \cdots m_s$. Будем искать решение в виде $x_{s+1} = x_s + c_s n_s$. Тогда $x_{s+1} - x_s = x_s + c_s n_s - x_s = c_s n_s = c_s(m_1 \cdots m_s) \vdots m_j$ для всех $j \in \{1, 2, \dots, s\}$, поэтому x_{s+1} удовлетворяет первым s сравнениям.
Подберем c_s так, чтобы $x_{s+1} \equiv a_{s+1} \pmod{m_{s+1}}$. $x_s + c_s n_s \equiv a_{s+1} \pmod{m_{s+1}} \Leftrightarrow c_s n_s \equiv a_{s+1} - x_s \pmod{m_{s+1}} \Leftrightarrow c_s \equiv (a_{s+1} - x_s)(n_s)^{-1} \pmod{m_{s+1}}$.
Так как $(n_s, m_{s+1}) = 1$, то обратный элемент существует и может быть найден.

3.26 Функция Мёбиуса. Сумма функции Мёбиуса по промежуточным делителям

Определение 3.9 (Функция обращения Мёбиуса)**.**

$$\mu(n) \coloneqq \begin{cases} 1, & \text{если } n = 1 \\ (-1)^k, & \text{если } n = p_1 \cdots p_k \text{ — произведение различных простых чисел} \\ 0, & \text{если } n \text{ делится на квадрат простого числа} \end{cases}$$

Лемма 3.8. *Пусть $m, d \in \mathbb{N}$, $m \vdots d$. Тогда*

$$\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & m = d \\ 0, & m > d \end{cases}$$

Доказательство. Пусть $k \coloneqq \frac{m}{d} = p_1^{t_1} \cdots p_r^{t_r}$ — каноническое разложение. Тогда

$$\sum_{d|n|m} \mu(\frac{m}{n}) = \sum_{s|p_1 \cdots p_r} = \sum_{l=0}^{r} C_r^l (-1)^l = (1-1)^r$$

Переход к C_r^l — l — количество простых делителей в s, тогда $\mu(s) = (-1)^l$, и всего таких можно выбрать ровно C_r^l. Далее переходим по биному Ньютона к $(1-1)^r$.

В итоге сумма равна 0 во всех случаях, кроме $r = 0$, а это в точности $k = 1 \Leftrightarrow m = d$. В остальных случаях сумма равна 1. □

3.27 Формула обращения Мёбиуса, аддитивный вариант

Теорема 3.20. *Пусть* $f, g \colon \mathbb{N} \to$, *причем* $f(m) = \sum\limits_{d|m} g(d)$.

Тогда $g(m) = \sum\limits_{n|m} \mu(\frac{m}{n}) f(n)$

Доказательство.

$$\sum_{n|m} \mu\left(\frac{m}{n}\right) f(n) = \sum_{n|m} \mu\left(\frac{m}{n}\right) \sum_{d|n} g(d) = \sum_{d|m} g(d) \cdot \sum_{d|n|m} \mu(\frac{m}{n}) = g(m)$$

□

3.28 Вывод формулы для функции Эйлера из формулы обращения Мёбиуса

Теорема 3.21. *Пусть* $n = p_1^{k_1} \cdots p_s^{k_s}$ *— каноническое разложение числа* n. *Тогда* $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_s})$.

Теорема 3.22. *По Теореме 3.17*

3.29 Формула обращения Мёбиуса, мультипликативнй вариант

3.30 Сумма мультипликативной функции по делителям числа мультипликкативна

3.31 Сумма натуральных делителей числа

3.32 Первообразные корни из 1 в C

Глава 4

Многочлены над полем

4.1 Сложение и умножение многочленов. Степень многочлена. Свойства

Определение 4.1. *Пусть K — коммутативное кольцо. Тогда кольцо многочленов над K состоит из бесконечных последовательностей $(a_0, a_1, \ldots, a_n, \ldots)$ с коэффициентами из K, в которых лишь конечное число ненулевых коэффициентов.*

Сложение многочленов покоэффициентное:

$$(a_0, \ldots, a_n, \ldots) + (b_0, \ldots, b_n, \ldots) = (a_0 + b_0, \ldots, a_n + b_n, \ldots)$$

Определим **умножение** многочленов:

$$(a_0, \ldots, a_n, \ldots) + (b_0, \ldots, b_n, \ldots) = (c_0, \ldots, c_n, \ldots)$$

где

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

(то есть произведение тех коэффициентов, чьи степени равны n)

Степень многочлена $f = (a_0, \ldots, a_n, \ldots)$ — это максимальный номер ненулевого коэффициента (обозначение: $\deg(f)$). Отдельно определим степень многочлена $0 := (0, \ldots, 0, \ldots)$: положим $\deg(0) = -\infty$. Если $\deg(f) = n$, $n \in \mathbb{N}_0$, то a_n называется **старшим коэффициентом** f.

Если $f = (a_0, \ldots, a_n, \ldots)$ и $deg(f) \leqslant n$, часто применяется формальная запись

$$f(t) = a_n t_n + \ldots + a_1 t + a_0$$

где t — формальная переменная. Кольцо многочленов над полем K обозначается через $K[t]$, где t — переменная

Свойство 4.1.1. $\deg(fg) \leqslant \deg(f) + \deg(g)$. *Если K — кольцо без делителей 0, то* $\deg(fg) = \deg(f) + \deg(g)$

Доказательство. Если один из многочленов равен 0, то и произведение равно 0. Тогда $\deg(fg) = -\infty = \deg(f) + \deg(g)$.

Пусть $\deg(f) = n$, $\deg(g) = m$, где $n, m \in \mathbb{N}_0$, $f = (a_0, \ldots, a_s, \ldots)$, $g = (a_0, \ldots, a_s, \ldots)$, $fg = (c_0, \ldots, c_s, \ldots)$.

Тогда, если $k > n + m$, то $c_k = (\sum\limits_{i=0}^{n-1} a_i b_{k-i}) + (\sum\limits_{i=n}^{k} a_i b_{k-i}) = 0$

В первой сумме $k - i$ будет больше, чем m (так как мы вычитаем из $k > n + m$ число, меньшее n), во второй сумме $i > n$ (кроме случая, когда $i = n$, но тогда $b_{k-n} = 0$), значит $a_i = 0$.

Значит $\deg(fg) \leqslant \deg(f) + \deg(g)$.

Теперь докажем равенство для случая, когда K — кольцо без делителей 0.

$$c_{n+m} = (\sum_{i=0}^{n-1} a_i b_{n+m-i}) + a_n b_m + (\sum_{i=n+1}^{n+m} a_i b_{n+m-i}) = a_n b_m \neq 0$$

□

Свойство 4.1.2. $\deg(f + g) \leqslant \max(\deg(f), \deg(g))$. *Если* $\deg(f) \neq \deg(g)$, *то* $\deg(f + g) = \max(\deg(f), \deg(g))$

Доказательство. При $k > \max(\deg(f), \deg(g))$ имеем $a_k + b_k = 0 + 0 = 0$. Значит $\deg(f + g) \leqslant \max(\deg(f), \deg(g))$.

Пусть не умоляя общности $\deg(f) = n > \deg(g)$. Тогда $a_n + b_n = a_n + 0 = a_n \neq 0$. □

4.2 Кольцо многочленов

Теорема 4.1. *Пусть K — коммутативное кольцо. Тогда $K[t]$ — тоже коммутативное кольцо. Если при этом K — кольцо с 1, то $K[t]$ — тоже кольцо с 1.*

Доказательство. Ассоциативность и коммутативность сложения в $K[t]$ следуют из ассоциативности и коммутативности сложения в K. (так как сложение покоэффициентное).

Несложно проверить, что многочлен 0 будет нейтральным элементом по сложению в $K[t]$ (т.е. нулем).

Обратный элемент по сложению. Для $f = (a_0, \dots, a_n, \dots)$ положим $-f := (-a_0, \dots, -a_n, \dots)$.

Коммутативность умножения: пусть $f = (a_0, \dots, a_n, \dots)$, $g = (b_0, \dots, b_n, \dots)$, $fg = (d_0, \dots, d_n, \dots)$, $gf = (d'_0, \dots, d'_n, \dots)$. Тогда $d_n = \sum\limits_{i=0}^{n} a_i b_{n-i} = \sum\limits_{i=0}^{n} b_{n-i} a_i = d'_n$

Дистрибутивность: пусть $h = (c_0, \dots, c_n, \dots)$, $(f+g)h = (d_0, \dots, d_n, \dots)$, $fh = (p_0, \dots, p_n, \dots)$, $gh = (q_0, \dots, q_n, \dots)$. Тогда $d_n = \sum\limits_{i=0}^{n} (a_i + b_i) c_{n-i} = (\sum\limits_{i=0}^{n} a_i c_{n-i}) + (\sum\limits_{i=0}^{n} b_i c_{n-i}) = p_n + q_n$, а это коэффициент многочлена $fh + gh$.

Ассоциативность умножения: пусть $fg = (d_0, \dots, d_n, \dots)$, $(fg)h = (p_0, \dots, p_n, \dots)$. Тогда:

$$p_n = \sum_{k=0}^{n} d_k c_n - k = \sum_{k=0}^{n} (\sum_{i=0}^{k} a_i b_{k-i}) c_{n-k} = \sum_{i,j,k \in \mathbb{N}_0, i+j+l=n} a_i b_i c_l$$

Аналогично можно доказать и для другого порядка скобок.

Если существует $1 \in K$, несложно проверить, что $1 := (1, 0, \dots, 0, \dots)$ — единица в $K[t]$. □

4.3 Вложение K в $K[t]$. Константы. Ассоциированные многочлены

Лемма 4.1. *Пусть K — коммутативное кольцо, $\varphi : K \to K[t]$ задано формулой $\varphi(c) = (c, 0, \dots, 0, \dots)$. Тогда φ — мономорфизм колец. (то есть φ — инъекция)*

Доказательство. Пусть $a, b \in K$. Тогда $\varphi(a+b) = (a+b, 0, \dots, 0, \dots) = (a, 0, \dots, 0, \dots) + (b, 0, \dots, 0, \dots) = \varphi(a) + \varphi(b)$

$\varphi(ab) = (ab, 0, \dots, 0, \dots)$, а $\varphi(a)\varphi(b) = (a, 0, \dots, 0, \dots) \cdot (b, 0, \dots, 0, \dots) := (c_0, \dots, c_n, \dots)$.

Тогда $c_0 = ab$, а при $n > 0$ $c_n = \sum\limits_{i=0}^{n} a_i b_{n-i} = 0$. Значит $\varphi(ab) = \varphi(a)\varphi(b)$.

Таким образом, φ — гомоморфизм.

Пусть $a \in \mathrm{Ker}(\varphi)$. Тогда $(a, 0, \dots, 0, \dots) = \varphi(a) = (0, 0, \dots)$, значит $a = 0$. □

Определение 4.2. *Многочлен вида $(a, 0, \dots, 0, \dots)$ называется* ***константой****.*

Мы будем отождествлять такой многочлен с числом $a \in K$ и считать, что $K \subset K[t]$.

Нетрудно проверить, что для $a \in K$ и $f = (b_0, b_1, \dots, b_n, \dots)$ выполнено $(a, 0, \dots, 0, \dots) \cdot (b_0, b_1, \dots, b_n, \dots) = (ab_0, ab_1, \dots)$. Мы будем обозначать такой многочлен af и говорить, что он получен из f умножением на константу.

Лемма 4.2. *Если K — поле, то обратимые элементы в $K[t]$ — в точности ненулевые Константы*

Доказательство. Пусть $f, g \in K[t]$, $fg = 1$. Тогда $0 = \deg(1) = \deg(f) + \deg(g)$, откуда следует, что $\deg(f) = \deg(g) = 0$, то есть f и g — ненулевые константы.

Наоборот, если $a \in K, a \neq 0$, то существует $a^{-1} \in K$, числам a и a^{-1} соответствуют взаимно обратные многочлены-константы в $K[t]$. □

Определение 4.3. *Пусть $f, g \in K[t]$, K — поле. Будем говорить, что f и g ассоциированы, если $f = cg$, где $c \in K, c \neq 0$. (обозначение: $f \sim g$)*

Лемма 4.3. *Ассоциированность — отношение эквивалентности.*

Доказательство. Рефлексивность: $f = 1 \cdot f$, значит $f \sim f$.

Симметричность. Пусть $f \sim g$, тогда $\exists a \in K$: $f = ag$. Тогда $g = a^{-1} f$, значит $g \sim f$. (по лемме 4.2)

Транзитивность: пусть $f \sim g$, $g \sim h$. Тогда $\exists a, b \in K$: $f = ag$, $g = bh$. Тогда $f = ag = (ab)h$, значит $f \sim h$.

Если $f, g \in K[t]$ и $f \sim g$, то $\deg(f) = \deg(g)$. $-f = (-1) \cdot f$, следовательно $-f \sim f$. □

4.4 Теорема о делении с остатком в кольце многочленов над полем

Теорема 4.2 (Теорема о делении с остатком)**.** *Пусть K — поле, $f, g \in K[t]$, причем $g \neq 0$. Тогда существуют единственные такие $q, r \in K[t]$, что $f = gq + r$ и $\deg(r) < \deg(g)$.*

Многочлен r называется остатком от деления f на g.

Доказательство. Пусть $\deg(f) = n$, $\deg(g) = m$, $f(t) = a_n t^n + \cdots + a_0$ и $g(t) = b_m t^m + \cdots + b_0$.

Докажем существование по индукции. База для случая $n < m$: тогда подходит $q = 0$ и $r = f$.

Переход: пусть для $n \geq m$ и для многочленов степени меньше чем n утверждение доказано.

Возьмем многочлен $f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} \cdot g(t) = a_n t^n + \cdots + a_0 - \frac{a_n}{b_m} t^{n-m} \cdot (b_m t^m + \cdots + b_0)$ Рассмотрим старшую степень многочлена: $a_n t^n - frac a_n b_m t^{n-m} \cdot b_m t^m = a_n t^n - a_n t^n = 0$. Таким образом, $\deg(f_1) < n$, значит, по индукционному предположению $f_1 = q_1 g + r$, где $\deg(r) < \deg(g) = m$.

Тогда $f = f_1 + \frac{a_n}{b_m} t^{n-m} \cdot g = q_1 g + r + \frac{a_n}{b_m} t^{n-m} \cdot g = (q_1 + \frac{a_n}{b_m}) g + r$. Так как $\deg(q_1) < \deg(f_1) < n$, $\deg(g) = m < n$, $\deg(r) < m < n$, то это — искомое представление.

Докажем единственность. Пусть $f = q_1 g + r_1 = q_2 g + r_2$, где $\deg(r_1) < m$ и $\deg(r_2) < m$. Тогда $r_1 - r_2 = q_2 g - q_1 g = (q_2 - q_1) g$.

Пусть $q_1 \neq q_2$. Тогда $\deg(q_2 - q_1) \in \mathbb{N}_0$ и $\deg((q_2 - q_1) g) = \deg(q_2 - q_1) + \deg(g) \geqslant g$ (по свойству 4.1.1 и так как $\deg(g) = m$).

С другой стороны, $\deg((q_2 - q_1) g) = \deg(r_1 - r_2) \leqslant \max(\deg(r_1), \deg(r_2)) < m$. (по свойству 4.1.2)

Получаем противоречие, значит $q_2 = q_1$, тогда и $r_1 = r_2$, то есть разложения полностью совпадают. □

4.5 Делимость многочленов. Свойства

Определение 4.4. *Пусть K — поле, $f, g \in K[t]$, $g \neq 0$. Говорят, что f делится на g ($f \vdots g$), если существует такой $h \in K[t]$, что $f = gh$.*

Свойство 4.4.1. *Если $f \vdots g$ и $g \vdots h$, то $f \vdots h$.*

Доказательство. $f = ag$, $g = bh$, $f = ag = (ab)h$. □

Свойство 4.4.2. *Пусть $f, g \vdots h$, а $p, q, \in K[t]$. Тогда $fp + gq \vdots h$.*

Доказательство. $f = ah$, $g = bh$, $fp + gq = ahp + bhq = h(ap + bq) \vdots h$. □

Свойство 4.4.3. *Пусть $f, g \in K[t]$, $f \neq 0$, $f \vdots g$. Тогда $\deg(f) \geqslant \deg(g)$.*

Доказательство. Тогда $f = gh$, где $h \in K[t]$, причем $g \neq 0$. Следовательно $\deg(f) = \deg(g) + \deg(h) \geqslant \deg(g)$. □

Свойство 4.4.4. *Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ и $\deg(f) = \deg(g)$. Тогда $f \sim g$.*

Доказательство. Тогда $f = gh$, где $h \in K[t]$ и $\deg(g) = \deg(f) = \deg(g) + \deg(h)$, значит $\deg(h) = 0$, значит $h \in K, h \neq 0$, значит $f \sim g$. □

Свойство 4.4.5. *Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ и $g \vdots f$, тогда $f \sim g$.*

Доказательство. Тогда $\deg(f) \geqslant \deg(g)$ и $\deg(g) \geqslant \deg(f)$, значит $\deg(f) = \deg(g)$. По свойству 4.4.4 $f \sim g$. □

4.6 Идеалы в кольце многочленов над полем

Теорема 4.3. *Пусть K — поле, а I — идеал в $K[t]$. Тогда $I = dK[t]$ для некоторого $d \in K[t]$.*

Доказательство. Если $I = \{0\}$ подойдет $d = 0$. Далее $I \neq \{0\}$.

Рассмотрим все ненулевые многочлены из I и найдем из них многочлен наименьший степени. Обозначим его за d.

Докажем, что все многочлены из I делятся на d (что равносильно тому, что $I = dK[t]$.).

Пусть некоторый многочлен f не делится на d. Тогда поделим его с остатком: $f = qd + r$, причем $\deg(r) < \deg(d)$ (по теореме о делении с остатком (теорема 4.2)).

Тогда, так как $f, d \in I$, получаем, что $r = f - qd \in I$. (из замкнутости идеалов над сложением)

Получаем противоречие с выбором многочлена наименьшей степени. □

4.7 НОД в кольце многочленов над полем: теорема о линейном представлении

Определение 4.5. *Пусть K — поле, $f_1, \ldots, f_n \in K[t]$. Тогда $\mathrm{OD}(f1, \ldots, f_n)$ — это множество всех многочленов, являющихся общими делителями $f_1, \ldots, f_n$, а их **НОД** — это любой многочлен наибольшей степени из $\mathrm{OD}(f_1, \ldots, f_n)$.*

Мы докажем, что многочлены наибольшей степени в $\mathrm{OD}(f_1, \ldots, f_n)$ — это в точности множество попарно ассоциированных между собой многочленов.

В таком случае нам все равно, какой из них считать НОДом, для удобства будем считать НОДом любой из них. Запись $(f_1, \ldots, f_n) = d$ следует понимать так: НОД — любой из многочленов, ассоциированных с d.

Определение 4.6. ***Линейное представление НОД*** *— это представление вида* $(f_1, \ldots, f_n) = p_1 f_1 + p_2 f_2 + \ldots p_n f_n$, *где* $p_1, \ldots, p_n \in K[t]$.

Если найти линейное представление любого НОД, то найдутся и линейные представления всех остальных (мы докажем, что все НОД попарно ассоциированы).

Теорема 4.4 (теорема о линейном представлени НОД)**.** *Пусть* K *— поле,* $f_1, \ldots, f_n \in K[t]$.

1. *Существует линейное представление* $(f_1, \ldots, f_n)$.
2. $\mathrm{OD}(f_1, \ldots, f_n)$ *состоит из всех делителей* $(f_1, \ldots, f_n)$.
3. *Все НОД* $f_1, \ldots, f_n$ *попарно ассоциированы.*

Доказательство.

1. Пусть $I = \langle f_1, \ldots, f_n \rangle$ (это идеал, состоящий из всех линейный комбинаций $f_1, \ldots, f_n$, см. билет **??**)

   По теореме 4.3, $I = dK[t]$ для некоторого многочлена $d \in K[t]$. Так как $f_1, \ldots, f_n \in I$, все они делятся на d Значит $d \in \mathrm{OD}(f_1, \ldots, f_n)$.

   Так как $d \in I$, существует представление $d = p_1 f_1 + p_2 f_2 + \ldots p_n f_n$.

   Пусть $g \in \mathrm{OD}(f_1, \ldots, f_n)$. Тогда $d \vdots g$ (по свойству 4.4.2, так как $f_1, \ldots, f_n \vdots g, d$). Значит $\deg(d) \geqslant \deg(g)$.

   Следовательно d — многочлен наибольшей степени из $\mathrm{OD}(f_1, \ldots, f_n)$, то есть НОД этих многочленов.
2. Выше доказано, что d делится на каждый многочлен из $\mathrm{OD}(f_1, \ldots, f_n)$.
3. Пусть $g \in \mathrm{OD}(f_1, \ldots, f_n)$ и $\deg(g) = \deg(f)$. Тогда по свойству 4.4.4 $d \sim g$.

   В обратную сторону, если $g \sim d$, то $g \in I$. Множество кратных d совпадает с множеством кратных g, поэтому $I = gK[t]$ и все доказанное выше для d верно и для g. Следовательно, НОДы $f_1, \ldots, f_n$ — это в точности все многочлены, ассоциированные с d.

□

4.8 Свойства НОДа в кольце многочленов над полем

Свойство 4.6.1. *Если* $f, g, h \in K[t]$, *то* (fh, gh) $(f, g)h$.

Доказательство. Пусть $I = \langle f, g \rangle$, и $I_h = \langle fh, gh \langle$ Первый идеал состоит из всех линейны комбинаций f и g, а второй — из линейных комбинаций fh и gh.

Следовательно, $p \in I \Rightarrow p = qf + rg \Leftrightarrow ph = q(fh) + r(gh) \Leftrightarrow ph \in I_h$ (здесь $q, r \in K[t]$)

Поэтому, если $I = dK[t]$, то $I = dhK[t]$. Тогда $(f, g) = d$, а $(fh, gh) = dh = (f, g)h$. □

Свойство 4.6.2. *Если* $f, g \in K[t]$ *и* $f \vdots g$, *то* (f, g) g.

Доказательство. Пусть $I = \langle f, g \rangle$. Так как $f \vdots g$, то все линейные комбинации f и g — в точности все кратные g многочлены, значит $I = gK[t]$. Тогда g — многочлен наименьшей степени в I и многочлен наибольшей степени в $\mathrm{OD}(f, g)$, то есть НОД (f, g). Таким образом, $(f, g) = g$. □

Свойство 4.6.3 (Алгоритм Евклида для полиномов)**.** *Если* $f, g, h, p \in K[t]$ *и* $h = f + pg$, *то* $(f, g) \sim (h, g)$

Доказательство. Пусть $I_f = \langle f, g \rangle$ и $I_h = \langle g, h \rangle$

Так как $h = f + pg$ линейная комбинация f и g из I_f является также и линейной комбинацией h из множества I_h, таким образом $I_f \supset I_h$.

Так как $f = h - pg$, аналогично получаем $I_h \subset I_f$. Значит $I_f = I_h = dK[t]$. Теперь, по теореме 4.4 ясно, что $(f, g) \sim d \sim (h, g)$. □

Теорема 4.4.4 не помогает найти линейное представление двух многочленов, а помогает алгоритм Евклида, который состоит в последовательном делении с остатком.

Последний остаток и будет НОДом по свойствам 4.4.2 и 4.4.3.

Двигаясь назад по алгоритму Евклида, можно получить линейное представление НОД.

(когда нибудь я допишу сюда пример)

С помощью следующей леммы строится линейное представление НОД нескольких многочленов.

4.9 Вычисление НОДа нескольких многочленов через НОДы двух

Лемма 4.4. *Пусть $n \geqslant 2$, $f_1, \ldots, f_n \in K[t]$. Положим $d_2 = (f_1, f_2), d_3 = (d_2, f_3), d_n = (d_{n-1}, f_n)$. Тогда $(f_1, \ldots, f_n) = d_n$.*

Доказательство. Индукцией по k докажем, что $\mathrm{OD}(f_1, \ldots, f_k)$ — все делители d_k.

База $k = 2$ доказана в теореме 4.4.

Переход $k \to k+1$. $\mathrm{OD}(f_1, \ldots, f_k, f_{k+1})$ — все многочлены из $\mathrm{OD}(f_1, \ldots, f_k)$, являющиеся делителями f_{k+1}.

Так как $\mathrm{OD}(f_1, \ldots, f_k)$ — это все делители d_k, получаем, что $\mathrm{OD}(f_1, \ldots, f_k, f_{k+1}) = \mathrm{OD}(d, f_{k+1})$, а это все делители $d_{k+1} = (d_k, f_{k+1})$ по теореме 4.4.

Таким образом, $\mathrm{OD}(f_1, \ldots, f_n)$ — все делители d_n. Наибольшую степень из них имеет d_n, а значит $d_n = (f_1, \ldots, f_n)$. □

4.10 Взаимно простые многочлены. Свойства

Определение 4.7. *Пусть K — поле, $f_1, \ldots, f_n \in K[t]$*

- *Многочлены $f_1, \ldots, f_n$ взаимно просты, если $(f_1, \ldots, f_n) \sim 1$.*
- *Многочлены $f_1, \ldots, f_n$ попарно взаимно просты, если любые два из них вазимно просты.*

Свойство 4.7.1. *Если $f, g, h \in K[t]$ и (f, g) 1, то (fh, g) (h, g)*

Доказательство. Пусть $p = (h, g)$ и $q = (fh, g)$. Из $h \vdots p$ следует, что $fh \vdots p$. Значит $p \in \mathrm{OD}(fh, g)$ и по Теореме 4.4 $q \vdots p$.

Из $g \vdots q$ следует, что $gh \vdots q$. Значит, $qin\,\mathrm{OD}(fh, gh)$.

По Свойству 4.6.1 и теореме 4.4, h $h(f, g)$ $(hf, gh) \vdots q \Rightarrow h \vdots q$

Значит $q \in \mathrm{OD}(h, g)$ и по теореме 4.4 $p \vdots q$ (так как $p = (h, g)$ — многочлен наибольшей степени в $\mathrm{OD}(h, g)$).

Из $q \vdots p$ и $p \vdots q$ по Свойству 4.4.5 p q. □

Свойство 4.7.2. *Если $f, g, h \in K[t]$, (f, g) 1 и $fh \vdots g$, то $h \vdots g$.*

Доказательство. По Свойству4.7.1 $(h, g) \sim (fh, g) \sim g$ (последнее верно так как $fh \vdots g$). Значит $(h, g) \sim g$, значит $h \vdots g$. □

Свойство 4.7.3. *Пусть $f_1, \ldots, f_n, g_1, \ldots, g_m \in K[t]$, причем $(f_i, g_j) \sim 1$ для всех $i \in \{1, \ldots, n\}$ и $j \in \{1, \ldots, m\}$. Тогда $(f_1 \cdots f_n, g_1 \cdots g_m) = 1$*

Доказательство. Докажем, что $(f_1 \cdots f_k, g_j) = 1$ для всех $j \in \{1, \ldots, m\}$ индукцией по k.

База $k = 1$: дано в условии

Переход $k \to k+1$: $(f_1 \cdots f_k f_{k+1}, g_j) \sim (f_1 \cdots f_k, g_j) \sim 1$ по индукционному предположению. (переход верен по свойству 4.7.1 так как $(f_{k+1}, g_j) \sim 1$)

Пусть $F = f_1 \cdots f_n$. Докажем, что $(F, g_1 \cdots g_k) \sim 1$ для всех $k \in \{1, \ldots, m\}$ индукцией по k.

База: $k = 1$ доказано выше. Переход $k \to k+1$: $(F, g_1 \cdots g_k g_{k+1}) \sim (F, g_1 \cdots g_k) \sim 1$ (аналогично по свойству 4.7.1 и так как $(F, g_{k+1} \sim 1)$) □

Свойство 4.7.4. *Пусть $f, p_1, \ldots, p_n \in K[t]$, причем $p_1, \ldots, p_n$ попарно взаимно просты, а $f \vdots p_i$ для всех $i \in \{1, \ldots, n\}$. Тогда $f \vdots p_1 p_2 \cdots p_2$.*

Доказательство. Пусть $q_l = p_1 \cdots p_l$. Докажем по индукции, что $f \vdots q_l$.

База $l = 1$ по условию.

Переход: $l \to l+1$. По индукционному предположению $f = hq_l$, где $h \in K[t]$. Так как $hq_l = f \vdots p_{l+1}$ и $(q_l, p_{l+1}) \sim 1$ (по свойству 4.7.3), по свойству 4.7.2 имеем $h \vdots p_{l+1}$, тогда $h = gp_{l+1}$ и $f = gp_{l+1}q_l = gq_{l+1}$

□

4.11 Неприводимые простые многочлены. Свойства

Определение 4.8. *Пусть* $f \in K[t], \deg(f) > 0$.

Многочлен называется приводимым, если $f = gh$, *где* $g, h \in K[t]$, $0 < \deg(g) < \deg(f)$ *и* $0 < \deg(h) < \deg(f)$.

Если такого разложения не существует, многочлен называется неприводимым.

Если $f \in K[t]$ — неприводимый и $f = gh$, где $g, h \in K[t]$, то один из многочленов g и h — константа, а другой тогда ассоциирован с f.

Если $f \in K[t]$ — неприводимый, $f \vdots g$ и $0 < \deg(g)$, то $g \sim f$.

Свойство 4.8.1. *Пусть* $f, g \in K[t]$, g *— неприводимый. Тогда либо* $f \vdots g$, *либо* $(f, g) \sim 1$.

Доказательство. Пусть $d = (f, g)$. Тогда $g \vdots d$, то есть $g = dh, h \in K[t]$.

Тогда либо $\deg(d) = 0$ (в этом случае $(f, g) = d \sim 1$), либо $\deg(h) = 0$. Тогда $h \in K$ — константа и $g \sim d$ (так как $g = dh$, где h — константа). Так как $f \vdots d$ и $g \sim d$, то $f \vdots g$. □

Свойство 4.8.2. *Пусть* $g, f_1, \ldots, f_n \in K[t]$ *таковы, что* $f_1 \cdots f_n \vdots g$ *и* g *— неприводимый.*

Тогда существуют такие $i \in \{1, \ldots, n\}$, *что* $f_i \vdots g$.

Доказательство. Предположим противное, пусть $\forall i$ f_i не делится на g. Тогда, по свойству 4.8.1 $(f_i, g) \sim 1$ (так как g — неприводимый)

По свойству 4.7.3 тогда и $(f_1 \cdots f_n, g) \sim 1$, однако так как $f_1 \cdots f_n \vdots g$, то $(f_1, \cdots f_n, g) \sim g$. Получили противоречие. □

4.12 Основная теорема арифметики в кольце многочленов над полем. Каноническое разложение

Теорема 4.5. *Пусть* K *— поле,* $f \in K[t]$, $\deg(f) \geq 1$, *а* c *— старший коэффициент* f. *Тогда существует разложение* $f = c \cdot p_1 \cdots p_n$, *где* $p_1, \ldots, p_n$ *— неприводимые, со старшим коэффициентом 1. Такое разложение единственно с точностью до порядка сомножителей.*

Доказательство. Индукция по $\deg(f)$. База — случай неприводимых многочленов. Тогда $p = c^{-1} \cdot f$ — тоже неприводимый, со старшим коэффициентом 1 и $f = c \cdot p$ — искомое разложение.

Переход. Пусть для многочленов степени меньше, чем $\deg(f)$ утверждение доказано и f — приводимый. Тогда $f = gh$, где $g, h \in K[t], \deg(g), \deg(h) < \deg(f)$.

Пусть a и b — старшие коэффициенты g и h. Тогда по индукционному предположению $g = a \cdot q_1 \cdots q_s$, $h = b \cdot r_1 \cdot r_l$, где $q_1, \ldots, q_s, r_1, \ldots, r_l \in K[t]$ — неприводимые многочлены со старшими коэффициентами 1. Тогда $f = abq_1 \cdots q_s \cdot r_1 \cdots r_l$ — искомое разложение для f.

Докажем единственность индукцией по $\deg(f)$. База: пусть f — неприводимый и имеет разложение $f = cp_1 \cdots p_n$, где $p_1, \ldots, p_n \in K[t]$ — неприводимые. Тогда $f = p_1 g$, где $g \in K[t]$ и $\deg(p_1) > 0$. Следовательно, $f \sim p_1$, но тогда $f = cp_1$, а такое разложение ровно одно.

Переход. Пусть единственность с точностью до перестановки доказана для многочленов степени меньше, чем $\deg(f)$. Предположим, $f = cp_1 \cdots p_n = cq_1 \cdots q_m$. Тогда $q_1 \cdots q_m \vdots p_1$. По Свойству 4.8.2 $\exists i \in \{1, \ldots, m\}$ такое, что $q_i \vdots p_1$. НУО $i = 1$.

Так как $q_1 \vdots p_1$, q_1 неприводим и $\deg(p_1) \geq 1$, имеем $q_1 \sim p_1$, но оба многочлена имеют старший коэффициент 1, следовательно $q_1 = p_1$.

Тогда $f = c \cdot p_1 g$, где $g \in K[t]$, причем для g разложение единственно с точностью до перестановки, значит разложения $g = p_2 \cdots p_n$ и $g = q_2 \cdots q_m$ могут отличаться только порядком сомножителей.

Значит $f = c \cdot p_1 \cdots p_n = cq_1 \cdots q_m$ также отличаются только порядком сомножителей.

□

4.13 Значение многочлена в точке. Корень многочлена. Теорема Безу

Определение 4.9. *Пусть* $f = a_n t_n + \cdots + a_1 t + t_0 \in K[t]$.

1. ***Значение многочлена*** f *в точке* $\beta \in K$ *— это число* $f(\beta) = a_n \beta^n + a_1 \beta + a_0$.
2. *Если* $f(\beta) = 0$, *то* β ***- корень многочлена*** f.

Теорема 4.6 (теорема Безу)**.** *Пусть* K *— поле,* $f \in K[t], \alpha \in K$. *Тогда остаток от деления* $f(t)$ *на* $t - \alpha$ *равен* $f(\alpha)$.

Доказательство. Разделим $f(t)$ на $t-\alpha$ с остатком.

$f(t)=(t-\alpha)q(t)+r(t)$. Тогда, по теореме о делении с остатком (4.2) $\deg(r)<\deg(t-\alpha)$, при этом $\deg(t-\alpha)=1$, значит $\deg(r)=0$, то есть r — константа.

Тогда $f(t)=(t-\alpha)q(t)+r$, где $r\in K$.

Подставим вместо t α.

$$f(\alpha)=(\alpha-\alpha)\cdot q(\alpha)+r=0\cdot q(\alpha)+r=r$$

то есть $r=f(\alpha)$. □

Следствие 4.6.1. *Пусть K — поле, $f\in K[t]$, α — корень f. Тогда $f(t)\vdots(t-a)$.*

Доказательство. По теореме 4.6 $r=f(\alpha)=0$. □

4.14 Кратность корня. Теорема о сумме кратностей корней

Определение 4.10. *Пусть $f\in K[t],\alpha\in K$. Число α называется **корнем кратности** m многочлена f, если $f(t)\vdots(t-\alpha)^m$, но $f(t)$ не делится на $(t-\alpha)^{m+1}$.*

Теорема 4.7. *Пусть K — поле, $f\in K[t]$. $\deg f=n$, $\alpha,\dots,\alpha_k\in K$ — все различные корни f, причем корень α_i имеет кратность m_i.*

Тогда:

- $f(t)\vdots\prod\limits_{i=1}^{k}(t-\alpha_i)^{m_i}$
- $m_1+\dots+m_k\leqslant n$, *в частности* $k\leqslant n$.

Доказательство. Для любых $i\neq j$ очевидно, что $((t-\alpha_i)^{m_i},(t-\alpha_j)^{m_j})\sim 1$. Теперь пункт 1 следует из свойства 4.7.4 (так как все $(t-\alpha_i)^{m_i}$ попарно взаимно просты, и $f\vdots(t-\alpha_i)^{m_i}$ как корень многочлена)

Тогда $\deg(\prod\limits_{i=1}^{k}(t-\alpha_i)^{m_i})=\sum\limits_{i=1}^{k}\deg((t-\alpha_i)^{m_i})=m_1+\dots+m_k$ (равенство верное даже если K имеет делители нуля (по идее отличные от 1), так как $1\times 1\neq 0$, то есть сохранится старшая степень) Тогда, так как $f\vdots\prod\limits_{i=1}^{k}(t-\alpha_i)^{m_i}$, то $m=\deg(\prod\limits_{i=1}^{k}(t-\alpha_i)^{m_i})\leqslant\deg(f)=n$ □

4.15 Производная многочлена. Производная суммы и произведения

Здесь K — поле. Значит, существует $1\in K$. Будем использовать в поле K обозначение $n:=\underbrace{1+\dots 1}_{\text{n раз}}$.

Тогда из дистрибутивности следует, что $m\cdot n=(\underbrace{1+\dots+1}_{n})\cdot(\underbrace{1+\dots+1}_{m})=\underbrace{1+\dots 1}_{mn}=mn$

Определение 4.11. *Пусть $f(t)=a_nt^n+a_{n-1}t^{n-1}+\dots+a_1t+a_0\in K[t]$.*

*Тогда **производная** многочлена f это:*

$$f'(t):=na_nt^{n-1}+(n-1)a_{n-1}t^{n-2}+a_1$$

Лемма 4.5. *Для $f,g\in K[t]$ выполнено $(f+g)'=f'+g'$.*

Доказательство. Пусть $f=a_nt^n+\dots+a_0$, $g=b_nt^n+\dots+a_0$. (степени можно считать одинаковыми, иначе допишем нулевых коэффициентов)

Тогда $(f+g)(t)=(a_n+b_n)t^n+\dots+(a_1+b_1)t+(a_0+b_0)$ и $(f+g)'(t)=n(a_n+b_n)t^{n-1}+\dots+(a_1+b_1)=(na_nt^{n-1}+\dots+a_1)+(nb_n+\dots+b_1)=f'(t)+g'(t)$ □

Лемма 4.6. *Для $f,g\in K[t]$ выполнено: $(fg)'=fg'+f'g$*

Доказательство. Сначала рассмотрим случай одночлена:

$$((a_kt^k)(b_lt^l))'=(a_kb_lt^{k+l})'=(k+l)a_kb_lt^{k+l-1}=ka_kb_lt^{k+l-1}+la_kb_lt^{k+l-1}=$$

$$=((ka_kt^{k-1})(b_lt^l))+((lb_lt^{l-1})(a_kt^k))=(a_kt^k)\cdot(b_lt^l)'+(a_kt^k)'(b_lt^l)$$

Теперь общий случай: $f(t)=a_nt^n+\dots+a_0$, $g(t)=b_mt^m+\dots+b_0$

$$(fg)'=((\sum_{i=0}^{n}a_it^i)(\sum_{j=0}^{m}b_jt^j))'=(\sum_{i=0}^{n}\sum_{j=0}^{m}a_jb_jt^{j+i})'=$$

$$\sum_{i=0}^{n}\sum_{j=0}^{m}(a_jb_jt^{j+i})' = \sum_{i=0}^{n}\sum_{j=0}^{m}(a_it^i)' + \sum_{i=0}^{n}\sum_{j=0}^{m}(b_jt^j)' =$$

$$= (\sum_{i=0}^{n}(a_it^i)')\cdot(\sum_{i=0}^{m}b_jt^j) + (\sum_{i=0}^{n}a_it^i)\cdot(\sum_{j=0}^{m}(b_jt^j)') =$$

$$(\sum_{i=0}^{n}a_it^i)'\cdot(\sum_{i=0}^{m}b_jt^j) + (\sum_{i=0}^{n}a_it^i)\cdot(\sum_{j=0}^{m}b_jt^j)' = f'g + fg'$$

□

4.16 Производная многочлена, раскладываемого на линейные множители

Лемма 4.7. *Для $f(t) = \prod_{i=1}^{n}(t-\alpha_i)$, где $\alpha_i \in K$ (не обязательно все числа различны) $f'(t) = \sum_{i=1}^{n}\frac{f(t)}{t-\alpha_i}$.*

Доказательство. Индукция по $n = \deg(f)$. База $n = 1$ очевидна (тогда $f'(t) = 1$)

Переход. Пусть $g(t) = \frac{f(t)}{t-\alpha_n} = \prod_{i=1}^{n-1}(t-\alpha_i)$

Тогда $f'(t) = (g(t)(t-\alpha_n))' = g'(t)(t-\alpha_n)+g(t)(t-\alpha_n) = \sum_{i=1}^{n-1}\frac{g(t)}{t-\alpha_i}(t-\alpha_n)+g(t) = \sum_{i=1}^{n-1}\frac{\frac{f(t)}{t-\alpha_n}}{t-\alpha_i}(t-\alpha_n)+\frac{f(t)}{t-\alpha_n} = \sum_{i=1}^{n}\frac{f(t)}{t-\alpha_i}$ □

Следствие 4.7.1. *Пусть $\alpha \in K$, $f(t) = (t-\alpha)^n$. Тогда $f'(t) = n(t-\alpha)^{n-1}$*

4.17 Определение кратности корня многочлена с помощью производной

Для $f \in K[t]$ и $s \in \mathbb{N}$ обозначим через $f^{(s)}(t)$ s–ю производную многочлена f.

Теорема 4.8. *Пусть K — поле, $char(K) = 0$, $f \in K[t]$, $\alpha \in K$ — корень f. Тогда α корень кратности m многочлена f, если и только если $f(\alpha) = 0, f'(\alpha) = 0, \ldots, f^{(m-1)}(\alpha) = 0, f^{(m)}(\alpha) \neq 0$.*

Доказательство. Если α — корень кратности m многочлена f, то $f(t) = g(t)\cdot(t-\alpha)^m$, где $g \in K[t]$, и $g(t)$ не делится на $(t-\alpha)$.

Тогда по лемме 4.5 и следствию 4.7.1

$$f'(t) = ((t-\alpha)^m(g(t)))' = ((t-\alpha)^m)'g(t) + (t-\alpha)^m g'(t) = m(t-\alpha)^{m-1}g(t) + (t-\alpha)^m g'(t) =$$

$$= (t-\alpha)^{m-1}(mg(t) + (t-\alpha)g(t))$$

Таким образом, $f'(t) \vdots (t-\alpha)^{m-1}$. Так как $g(t)$ не делится на $(t-\alpha)$ и $m \neq 0$ ввиду $char(K) = 0$ следует, что $f'(t)$ не делится на $(t-\alpha)^m$.

Таким образом, при взятии производной кратность корня α понизилась ровно на 1. Значит все производные до $m-1$ включительно будут делится на $t-\alpha$, а $f^{(m)}$ не будет. По-этому, по следствию 4.6.1 $f(\alpha) = 0, f'(\alpha) = 0, \ldots, f^{(m-1)}(\alpha) = 0$ и $f^{(m)}(\alpha) \neq 0$.

Теперь докажем необходимость. Пусть α — корень кратности l, очевидно $l \in \mathbb{N}$. Тогда по доказанной ранее части $f(\alpha) = 0, f'(\alpha) = 0, \ldots, f^{(l-1)}(\alpha) = 0$, откуда понятно, что $l = m$. □

4.18 Основная теорема алгебры (формулировка). Неприводимые многочлены в $\mathbb{C}[t]$, разложение на линейные множители многочлена в $\mathbb{C}[t]$.

Теорема 4.9 (Основная теорема алгебры)**.** *Любой многочлен из $\mathbb{C}[t]$ имеет корень из $\mathbb{C}$.*

Следствие 4.9.1. *Неприводимые многочлены в $\mathbb{C}[t]$ — это в точности многочлены степени 1.*

Доказательство. Многочлены степени 1 всегда являются неприводимыми, это следует из определения.

Пусть $f \in \mathbb{C}[t]$ неприводимый, причем $\deg(f) > 1$. Тогда по основной теореме алгебры он имеет корень α. Тогда $f(t) = g(t)(t-\alpha)$, причем $\deg(t-\alpha) = 1$, $\deg(f) > 1$, значит $\deg(g) > 0$, то есть g — не константа, получаем противоречие с неприводимостью f. □

Следствие 4.9.2. *Пусть $f \in \mathbb{C}[t]$, $n = \deg(f)$, c — старший коэффициент f. Тогда $f(t) = c(t-\alpha_1)\ldots(t-\alpha_n)$, где $a_1, \ldots, a_n \in \mathbb{C}$ (не обязательно все эти числа различны)*

Доказательство. □

4.19 Сопряженные корни. Теорема о корнях многочлена с вещественными коэффициентами

Определение 4.12. *Для многочлена $f(t) \in \mathbb{C} = a_n t^n + \cdots + a_0$ введем обозначение $\bar{f}(t) = \bar{a_n} t^n + \cdots \bar{a_0}$.*
Так как $\overline{xy} = \overline{x} \cdot \overline{y}$ и $\overline{x+y} = \overline{x} + \overline{y}$, мы имеем $\overline{f}(\bar{t}) = \overline{f(t)}$.

Лемма 4.8. *Пусть $f \in \mathbb{C}[t]$, $\alpha \in \mathbb{C}$ — корень f кратности m. Тогда $\overline{\alpha}$ — корень $\overline{f}$ кратности m.*

Доказательство. По условию $f(t) = (t-\alpha)^m g(t)$. Тогда $\overline{f}(\bar{t}) = (\bar{t} - \overline{\alpha})^m \overline{g}(\bar{(t)})$.
Значит $\bar{t}$ имеет корень $\overline{\alpha}$ кратности не менее m.
Если бы кратность корня $\overline{a}$ была $k > m$, то аналогично доказывается, что $\alpha = \overline{\overline{a}}$ — корень $f = \overline{\overline{f}}$ кратности не менее k, что не так.
Значит $\overline{a}$ — корень $\bar{f}$ кратности ровно m. □

Теорема 4.10. *Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{C}[t]$ на множители*

$$f(t) = c(t-\alpha_1)^{k_1} \cdots (t-\alpha_s)^{k_s} (t-\beta_1)^{m_1} (t-\bar{\beta_1})^{m_1} \cdots (t-\beta_l)^{m_l} (t-\bar{\beta_l})^{m_l}$$

где $\alpha_1, \ldots, \alpha_s \in \mathbb{R}, \beta_1, \ldots, \beta_m \in \mathbb{C} \setminus \mathbb{R}$, и никакие из $\beta_1, \ldots, \beta_s$ не сопряжены друг к другу, и $n = \sum\limits_{i=1}^{s} k_i + 2\sum\limits_{j=1}^{l} m_j$

Доказательство. По Следствию 4.9.2 существует разложение $f(t) = c\prod\limits_{i=1}^{p}(t-\alpha_i)^{k_i}$, где $\sum\limits_{i=1}^{p} k_i = n$.
Не умоляя общности можно считать, что $\alpha_1, \ldots, \alpha_s \in Real$ (возможно $s = 0$), а остальные корни не вещественны.
По Лемме4.8, если $\beta \in \mathbb{C} \setminus \mathbb{R}$ — корень f кратности m, то и $\bar{b}$ — корень $\bar{f} = f$ (так как все мнимые части равны 0) кратности m.
Следовательно, $p - s \vdots 2$. Если $p \neq s$, то $p - s = 2l$ и корни $\alpha_{s+1}, \ldots, \alpha_p$ можно переобозначить как $\beta_1, \bar{\beta_1}, \ldots, \beta_l, \bar{\beta_l}$ так, что кратности корней β_i и $\bar{\beta_i}$ одинаковы и равны m_i. □

4.20 Неприводимые многочлены в $\mathbb{R}[t]$, разложение на линейные множители многочлена в $\mathbb{R}$[t].

Теорема 4.11. *Неприводимые многочлены в $\mathbb{R}[t]$ — это многочлены степени 1 и многочлены степени 2 с отрицательным дискриминантом.*

Доказательство. Пусть $f \in Real[t]$ — неприводимый и $\deg(f) = n > 1$. Если f имеет корень $\alpha \in \mathbb{R}$, то $f(t) = (t-\alpha)g(t)$, где $g \in \mathbb{R}[t]$, $0 < \deg(g) < n$, противоречие с неприводимостью f.
Значит, f не имеет вещественных корней. По Теореме 4.9 тогда f имеет корень $\beta \in \mathbb{C} \setminus \mathbb{R}$, но тогда по Теореме 4.10 и $\bar{\beta}$ — корень f, причем $f(t) \vdots (t-\beta)(t-\bar{\beta}) = t^2 - 2\operatorname{Re}(\beta)t + N(b)$.
При $n \geq 3$ имеем $f(t) = (t^2 - 2\operatorname{Re}(\beta)t + N(b))g(t)$, где $0 < \deg(g) < n$, противоречие с неприводимостью f.
Если $n = 2$, то $f(t) = c(t^2 - 2\operatorname{Re}(\beta)t + N(b))$, где c — старший коэффициент f и его дискриминант $D = 4c^2((\operatorname{Re}(\beta))^2 - N(\beta)) = -4c^2(\operatorname{Im}(\beta))^2 < 0$ □

Следствие 4.11.1. *Многочлен $f \in \mathbb{R}[t]$ нечетной степени обязательно имеет $\mathbb{R}$ корень.*

Доказательство. По Теореме 4.10 сумма кратностей всех комплексных корней f равна $\deg(f) \not\vdots 2$, а сумма кратностей невещественных корней четна.
Значит, сумма кратностей вещественных корней f нечетная, то есть, такой корень есть. □

Следствие 4.11.2. *Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{R}[t]$ на множители $f(t) = c(t-\alpha_1)^{k_1} \cdots (t-\alpha_s)^{k_s} \cdot (t^2 + p_1 t + q_1)^{m_1} \cdots (t^2 + p_l t + q_l)^{m_l}$, где $D(t^2 + p_i t + q_i) = p_i^2 - 4q_i < 0$ для всех i.*

Доказательство. По основной теореме алгебры (4.5) существует разложение многочлена $\frac{1}{c}f$ в проиведение неприводимых многочленов со старшим коэффициентом 1, которые имеют такой вид по теореме 4.11. □

4.21 Теорема Виета

Определение 4.13. *Пусть K — коммутативное кольцо, $a_1, \ldots, a_n \in K$ (не обязательно все числа различны). Введем обозначения:*

- $\sigma_1(a_1, \ldots, a_n) = a_1 + a_2 + \cdots + a_n$
- $\sigma_2(a_1, \ldots, a_n) = \sum\limits_{1 \leq i < j \leq n} a_i a_j$
- *при $k \leq n$* $\sigma_k(a_1, \ldots, a_n) = \sum\limits_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} a_{i_1} a_{i_2} \cdots a_{i_k}$

- $\sigma_n(a_1, \ldots, a_n) = a_1 a_2 \cdots a_n$

Теорема 4.12. *Пусть* $f = c_n t^n + \cdots + c_1 t + c_0 \in K[t]$, *причем* $f = c_n(t-a_1)\cdots(t-a_n)$. *Тогда* $\frac{c_i}{c_n} = (-1)^{n-i}\sigma_{n-i}(a_1, \ldots, a_n)$ *для каждого* $i \in \{0, \ldots, n-1\}$.

4.22 Интерполяция: формула Лагранжа

4.23 Метод интерполяции по Ньютону

4.24 Рациональные функции над полем. Правильные дроби и их свойства

4.25 Разложение правильной дроби в сумму правильных дробей, знаменатели которых — степени неприводимых многочленов

4.26 Разложение правильной дроби в сумму простейших

4.27 Связь задачи разложения правильной дроби в сумму простейших с интерполяцией. Критерий отсутствия кратных корней

4.28 Поле $\mathbb{C}$, как факторкольцо $[x]$.

4.29 Многочлен деления круга. Представление t^{n-1} в виде поризведение многочленов деления круга.

4.30 Многочлен деления круга: формула, целые коэфициенты

Глава 5

Многочлены и теория чисел

5.1 Показатель, к которому принадлежит вычет. Свойства.

Определение 5.1. *Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$, $d \in \mathbb{N}$. Вычет a принадлежит к показателю d, если $a^d = 1$, но $a^s \neq 1$ при $s \in \mathbb{N}$, $s < d$.*

Обозначение: $a \in_p d$.

Лемма 5.1. *Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$. Тогда выполнены слеующие утверждения:*

1. *Если $a^d = 1$ и $a \in_p s$, то $d \vdots s$.*
2. *Если $a \in_p d$, то $p - 1 \vdots d$.*

Доказательство. Предположим противное и поделим d на s с остатком: $d = sq + r$, $0 < r < s$. Тогда:

$$1 = a^d = a^{sq+r} = (a^s)^q \cdot a^r = 1 \cdot a^r = a^r$$

Получили число, такое что $a^r = 1$, при этом $a^s = 1$, s - минимальное возможное, и $r < s$. Противоречие.

Докажем второе утверждение. По теореме Эйлера $a^{\varphi(p)} \equiv_p 1$, значит $a^{p-1} = 1$. Воспользуемся первым утверждением. □

5.2 Количество корней многочлена $t^d - 1$ в $\mathbb{Z}_p$

Лемма 5.2. *Если $p \in \mathbb{P}$, и $p - 1 \vdots d$, то многочлен $t^d - 1 \in \mathbb{Z}_p[t]$ имеет ровно d корней, причем все они не 0.*

Доказательство. TODO!!! □

5.3 Количество вычетов, принадлежащих к показателю d.

Теорема 5.1. *Если $p \in \mathbb{P}$ и $d|p-1$, то к показателю d принадлежит ровно $\varphi(d)$ вычетов.*

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

Определение 5.2. *Пусть $p \in \mathbb{P}$. Вычет $a \in \mathbb{Z}_p$ — первообразный корень по модулю p*

По

5.5 Квадратичные вычеты и невычеты в Zp, их количества.

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

5.7 Решение квадратных уравнений в Zp.

5.8 Символ Лежандра

5.9 Формула при любом n

5.10 Формула при нечетном n.

5.11 Квадратичный закон взаимности Гаусса.

5.12 Лемма Гаусса и следствие о содержании произведения многочленов.

5.13 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].

5.14 ОТА в Z[x].

5.15 Критерий Эйзенштейна.

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

5.17 Разностный многочлен.